iapp

Privacy Risks to Individuals in the Wake of COVID-19

By IAPP Senior Westin Research Fellow Müge Fazlioglu, CIPP/E, CIPP/US

Privacy Risks to Individuals in the Wake of COVID-19

By IAPP Senior Westin Research Fellow Müge Fazlioglu, CIPP/E, CIPP/US

Privacy risks to individuals tend to be neglected due to the emphasis placed on privacy risks to organizations. Considering privacy risks to individuals, however, is critical to effective privacy risk management.

More specifically, privacy risks that threaten individuals — and, in turn, society — ultimately also present risks to businesses. An individual in this context means an employee, customer, client, board member, donor or any other person with whom an organization has a relationship.

Given the urgency of the public health emergency due to the COVID-19 pandemic, it is worth analyzing the unique privacy risks that have emerged. Organizations that take these privacy risks to the individual and society into account in their risk management programs will be better equipped to manage the overall risks to privacy brought about by the pandemic.

The privacy burdens on individuals and regulators

The protection and enforcement of privacy and data protection rights around the world depend considerably on the individual data subject. Indeed, many of the most fundamental rights within the privacy and data protection landscape — access, consent, correction, deletion, data security, transparency — have force primarily only when and if an individual proactively does something to protect their own data.

Laws and policies that require individuals to constantly update their knowledge and take initiative, however, have several limitations.

First, even highly motivated individuals may not know or be able to figure out how to navigate their lives in privacy-preserving ways, given the ubiquity of the surveillance systems observing them. Privacy laws and policies are often complex and difficult to understand, including for privacy professionals. Even "how to" guides regarding privacy protection aimed at consumers can be daunting to read and implement.

Second, and relatedly, the nature of consumer choices regarding privacy protection has usually been that of "take it or leave it." A common refrain from privacy scholars focused on the problems of choice and consent is to advise people who value privacy simply to not use a product or service. Interestingly, this is a choice that more and more consumers seem to be making. Pew Research recently reported, for example, that about half of U.S. adults have decided not to use a particular product or service due to privacy concerns.

Given that meaningful protection against privacy risks usually requires individuals to be both knowledgeable and assertive — a difficult task — privacy regulators and data protection authorities have stepped in to fill this void. As an aid to consumers, many privacy regulators have adopted public outreach, education and awareness as part of their primary duties.

> ***COVID-19 has proven to be one of the most effective phishing lures of recent years, as epidemics and health scares tend to provide fertile ground for social engineering attacks.***

Regarding scams that have emerged in the wake of the pandemic, for example, the U.S. Federal Trade Commission has responded by seeking to better educate consumers about these risks. Indeed, COVID-19 has proven to be one of the most effective phishing lures of recent years, as epidemics and health scares tend to provide fertile ground for social engineering attacks. As of May 2020, the FTC reported it had received more than 60,000 reports of fraud related to COVID-19, with individual losses estimated to be more than $44 million. Most of these schemes have been related to travel/vacations, online shopping and health care. While cybercriminals have gone after almost every demographic and firmographic, those working in health care, government, hospitality, retail, and research and education have been especially targeted.

More recently, scammers have impersonated public health authorities, claiming to be conducting contact tracing for COVID-19 and sending text messages that request personal information or ask people to click a malicious link. Thus, guidance from the FTC has urged consumers not to click links in unsolicited text messages, to be wary of COVID-19 contact-tracing text message scams, and to avoid falling prey to COVID-19 government imposter scams. Other pieces of advice have focused on COVID-19 scams targeting college students and how to work from home securely.

Yet, there remain a host of privacy risks to individuals who are outside the domain of either the individual affected or DPAs. For many privacy risks to individuals, organizations that control and process their data may be in the best position to assess and manage them. Organizations' efforts to reduce these risks can take many forms, such as by playing a supplemental role to DPAs and distributing their guidance or by working to address them through direct organizational actions.

