The current COVID-19 pandemic raises some significant issues and risks relating to cybersecurity and data privacy in the US that should be considered carefully and addressed appropriately. Concerns range from cybercriminals targeting a newly-remote workforce with clever phishing scams that prey on the environment of uncertainty, to worries that the crisis will give cover to expanded and potentially problematic uses of technologies such as geolocation and facial recognition. Many businesses are unsure of whether and how to collect and disclose their employees’ health information under applicable privacy laws during an outbreak of infectious disease such as we are experiencing. This article addresses these and other data protection-related issues businesses are facing and offers some helpful guidance on mitigating such issues.

Rise in Cybersecurity Incidents

Cybersecurity incidents have increased since the COVID-19 outbreak and are expected to increase further during the coming months, as more and more of us are working remotely and as fraudsters look to leverage the uncertainty created by the crisis for phishing attempts and other forms of social engineering. Already there are reports of cybercriminals (as well as nation-state hackers) using interactive maps
displaying Coronavirus statistics and other types of bait documents to plant malware on devices. Fraudsters have also taken to posing as Centers for Disease Control ("CDC") officials in attempts to obtain financial account information. Despite the limited ability to undertake large IT projects at this time, there are some sensible measures that businesses can take to mitigate these threats. Examples of these measures include:

- Reminding employees that phishing attacks are rising rapidly; consider rolling out refresher training on how to detect phishing attacks other forms of social engineering and the organization’s procedures for responding to and reporting them.
- Reminding employees of the requirements of your information security, data handling, BYOD (bring your own device), data classification, data destruction, and other relevant policies, and the types of information that they need to continue to safeguard even when working remotely. Sensitive information, such as personnel records and financial information, stored on or sent to or from remote devices should be subject to heightened safeguards, such as the encryption of data in transit and at rest on the device and on any removable media used by the device.
- Reminding employees (if applicable) that they are required to use the company’s virtual private network (VPN) when working and accessing company information to ensure that internet traffic is encrypted, especially if connected to a public Wi-Fi network. As more companies rely on VPNs, hackers are identifying and taking advantage of vulnerabilities. See the US Department of Homeland Security’s alert [here](#).
- Reviewing incident response plans to ensure that the plan’s provisions are still practicable when the organization’s incident response team is working remotely. You should ensure that the protocols around incident response are clear, that incidents continue to be appropriately flagged and escalated, and that the incident response team can communicate effectively and efficiently. In order to do so, consider using communication techniques that operate outside of regular company communication methods (so-called “off-band” communication methods). Such off-band communication techniques should not be specified in your incident response plan, however, in the event cybercriminals obtain a copy of the plan.
- Of course, not all organizations will have adopted the types of dedicated policies and trainings referenced above. So this would be a good time for organizations to review the policies they have to determine whether they adequately address security requirements for remotely accessing company systems. If no such policies address this issue, then we highly encourage communicating to employees some basic guidelines for remotely accessing company systems and using personal devices for company business, even if not in the form of a formal policy.
- Ensuring that your organization has installed all relevant security patches. These patches address known security vulnerabilities and failure to install patches allows cybercriminals to exploit such vulnerabilities to gain access to company systems.
- If your organization hasn’t implemented multi-factor authentication, you should strongly consider doing so. Although this may be a larger IT project than is currently feasible, it will ensure greater security of the organization’s systems.
Tracking COVID-19 with Geolocation and Facial Recognition: Logistics and Concerns

In an attempt to halt the spread of COVID-19 and enforce social-distancing practices, the US government is reaching out to various companies in the private sector, including social media companies and telecommunications providers, to use existing technology, including app-enabled geolocation features and facial recognition technology. The government hopes that the use of this information will provide them with a better understanding of how the virus is spreading globally and whether or not individuals are practicing appropriate social distancing measures. Unsurprisingly, a variety of privacy considerations have arisen as a result of this information-sharing between the public and private sector.

The CDC is working with Palantir and Google, among others, to model the spread of the virus using data scraped from public social media. A task force has also been developed that is working in conjunction with the government, and includes several companies from the technology sector.

Data analytics company Palantir is working with the CDC to track COVID-19 through the use of data mapping and integration. The CDC previously worked with Palantir during the 2010 cholera outbreak in Haiti to monitor communications within the populace and track the spread of the disease. Similarly, the facial-recognition firm Clearview AI may potentially collaborate with state authorities to use facial-recognition technology to track infected individuals. Clearview reportedly developed its facial recognition algorithm using approximately 3 billion images scraped without permission from various websites. The company hopes to contribute to a greater understanding of “contact tracing”, the term given to the practice of identifying individuals that infected individuals may have been in contact with.

