All over the country, states are re-opening their economies. This is happening in defiance of recommendations from experts in infectious disease, which suggest that states only re-open after they have seen a fourteen-day decline in cases, have capacities to contact trace, have sufficient personal protective equipment for healthcare workers, and have sufficient testing capabilities to identify hotspots and deal with problems when they arise.

Experts do not insist that things need to be shut down until the virus disappears. Instead, we need to change our practices; we need to open only when it is safe to do so and we need to employ common sense practices like social distancing, mask-wearing, and hand-washing and sanitizing when we take that step. The ability to identify people who either have or might have coronavirus and to contact those with whom they might have come into contact could play a significant role in this process. Instead of isolating everyone, we could isolate those we have good reason to believe may have become infected.

Different countries have approached this challenge differently. Many have made use of technology to track outbreaks of the virus. Without a doubt, these approaches involve balancing the value of public safety against concerns about personal privacy and undue governmental intrusion into the lives of private citizens.

Many in the West were surprised to hear that Shanghai Disney was scheduled to re-open, which it did on May 11th. Visitors to the park won’t have the Disney experience that they would have had last summer. First, unsurprisingly, Disney is restricting the number of people it will allow into the park at any one time to 24,000 people a day. This is down from its typical 80,000 daily guests. When guests arrive, they must have their temperatures taken, must use hand sanitizer, and must wear masks. Crucially, they must open an app on their phone at the gate that demonstrates to the attendant that their risk level is green.

Since the COVID-19 outbreak, people in China have been required to participate in a system that they call the “Alipay Health Code.” To participate, people download an app on their phones which makes use of geolocation to track the whereabouts of everyone who has it. People are not required to have a COVID-19 test in order to comply with the demands of the app. Instead, the app tracks how close people have come to others who have confirmed cases of the virus. The app assigns a person a QR code depending on their risk level. People with a green designation are low risk and can travel through the country and can go to places like restaurants, shopping malls, and amusement parks with no restrictions. Those with a yellow designation must self-quarantine for nine days. If a person has a red designation, they must enter mandatory government quarantine.
At first glance, this app appears to be a reasonable way of finding balance between preventing the spread of disease on one hand, and opening up the economy and freeing people from isolation on the other. China isn’t simply accepting the inevitable—opening up the economy and disregarding its obligation to vulnerable populations. Instead, it is trying to maximize the well-being of society at large.

Things are more complicated than they might originally appear. First, the process is not transparent to citizens. The standards for reassignment from one color designation to another are not made public. Some people are stuck in mandatory government quarantine without knowing why they are there or how long they might expect to be detained.

There are also concerns about regional discrimination. It appears that a person can be designated a particular threat level simply because they are from or have recently visited a particular region. Citizens have no control over how this process is implemented, and the concern is that decision-making metrics might be discriminatory and might serve to reinforce oppressive social conditions that existed before COVID-19 was an issue. We know that COVID-19 disproportionately affects people living in poverty who are forced to work in unsafe conditions. This kind of tracking may make life for these populations even worse.

There are also significant concerns about the introduction of a heightened degree of governmental surveillance. Before COVID-19 hit, the Chinese government had already slowly begun to implement a social credit system that assigns points to people based on their social behaviors. These points then dictate the quality of services for which the people might be eligible. The Alipay Health Code increases governmental surveillance and encroachment. When people download the Alipay app, the program that is launched includes a command labeled “reportInfoAndLocationToPolice” that sends information about that person to a secure server. It is unclear for what purpose that information will be used in the future. It is also unclear how long it will be mandatory for people in China to have this app on their phones.

But China is not the only country that is using tracking technology to manage the spread of COVID-19. Other countries doing this include South Korea, Singapore, Taiwan, Austria, Poland, the U.K., and the United States. There are advantages and disadvantages to each system. Each system reflects a different balance of important societal values.