The privacy gap organizations can fill

Privacy harms to individuals have tended to be ignored in the face of economic harm or reputational damage to corporations. Precisely because privacy risks to individuals are often the last ones to be considered in an organization's threat analysis, the danger they pose is much less understood than that of data

breaches and reputational damage. In other words, it is precisely because privacy risks to individuals are rarely assessed that less is known about the nature of the threat they pose to others in society, as well as businesses.

As the NIST Privacy Framework explains, failure by an organization to manage privacy risks "can have direct adverse consequences at both the individual and societal levels, with follow-on effects on organizations' brands, bottom lines, and future prospects for growth." And, although the consideration of societal harms is not required by the EU General Data Protection Regulation, as the Centre for Information Policy Leadership states, "the consideration of societal harms may be relevant and could be considered in appropriate circumstances."

Thus, organizations that integrate individual and societal privacy risks into their risk assessment programs will be better positioned to deal with privacy risk in general while filling gaps that individuals and authorities are either unable or unequipped to fulfill.

Identifying privacy risks to individuals

An important first step for an organization is to simply concede that privacy risks and harms are notoriously hard to define. There are widespread discrepancies not only in how laws define privacy harms, but also in how people think about them. Rather, because several alternative methodologies exist for identifying and classifying risks, harms or "feared events," this task remains a largely subjective exercise. Currently, no standard, widely used scheme exists to evaluate the likelihood and severity of privacy risks in a reliable way.

Organizations that integrate individual and societal privacy risks into their risk assessment programs will be better positioned to deal with privacy risk in general while filing gaps that individuals and authorities are either unable or unequipped to fulfill.

One of the reasons for the lack of reliability in privacy risk analysis is that a privacy harm may occur at a much later point in time than the privacy violation that generated it. This often makes it hard to trace a harm to a specific data point or violation. This decoupling of privacy harm from privacy violations and a focus on reducing the latter is an important principle in privacy by design, a point R. Jason Cronk has repeatedly made salient.

Among the numerous conceptual definitions of privacy risk/harm that have been development, Sourya Joyee De and Daniel Le Métayer describe it as "a negative impact of the use of a processing system on a data subject, or a group of data subjects, or society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, self-actualization, domestic life, freedom of expression or any fundamental right."

Similarly, a framework developed by CIPL includes tangible damage and intangible distress as two forms of individual privacy risks, resembling the dichotomy offered by University of Washington Professor Ryan Calo regarding objective privacy harms and subjective privacy harms. Some of the risks to individuals strike at the heart of democratic society and institutions: loss of self-determination, discrimination and loss of trust are examples of privacy risks to individuals that can have wide-ranging consequences for societies.

> ***The disclosure of a COVID-19 diagnosis can lead to certain privacy harms to individuals, as they become subjects of avoidance or exclusion from economic and social life.***

So, given these factors, how should an organization work to identify privacy risks to individuals?

The following sections analyze several specific privacy risks to individuals in the context of various data-processing operations that have emerged in the context of COVID-19. Namely, it analyzes the particular risks of stigmatization, scapegoating, ostracization and the broader risk of identification/re-identification.

COVID-19 privacy risks to individuals

Stigmatization, scapegoating and ostracization

The disclosure of a COVID-19 diagnosis can lead to certain privacy harms to individuals as they become subjects of avoidance or exclusion from economic and social life. Cases have already been reported in the media on the privacy harms suffered by individuals who have contracted COVID-19 and been socially ostracized, doxed or threatened. As a piece in The New York Times recently pointed out, even people who have recovered from COVID-19 are being shunned, "forced to navigate a world that clearly is not yet ready to welcome them back into a still-sheltering society."

Indeed, the particular harm stemming from the stigmatization of people with COVID-19 is that, rather than being treated as a person in need of care, they are often seen as a threat to others. Joint guidance from IFRC, UNICEF and the World Health Organization notes that the language used to describe people with COVID-19 ("cases" or "victims") and people who may have COVID-19 ("suspect" or "suspected cases") can lead to further stigma through its criminalizing vocabulary. Additionally, words that imply intention of transmission and assign blame ("transmitting COVID-19," "infecting others" and "spreading the virus") and the use of hyperbolic language ("plague" or "apocalypse") generate further stigma and fear.

