Legal Issues

Zoombombing, Location Tracking, and Contact Tracing, Oh My! Data Privacy & Cybersecurity During the COVID-19 Pandemic – April 17, 2020

Shannon M Holmberg

Throughout the COVID-19 pandemic, many businesses have implemented work from home policies to allow their business to remain in operation. As part of this effort, videoconferencing has become a common form of communication for businesses and individuals alike. This increased use of technology has exposed a corresponding increase in the exploitation of the technology's security vulnerabilities, putting private information at risk.

There has also been an increased use of technology for location tracking and contact tracing with the goal of reducing the spread of COVID-19. However, this use of technology is raising questions and concerns about the protection of individuals' data privacy rights.

While individuals and businesses continue to focus on maintaining their physical health and safety, they should also take steps to protect the health of their networks in order to bolster their cyber protections in light of the privacy and cybersecurity risks posed by COVID-19.

Zoombombing – A New Form of Cyber Attack

Pranksters and bad actors have capitalized on the increased usage of teleconferencing applications like Zoom to cause disruption and exploit this technology, putting individuals' and companies' information at risk.

"Zoombombing," a form of digital hijacking, is the unwanted intrusion into a videoconference by an uninvited participant. The term has grown out of the widespread use of the teleconferencing application Zoom during the COVID-19 pandemic, but similar incidents can occur on other platforms such as Skype and WebEx. Understandably, Zoombombings are wreaking havoc on schools, businesses, and individuals using these platforms, with bad actors entering the virtual meeting and posting lewd content or covertly listening in on discussions of confidential business information.

More than just being a nuisance, these unwanted intrusions expose significant security flaws that can be challenging to detect until an incident happens. While it can be challenging to detect vulnerabilities in your data

security systems until a breach incident occurs, there are actions your business can and should take to ensure your networks are secure:

- Create an **inventory list**, including the operating systems and software these assets use, and **audit** your business's network. This will help you ensure your network security is up to date and nothing is missed.
- **Penetration testing** - Hire cybersecurity professionals to perform simulated attacks on your network to exploit vulnerabilities and find new points of weakness.
- Work with a cybersecurity professional and your attorney to **bolster data security infrastructure** in accordance with legal requirements and best practices in order to eliminate those vulnerabilities.
- Create and test your **incident response plan** to contain the simulated attacks during the penetration testing, and make regular improvements to the plan.

In the short term, you can better protect your virtual meetings by enabling a number of security features within videoconferencing applications themselves:

- **Familiarize yourself** with the technology and security features before the meeting.
- **Avoid publicly sharing** meeting invitations.
- Require meeting **passwords** and keep them secure.
- Use **waiting rooms** to individually admit people to meetings.
- **Limit screen-sharing** access to the host.

While these measures will not necessarily protect your information from being shared in other ways, they can help you prevent unwanted intrusions.

While Zoombombing is a major concern for individuals and businesses alike, the privacy problems don't stop there. Several lawsuits have been filed against Zoom alleging failure to protect users' data from other sites who could use the information for marketing and other purposes.

Location Tracking

While governments, businesses, and individuals have engaged in monumental social distancing efforts to curb the spread of COVID-19, governments are now turning to social media companies and telecommunications providers to utilize technology to track whether individuals are following social distancing requirements through the use of geolocation and facial recognition technologies.

The use of these technologies necessarily requires that information about an individual's location and/or image are collected and shared with the government, creating concerns about the protection of individuals' privacy. While the U.S. does not currently have a uniform framework for data privacy regulations, other countries and specific states have enacted legislation protecting consumers' data privacy rights.

Using geolocation data from cell phones or other devices, the government can track the locations of individuals and use this information to break up gatherings and potentially prosecute offenders. In times of emergency and health pandemics, it is not uncommon for certain liberties to be restricted in the public interest. However, such use of technology and the sharing of information between private companies and the government raises a number of

