WHEN COVID-19 WENT VIRAL, WERE YOUR PRIVACY RIGHTS INFECTED AS WELL?

BY KENNETH A. LINZER, ESQ. & FRANCES STRNAD

The novel coronavirus or COVID-19 pandemic has forced tens of millions and possibly billions of people to adapt to a "*new abnormal.*" This new abnormal includes social distancing, working from home, wearing face masks in public, attending remote video meetings on technologies like Zoom, Google Hangouts, Skype or Cisco Webex, to name just a few. Accompanying these adjustments, there has been a surge in the use of surveillance technologies and so-called contact-tracing apps by both employers and governments around the globe.

These surveillance technologies are commonly used by employers to ensure worker productivity and workplace connectivity, and by governments to monitor infection rates, prevent the further spread of the virus, keep track on their citizens and even to enforce social distancing guidelines. Some employers are using cameras in their offices, originally installed to monitor use of their workspaces, for the purpose of monitoring employee movements, ostensibly in order to ensure they maintain the proper social distancing. *But*, what other uses and possible impermissible invasions of workers' privacy does the use of these technologies portend?

Not to left out in the cold, some law enforcement agencies have even adapted aerial drones, used to remotely view and catalog activities in their jurisdictions, to track heat signatures and distances between citizens on the street. Ostensibly, these drones are being deployed for the purpose of monitoring compliance with social distancing guidelines and to prevent the spread of the virus; however, what other uses can and will be made of these various technologies?

In the United States, employers have implemented several measures to ensure that workers are productive while working remotely, whether from home, their automobile, their backyard or even the beach. Thousands of companies have begun monitoring their employees via surveillance software that tracks an employee's web searches, keystrokes, and screen time during active work hours. The surveillance software, sometimes called "tattleware," then sends screenshots of the employee's computer screen to their manager along with a daily report about that employee's productivity.

Additionally, some companies are enforcing "always on" webcam policies so that managers can randomly check on employees at any time. Although these policies are intended to provide workers with a feeling of human interaction, they often times end up invading privacy and distracting employees from their work.

In China, the government has used surveillance technology to enforce social distancing by installing cameras both inside and outside the homes of many of its citizens. Surveillance cameras located inside homes are placed facing the front door to record individuals entering and exiting the home. If a person attempts to leave their home and break a government-imposed quarantine, the surveillance technology immediately alerts authorities. Meanwhile, cameras located in public spaces use facial recognition software and artificial intelligence technology to detect human shapes, allowing government officials to monitor the public and ensure proper social distancing. According to a recent CNN report, it is estimated that China has approximately 567 million of these surveillance cameras in use, which is over six times as many as the U.S. does.

Similarly, the French government has installed security cameras in many public spaces, such as outdoor markets and buses, to ensure that people are wearing face masks and maintaining social distance. The surveillance technology automatically notifies the police when a person removes their mask or comes within 3 feet (1 meter) of another person. However, the French surveillance system differs from that of China because it does not use facial recognition technology or store identifying data about individuals, according to French data analytics company *Datakalab*.

Other countries have implemented GPS tracking technologies to monitor quarantined individuals. In South Korea, the government has created a mandatory phone app that tracks the location of people in quarantine and sets off an alarm if they leave their home. Many countries in South America have developed similar apps that track a user's location as a means of contact tracing. In Poland, people have the option to choose between randomly scheduled police visits to their home to ensure that they are staying in quarantine, or downloading an app that uses geolocation and facial recognition to confirm that the individual is staying at home.

As the line between public and private space has become increasingly blurred, these new surveillance technologies challenge legal norms regarding privacy, especially in the U.S. While the purpose of some of these technologies is apparent, such as contact tracing apps, what other purposes could and would they serve? While contact tracing apps are intended to provide a solution for public health officials, what protections have been implemented to protect the privacy rights of citizens. Some of the suggested apps, such as one being developed by Google-Apple, called Exposure Notification, maintains data on the individual's mobile device and is not passed on to a central database, while others pass this data to a central database.