Moreover, researchers in health policy have noted that throughout history, viruses have tended to be blamed on a "foreign other." This is also revealed by the militaristic terms that are commonly used to address COVID-19: "enemy," "target," "fight," "mobilize," "combat," as if it were an external invader or infiltrator rather than a naturally occurring part of the biome in which humans are embedded. These warlike metaphors undoubtedly add fuel to the fire of stigmatization. The origin of the coronavirus has been an issue of political debate and led to unwanted attention and hostility toward Asians around the world, including in European countries and the United States. An increase in the stigmatization of Asians, which has been fueled in part by online misinformation, has been documented during the COVID-19 era.

> ***The particular harm stemming from the stigmatization of people with COVID-19 is that, rather than being treated as a person in need of care, they are often seen as a threat to others.***

The impact of stigma from COVID-19 can be severe. More broadly, stigma of COVID-19 can "undermine social cohesion and prompt possible social isolation of groups," effects that themselves would also exacerbate the spread of the disease. Indeed, the uniqueness of the harm of stigmatization is such that it can engender more problems and even hamper solutions to the underlying problem. Stigmatization can motivate people with the disease to hide it to avoid discrimination, discourage people from seeking prompt medical care and demotivate their adoption of healthy behaviors. The reactions that characterized early responses to the development of the HIV antibody test may be instructive to understanding the stigma associated with being tested for COVID-19 today. As Columbia University Professor of Sociomedical Sciences Ronald Bayer had documented, some leaders in the LGBTQ+ community at the time thought that "[b]ehavioral change was critical for survival, yet testing might lead only to identification and stigma."

> ***Stigmatization can motivate people with the disease to hide it to avoid discrimination, discourage people from seeking prompt medical care and demotivate their adoption of healthy behaviors.***

Social distancing, which is a cornerstone of most public health efforts to mitigate the spread of COVID-19, has the potential to be enacted in a way that exacerbates stigmatizing behavior, such as through "othering, avoidance, and mistreatment toward persons associated with COVID-19."

But what is perhaps most worrying is that the stigma of COVID-19 is not simply promulgated by publics living in fear of the unknown, but through law and policy. In the technical assistance question and answers released by the U.S. Equal Opportunity Commission on what employers should know regarding COVID-19 and the Americans with Disabilities Act, for example, it states that an employer may withdraw a job offer to an applicant it needs to start immediately if that person displays the symptoms of COVID-19.

There have also been indications of the criminalization of people living with COVID-19. A memorandum from the U.S. Department of Justice sent to heads of law enforcement, for example, warned them that "you may encounter criminal activity ranging from malicious hoaxes to … the purposeful exposure and infection of others with COVID-19," an act it suggests "potentially could implicate the Nation's terrorism-related statutes." Reports of people being arrested for having COVID-19 and being in public spaces, not complying with self-isolation or merely claiming to have COVID-19 have been documented across various states in the U.S. and in countries around the world.

In Italy, for example, it was reported that 40,000 people who were found outside of isolation were charged with "aiding the epidemic" or investigated for "aggravated attempt to spread the epidemic." Other outlets reported that under Italian law, a person can be charged with "causing injury" or even "malicious or intentional murder" if it is determined that they passed the virus onto an elderly or vulnerable person who dies. Indeed, many of those whom have flouted the advice of public health authorities have been named and shamed online, as well.

Organizations can take many different actions to reduce or overcome the privacy risks of stigmatization, scapegoating and ostracization stemming from COVID-19. These can be symbolic in nature, such as through language choices that retain the dignity, autonomy and agency of people who contract COVID-19 or purposeful messaging campaigns, such as the "hero" campaigns regarding health care workers and others at higher risk of exposure to the virus that can contribute to reducing the risk of stigmatization.

> ***Consulting the guidance of national DPAs, which is updated regularly, should be at the forefront of privacy risk management programs.***

Other practical steps that organizations can take to reduce these privacy risks include ensuring that controlled procedures are in place for collecting and processing employee health information. For example, if an employer decides to implement temperature screenings for employees entering the office, these should be done in a non-public space. This will reduce the chances that this health information will be visible to others during collection.