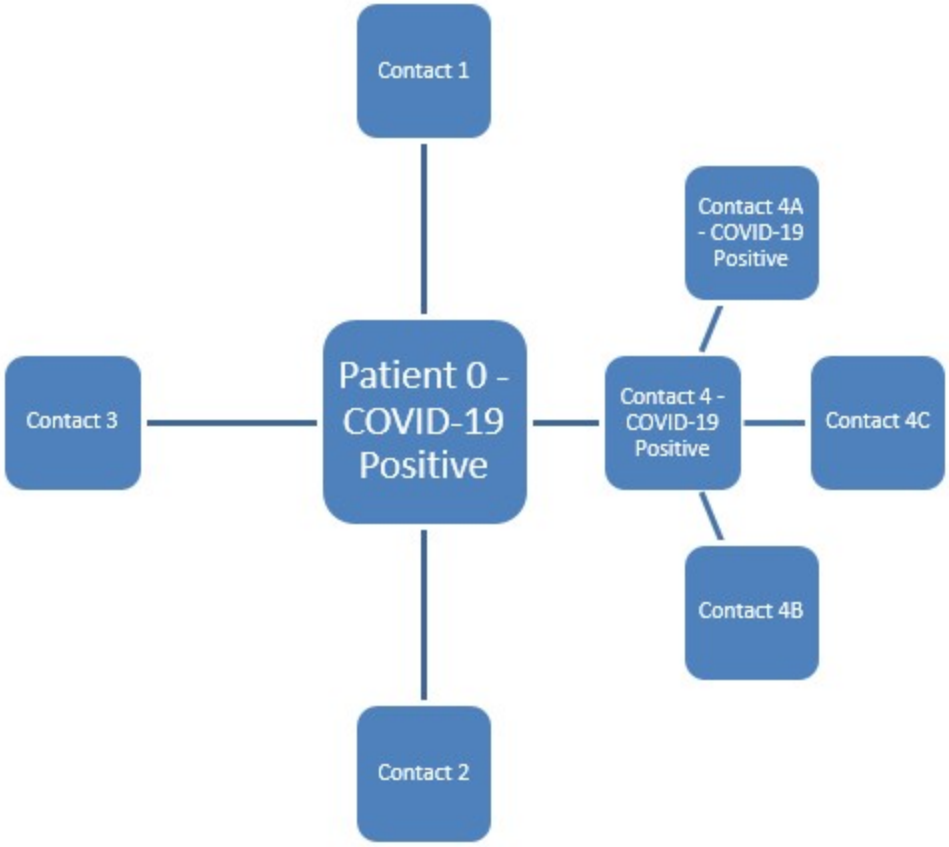
questions such as: What information is being collected and shared? What can the information be used for? How long is it kept and is it being stored securely?

Businesses seeking to engage in this type of activity should be transparent and disclose their data collection and sharing practices to consumers, as well as provide mechanisms by which consumers can opt out of such data collection. Be sure your privacy policy is up to date and reflects the activities you will engage in with respect to consumer data. Internally, be sure you are safeguarding data, limiting access, retaining data for limited periods of time, and securely destroying data when it is no longer necessary to maintain.

Individuals with concerns about their privacy rights should consult an attorney to determine whether their local laws provide additional protection and recourse.

Contact Tracing

Public health officials are also seeking to utilize technology for contact tracing - identifying and tracking individuals who come into contact with COVID-19 infected individuals. Contact tracing generally works by first identifying infected individuals and interviewing them or tracking their location to determine who they have come into contact with and where they have been. Public health officials then reach out to those exposed individuals and instruct them to monitor their health and/or quarantine. If the individual who was exposed becomes infected, their recent contacts and interactions are traced, and the process continues.



Companies such as Google and Apple have announced they are building systems that utilize Bluetooth technology to track the proximity of individuals and notify people who may have been exposed to an infected individual. Like

the location tracking technology used to implement social distancing, contact tracing raises important questions about the information collected and how and with whom it is shared.

There are also concerns over how this technology could be expanded. For example, Wuhan, China, which has recently reopened its borders, has begun to track citizens through an application that requires individuals to enter personal identification information, as well as respond to a series of health-related questions. Based upon these responses, the application generates a color code (red, yellow, or green) which corresponds to the individual's health and COVID-19 risk. Movement is then restricted based upon the individual's color-coded status, creating concerns that this intense surveillance could be used for purposes like targeting political protestors and other nefarious purposes.

Protecting Privacy During the Pandemic

Businesses and individuals should take steps to bolster the security of their networks and technology in light of the privacy and cybersecurity risks posed by COVID-19. In order to protect and secure data, businesses must be aware of their network vulnerabilities--especially while their workforce works remotely. Furthermore, businesses and individuals should ensure they are practicing the same data security practices they utilize while in the office, and they should also be cognizant of security features they can utilize when using videoconference and other technology.

Don't Forget the Human Component

With employers utilizing novel work from home platforms and strategies it can be overwhelming to make sure your workforce is up, running, and fully trained. It is easy for employees who may not normally use these platforms to become confused and fall victim to a phishing scam or allow a scammer access to passwords in the guise of facilitating a meeting. Focus your training on these developing issues. Make sure staff know that phishing attempts have exploded during the pandemic with everything from fake accounts and money transfer requests, to fake charities and larger hacking attempts. People are out of their comfort zone and processing change at a rapid pace–they might forget you have rules about wire transfer changes in this situation, so remind them. Also, some platforms are less secure than others and may not be appropriate depending on the type of meeting or data to be shared. While the Office of Civil Rights has loosened HIPAA/HITECH requirements for some platforms during the pandemic–others remain problematic.

The Big Picture

Like everything else compliance-related right now, these concerns may seem like they can take a back seat to immediate concerns about making payroll and whether you have a business tomorrow. However, because data privacy violations can come with expensive fines and cybersecurity lapses can cause massive disruption and monetary penalties, it is worth taking time now to consider your compliance and training carefully.