South Korea’s system keeps its residents informed of the movement of people who have tested positive for COVID-19. The government sends out texts informing people of places these individuals have been so that others who have also been to those places know whether they might be at risk. This information also lets people know which places might be hotspots so they know to avoid those places. All of this information is useful to prevent the spread of the virus. That said, there are serious challenges here too. Information about the location of individuals at particular times leads to speculation about their behaviors that might lead to discrimination and harassment. The information is anonymous in principle; COVID-19 patients are assigned numbers that are used in reports. In practice, however, it is often fairly easy to deduce who the people are.

Some countries, like the U.K., Singapore, and the United States have “opt-in” tracking programs. Participation in these programs is voluntary and there tend to be regional differences in what they do and how they operate. Singapore uses a system called “TraceTogether.” Users of the app turn on Bluetooth capabilities for their devices. Each device is associated with an anonymous code. Devices communicate with one another and store each other’s anonymous codes. Then, if a person has interacted with someone who later tests positive, they are informed that they are at risk. They can then take action; they may be tested or may self-quarantine. This system appears to have established a comfortable balance between competing interests.

One problem, however, is that its voluntary nature results in low participation numbers—only 1.5 of Singapore’s 5.7 million people are using the app. What follows from this is that a person has the peace of mind of knowing that if they have been in contact with another app user who contracts COVID-19, they’ll know about it. However, this kind of system doesn’t achieve that much-desired balance between concerns for public safety and concerns for a healthy functioning economy. If a person knows only about some, but not all, of the people they’ve encountered who have
tested positive for COVID-19, they’re no safer out in the world as a consumer in a newly-opened economy. This app also does nothing to prevent the spread of the virus by asymptomatic people who may never feel the need to get tested because they feel fine.

There are other, less straightforward ways of collecting and using data about the spread of the virus. Government agencies are attaining geo-tracking information from corporations like Google and Facebook. Most users don’t pay much attention when an app asks if it can track the user’s location. People tend to provide a morally meaningless level of consent—they click “okay” without even glancing at terms and conditions. Corporations use this information for all sorts of purposes. For example, police agencies have accessed this information to help them solve crimes through a process of “digital dragnet.” Because these apps track people’s movements, they can help the government to see who was present at sites later identified as hotspots and can identify where people at those sites at the time in question went next. This can help governments direct their attention to where it might do the most good.

Again, in many ways, this seems like a good thing. We don’t want to waste valuable time searching for information where there isn’t any to be found. It’s best instead to find the clues and follow them. On the other hand, this method of attaining information highlights something troubling about trust and privacy in the United States. A Pew poll from November, 2019 suggests that citizens view themselves as having very little control over who is collecting data about them and very little knowledge about what data is being collected or the purposes for which it is being used. Even so, people tend to pay very little attention to the fact that they are being tracked. They simply accept the notion that, if they want to use an app, they have to accept the terms and conditions.

People concerned about personal liberties are front and center on the public stage right now as their protests make for attention-catching headlines. People are unlikely to want to be forced by the government to use a tracking app. Their fears are not entirely unfounded—China’s program seems to open the door for human rights violations and a troubling amount of governmental surveillance of private citizens. Ironically, though, these people give that same information without any fuss to corporations through the use of apps. This may be even worse. At least in principle, governments exist for the good of the people, while the raison d’être of corporations is to make a profit.

The case of tracking poses a genuine moral dilemma. There are very good public health reasons to use technology to track and control the spread of the virus. There are also very good reasons to be concerned about privacy and human rights violations. Around 3,000 people died in the tragic terrorist attacks that took place on September 11th, 2001. As a result, Congress passed The Patriot Act, which significantly limited privacy rights of the people. Its effect on the way respect for individual privacy changed at airports is also noteworthy. How much privacy should we be willing to give up in exchange for safety? If we were willing to give up privacy for safety in response to 911, how much more willing should we be to do so when the death count is so much higher?