Electronic technology is protecting us from COVID-19, but is it violating our privacy?

Individuals and institutions are taking drastic measures to flatten the curve of COVID-19 infections, and these measures, while important, may threaten our recently recognized privacy rights. This article examines the efforts taken to protect our society and how these efforts may interfere with individual privacy.

The most significant privacy infringements are playing out on a macro scale as governments and businesses join together to track and halt the spread of the disease. China locked down more than 500 million mostly-healthy people to keep COVID-19 in check, and has been using unmanned aerial vehicles to scan crowds and spot feverish people from hundreds of feet away, signaling alerts to watchers on the ground. Chinese state television noted that people in Shanghai who were ordered to be sequestered have digital monitoring devices attached to the doors of their homes. Baidu developed an algorithm for the Beijing subway police to quickly identify commuters not wearing masks.

South Korea is often cited as handling its virus response better than most other
countries and its government employed disinfectant-spraying drones and thermal goggles that read people’s temperature from a distance. South Korea also “rolled out a ‘Self-Quarantine Safety Protection’ tracking app to keep digital eyeballs on the roughly 30,000 people officials told to stay home for two weeks. If a person brings their phone out of the permitted area, a mobile alert gets beamed to the individual and their government case officer.”

The State of Israel gave an order to shelter at home to all of its citizens and used a cell phone tracking tool previously only used by the government for fighting terrorism. This tool notes movement of mobile phones so the government can tell if you are defying its orders and track your activities. Singapore is using QR codes to track citizens.

The U.S. is not immune to acceleration of government surveillance to fight the novel virus. According to the Wall Street Journal, data mining company Palantir is working with the Centers for Disease Control to model the viral spread, and “Other companies that scrape public social-media data have contracts in place with the agency and the National Institutes of Health.” The same article points out, “Crimson Hexagon, now part of Brandwatch, has a $30,000 contract with the CDC that was initiated last fall, according to government records. Crimson provides companies and governments with “social listening” tools, meaning it scrapes public Facebook, Instagram and Twitter posts in part to gauge sentiment.” Social media databases can be used to look for symptoms people discuss like shortness of breath, fever or cough.

That Google-sponsored website noted by the President, called Project Baseline, will link the information of people seeking testing with the other data Google collects about them. The Washington Post writes that the U.S. government is working with Facebook to track people’s movements and with Google to find insights through personal use of mapping applications. We also know that federal law enforcement has purchased large cell phone location databases from Verizon and AT&T, likely at least in part a reaction the SCOTUS Carpenter decision, limiting the government’s subpoena-free access to this information. No word of what kind of government databases will be left in the hands of the administration after the crisis is over.

Facial recognition database giant Clearview A.I., the current (and justified) boogie man of privacy intrusion, is according the WSJ, “in discussions with state agencies about using its technology to track patients infected by the coronavirus.” This would mean states tracking individuals using facial recognition and matching to public or business cameras. It is likely that license plate recognition operated by nearly all state law enforcement agencies will be harnessed for this task as well.

Our individual health information may also be at risk. Group health protection trumps individual privacy protection. At this stage, the US is failing to provide adequate testing resources to properly measure the growth of COVID-19 infections. If you should be tested, or if you have been tested positive, what happens to that information? Reports of your illness are dropped into aggregated statistics for national, state, and local governments, but some people need more specificity to protect them your contraction of this highly contagious illness.

Your employer, for example, will likely find out, and what will the company do with
the information? Will HR keep your name under wraps – formally and informally? Even if they don’t use your name, but announce that someone has contracted the disease, or several people contracted it, how easy will it be to figure out that one of them was you? The same may be true for your neighborhood association, the schools that your children attend and other social groups. If you attended a conference, everyone you contacted may be alerted to your condition. Climbing off a cruise ship can get you quarantined and followed by government. Protecting the community from infection runs entirely counter to your desire to hide your contraction of a seriously infectious disease.

Containing the COVID-19 outbreak is vital and, in such crises, the health of the many outweighs the privacy of the one. But will this incident simply push us three steps further into a complete surveillance community? It has allowed China to test technological methods for social control, and I doubt those tools will be shoved back in the closet. Our own government is building many new types of databases and analytics for learning about the population, including individual people and small communities. Will these tools be maintained or ditched? State and local police are bringing more surveillance technology to bear as well. They will surely keep using the information they learned even after the viral threat is gone.

2020 promises to be a year of continued breakthroughs in genetics and our knowledge of biological processes, but the containment of one virus has triggered an army of electronic and data-focused technology that will clearly help save lives. We must also be careful of what we lose in the process of implementing this tech.

[1] A blog post on privacy issues with Clearview A.I. is written but not published here yet. Watch this space.

Copyright © 2020 Womble Bond Dickinson (US) LLP All Rights Reserved.