The government is also in active talks with technology companies about using location data gleaned from cell phones to track the proliferation of the virus and to track whether Americans are adhering to social distancing protocols. As currently developed, the plan would involve the technology companies sending collected anonymous and aggregated geolocation and facial recognition data from their apps to the federal government as a means to map the presence of the virus. At this time, Google has indicated that the plan would not involve sharing an individual’s movement or individual location. The data could be used to demonstrate the impact of social distancing and spread of COVID-19, similar to the way Google is able to show store traffic or traffic patterns. The assumption is that the spikes in aggregated geolocation data could help the government track COVID-19, while detecting, disrupting, and discouraging gatherings that could result in a dramatic transmission of the virus between infected and non-infected populations.

The use of this data seemingly pushes the bounds of US privacy laws. The data likely is not being used in a manner that has been clearly communicated to users and many obvious questions have yet to be answered:

- What information is being shared with the task force?
• How is the information being kept secure?
• What conditions are being placed on the use of this data?
• What are the processes and procedures in place for destroying the data (or returning it) once it is no longer useful to the task force?
• Will the data be used for additional purposes beyond tracking COVID-19 (e.g., for law enforcement purposes)?

Although the information is being shared for altruistic purposes (i.e., the tracking of COVID-19), opponents of the data sharing practice argue that there needs to be more clarity in how the data is being shared and there must be an emphasis on consumer protection.

These data sharing practices come on the heels of more draconian data sharing practices around the world, including extensive surveillance practices in Singapore tracking where infected individuals have been and the Iranian-state developed app for individuals to check their symptoms but which also includes a geo-tracking feature.

**Clarification of HIPAA Privacy Rules and Relaxation of HIPAA Enforcement**

In the wake of the COVID-19 outbreak, a host of unexpected issues and questions have arisen for entities that are regulated under the Health Insurance Portability and Accountability Act (“HIPAA”). Although HIPAA generally does not apply to an employer collecting health information in its capacity as an employer, employer-sponsored group health plans are subject to HIPAA directly and there is often ambiguity regarding the function an employer is performing. For example, HR personnel often perform both “employment” functions (not subject to HIPAA) and “group health plan” functions (subject to HIPAA). State laws also vary widely.

For entities that are covered under HIPAA (“Covered Entities”), the Office for Civil Rights (“OCR”) at the US Department of Health and Human Services released a bulletin in February addressing HIPAA Privacy in the context of the COVID-19 public health emergency (the “Bulletin”) and issued a notice in March regarding the exercise of its enforcement discretion in the area of telehealth (the “Notice”). Each of these developments is addressed below.

**Guidance for Employers**

The US Equal Employment Opportunity Commission has recently issued additional guidance for employers dealing with the issues presented by the COVID-19 pandemic. This information (available here) includes confirmation that employers may ask employees who report feeling ill or who call in sick whether they are experiencing any symptoms consistent with the coronavirus infection and may require employees to submit to non-invasive temperature testing to ensure employees are fever-free, each without violating the Americans with Disabilities Act (the “ADA”). The guidance additionally indicates that, consistent with the ADA, employers may require sick employees to stay home, and that employers may require employees who have been away from work due to illness to provide a doctor’s note certifying the employee’s fitness to return to duty, although the guidance indicates
that with the current demand on the healthcare system, alternatives to physician notes may be necessary. However, employers should still ensure that they are acting consistent with state paid sick leave laws, if applicable, to the extent they address return-to-work authorization.

We have put together helpful guidance in response to employers’ frequently asked questions about their obligations and exposure relating to the COVID-19 pandemic that is available here.

**Does COVID-19 halt the momentum of data privacy legislation?**

Among the unknown impacts of the COVID-19 pandemic is that on the momentum of new data privacy legislation in the US. While state legislatures and Congress are working overtime on addressing the economic fallout from the virus, other priorities are necessarily being pushed aside, including data privacy. In California, where a ballot initiative is pending that would strengthen the California Consumer Privacy Act, it is unclear whether the proponents will be able to gather the requisite signatures to get the proposal on the ballot, given that large parts of California are facing shelter in place orders. Businesses are alsopressuring the California Attorney General to delay enforcement of the California Consumer Privacy Act so they dedicate resources elsewhere. For unrelated reasons, the Washington Privacy Act failed to pass for a second straight year and it may be that such comprehensive bills were going to lose momentum in any event. But it seems clearer by the day that what was once a flood of new state data privacy bills will likely be reduced to a trickle until the COVID-19 crisis passes.

© Copyright 2020 Squire Patton Boggs (US) LLP