Lastly, consulting the guidance of national DPAs, which is updated regularly, should be at the forefront of privacy risk management programs. The IAPP has aggregated DPA guidance on COVID-19 to make it easier for organizations to stay up-to-date.

Identification

Given the risks of stigmatization of people with COVID-19 and the scapegoating of various individuals and groups of people, another privacy risk presented by the COVID-19 pandemic is simply that of being identified or identifiable. It seems all but certain that an increase in surveillance and the privacy harms that accompany surveillance practices will be seen in the coming months and years.

While understanding that certain data-sharing practices during the pandemic are legally necessary (e.g., hospitals or testing centers that share data with public health authorities) or can play an important role in advancing public health (e.g., making data available to researchers), organizations should also be cognizant that sharing the names of people who have had or recovered from COVID-19 presents a privacy risk for them. Even if that data is anonymized before being sharing, the risk of re-identification and subsequent privacy harms can remain.

Numerous studies have documented that deidentified data, or data that is absent explicit identifiers, such as names, addresses or phone numbers, "can, in practice, be used to uniquely identify a person, to reveal sensitive information about them, and lead to significant privacy harms." A pioneer of this research, Latanya Sweeney, has shown that through the combination of publicly available datasets using methods known as data linking or data fusion, individuals can be re-identified by unique constellations of "quasi-identifiers." In a recent re-identification study, for example, she demonstrated that newspaper stories about hospital visits in Washington state could be linked to a specific individual 43% of the time.

> ***It seems all but certain that an increase in surveillance and the privacy harms that accompany surveillance practices will be seen in the coming months and years.***

> ***For employers that do choose to reveal the names of employees who have COVID-19 to other employees or business partners, they should analyze the nature of the privacy risks that such data sharing generates for those people.***

As the European Data Protection Board explained in its statement on the processing of personal data in the context of the COVID-19 outbreak, if it is "necessary" to reveal the name of an employee and if national law allows it, then "the concerned employee shall be informed in advance and their dignity and integrity shall be protected." Some DPAs have also noted that rules prevent the naming of employees who have acquired COVID-19. For employers that do choose to reveal the names of employees who have COVID-19 to other employees or business partners, they should analyze the nature of the privacy risks that such data sharing generates for those people.

A key step that organizations can take to reduce identification risks to individuals is to create a policy for COVID-19 data sharing and make that policy transparent to all individuals who may be affected by it. A key part of this policy should concern with whom it is necessary (outside of HR) to share diagnostic and other employee health data, keeping in mind the aim of data minimization. Organizations should also have a plan in place about when and how to notify health authorities, other employees or other affected stakeholders in various scenarios (e.g., when a person is displaying COVID-19 symptoms, when a person may have COVID-19 or when a person tests positive for COVID-19).

Having a plan for securely storing and deleting this data when it is no longer needed would also help to mitigate future privacy risks to individuals.

Conclusion

Specific privacy risks to individuals have accompanied the spread of COVID-19. Regulators have warned us about some; others have received less attention. Stigmatization, scapegoating and ostracization are particularly worrisome, as they can lead to loss of trust in organizations and institutions that collect and process data. This lack of trust, in turn, can reduce cooperation and foster behaviors that run counter to other important societal goals, such as public health, which is of utmost importance, especially during a pandemic.

Yet, there are multiple ways in which organizations are uniquely positioned to account for and work to mitigate these risks. Only considering privacy risks through an organizational lens can obscure more likely and impactful privacy risks to individuals that can ultimately harm an organization, both directly and indirectly through the ill effects they can have on society.

The COVID-19 pandemic will likely prompt many lawmakers, regulators and business leaders to think about risks to business, including privacy and data protection risks, differently. Broadening this discussion by including privacy risks to individuals can aid leaders seeking to rethink and better align their privacy risk management strategies with the complex and constantly changing reality in which we find ourselves.