When it comes to privacy rights, U.S. law protects a broad range of personal information and user data. These protections have thus far prevented the U.S. from utilizing many of the video surveillance and GPS tracking technologies that other countries have begun using to prevent the spread of COVID-19, or so, we have been led to believe.

When it comes to regulating video surveillance, the U.S. differs greatly from countries such as China, where government surveillance is generally accepted as the norm. U.S. laws, including the Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. §2511 *et seq*.) and the Fourth Amendment right that protects individuals from "unreasonable search," limit government video recording to public areas, excluding public areas where an individual could "reasonably expect privacy" (e.g. restrooms, hotel rooms, changing rooms). So, it is unlikely that the U.S. government will begin placing cameras inside of people's homes anytime soon. In contrast, China

currently does not have any national laws regulating the use of surveillance cameras in public areas, making it much easier for the Chinese government to monitor its citizens.

The United States Privacy Act of 1974 (5 U.S.C. § 552a) also provides a number of protections for user information, including location data. This makes it difficult for the U.S. to utilize location information collected by phone companies or GPS tracking apps for contact tracing.

Other countries that have similar data protection laws to the U.S. have found ways to utilize location data without infringing on privacy rights. In Singapore, for example, people participate in a voluntary location tracking system which assigns each person a unique QR code that they can scan in restaurants, taxis, and other checkpoints. This creates a virtual trail that can be used by the government to aid with contact tracing.

Another option that keeps location data private but also accessible to governments is using anonymized and aggregated location information. Austrian, German, and Italian telecommunication companies have provided their governments with anonymous location information which can help public health officials study the effects of social distancing.

Following in the footsteps of these European countries, the U.S. government is currently in negotiations with major technology companies, including Google and Facebook, about acquiring anonymized and aggregated location data that those companies have collected from users. However, it is uncertain when or if agreements with these companies will be made.

Privacy rights in the U.S. have also been challenged by surveillance technology implemented by employers. For example, software that records what an employee is typing, or collects data about an employee's web browsing history may accidentally collect private information. Depending on the type of information collected, the software may violate the Stored Communications Act (18 U.S.C. §2701 *et seq*.) which protects personal communication via email, social media accounts and other online messaging.

Surveillance software that tracks an employee's typing and computer usage may also collect an individual's medical information, social security number, financial information, and social media passwords. Obtaining this information without employee consent violates a variety of laws including the Americans with Disabilities Act (ADA) (42 U.S.C. § 12101), the California Consumer Privacy Act (CCPA) (Cal. Civ. Code §1798), and the Fair and Accurate Credit Transactions Act (FACTA) (15 U.S.C. §1681). Additionally, collecting an employee's social media passwords violates the law in 26 U.S. states, including California (Cal. Lab. Code §980).

In some cases, employer surveillance can also be uncomfortable because it invades the privacy of an employee's home. This provides further opportunity for the employer to accidentally listen in on personal communications or observe other private aspects of an employee's personal life. It may also violate laws protecting personal communication, such as the Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. §2511 *et seq*.), by infringing on an employee's reasonable expectation of privacy in their home.

In the coming months, employers and governments will need to find a balance between protecting individual privacy rights and ensuring public health. Finding this balance will determine the extent to which the various surveillance technologies impact each and every citizen's daily life.

June 2020

Sources:

https://www.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html
https://www.bbc.com/news/world-europe-52529981
https://www.cnn.com/asia/live-news/coronavirus-outbreak-03-04-20-intl-hnk/h_878ccdcbf1c36b0a299cbf9b784a36e5
https://www.france24.com/en/20200320-selfie-app-to-keep-track-of-quarantined-poles
https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/
https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html
https://www.samakowlaw.com/articles/law-video-surveillance/
https://www.natlawreview.com/article/out-sight-not-out-mind-monitoring-workers-working-home
https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/