Privacy vs. Security in the Post-Pandemic World

Article By

Jeffrey L. Turner
Squire Patton Boggs (US) LLP
Capital Thinking Blog

Related Practices & Jurisdictions

- Coronavirus News
- Communications, Media & Internet
- All Federal
- European Union

Friday, June 12, 2020

"Do you give up a little liberty to get a little protection?"

As green sprouts start to appear in parts of the global economy, much uncertainty remains about how the COVID-19 pandemic will affect our collective future. Amidst this ambiguity, one of the few things that appears certain is that technology will play a significant role in any solution to containing the virus. Whether the technology solution is the user-first, privacy-oriented model championed by Google and Apple in the United States or is more akin to the more draconian – and arguably more effective – regimes in other parts of the world will depend largely on how the public responds in making the choice between liberty and protection. This dilemma is as old as the internet itself.

With the growth of electronic commerce in the early to mid-1990s, policymakers in the European Union and the United States began to grow increasingly concerned
about the data collection policies of Internet Service Providers and other companies engaged in this newly emerging marketplace. In 1995, for example, the European Union adopted the Data Protection Directive, which sought to enhance an individual’s right to privacy. Among other things, the Directive sought to ensure that companies would not process personal data unless they met certain broadly defined conditions.

In the United States, policymakers similarly grew concerned about user privacy, especially for children under the age of 13. Their initial efforts led to the enactment of the Children’s Online Privacy Protection Act in 1998. In broad terms, it required a website operator to establish a privacy policy, to seek viable consent from a parent or guardian before granting access to their children, and then to protect their privacy and safety when they were online. In 1999, as part of a major financial services reform bill (better known as the Gramm-Leach-Bliley Act), the US Congress included a Financial Privacy Rule, which required financial institutions to provide consumers with a privacy notice when establishing a relationship and annually thereafter. It also required financial institutions to give consumers the right to opt out of sharing personal information with unaffiliated parties.

With the growth of AOL (then known as America Online) and other Internet Service Providers in the early days of the Internet (when the word was still capitalized), the US Congress turned its attention to how these companies used the personal data they collected from their users. In broad terms, that debate over privacy legislation came down to two fundamentally different approaches: “opt in” or “opt out,” i.e., could companies make use of personal information only if users agreed in advance (opt in) or could companies make use of that information as long as a user had not said no (opt out)? There of course was a wide-ranging debate about what information would be covered, how it could be collected and how it could be used, but the larger issue was essentially a binary one. And it was still unresolved as of September 11, 2001.

Following the 9/11 attacks, the terms of the debate shifted to another binary choice, but a fundamentally different one: privacy vs. security. With virtually no debate, security won. By October 2001, Congress had approved, and the President had signed into law, the USA Patriot Act. Among other things, the new legislation authorized the Federal Bureau of Investigation to search an individual’s telephone, email, and financial records without a court order; it gave law enforcement authorities the right to search homes and businesses without the owner’s knowledge or consent; and it gave these authorities expanded access to individual and business records, including access to a person’s library records. By 2002, Congress had created the Department of Homeland Security, further enhancing the power of the federal government to protect the American public.

For roughly a decade, security continued to win that debate. But as the harrowing memories of the twin towers began to fade and as the small “I” internet became more pervasive across the globe and electronic commerce continued to grow exponentially, policymakers again began to focus on the privacy rights of individuals. The US Congress began to debate the issue again, but without reaching consensus on whether and how to address various competing concerns. Across the pond, the European Union took action. By 2016, it had adopted the General Data
Protection Regulation (GDPR), which in broad terms is intended to protect individuals with respect to the processing of personal data and limits how that data can be shared.

Impatient with the lack of action at the federal level in the United States, the California legislature adopted the California Consumer Privacy Act (CCPA) in 2018. Among other things, the CCPA creates new consumer rights relating to access to, deleting of, and sharing of personal information collected by businesses. In contrast to the general acceptance and implementation of GDPR, the business community has largely fought implementation of the CCPA and sought further revisions to it in order to address major compliance and implementation issues. Many tech sector companies in particular began making a major push last year for the US Congress to adopt a privacy bill that would preempt the CCPA and other emerging state efforts modeled on the California approach.

As of today, the US Congress has not taken action on any of the pending privacy bills, as no consensus has been reached on two fundamental issues: federal preemption of state law, including the CCPA, and the right of private parties to sue to enforce their rights. We recognize the challenge of overcoming the largely partisan divisions that have stood as a barrier to compromise over the past decade. But, as we suggest below, enactment of at least a narrowly limited bill dealing with ensuring the privacy of contact tracing data would undoubtedly help encourage greater use of the technology.

As policymakers in the United States and around the globe deal with the COVID-19 pandemic, we have arrived again at a point in time in which they appear to face virtually the same binary choice as policymakers did after 9/11: privacy vs. security. While the scale, scope and speed of technology has changed dramatically in the two decades since the last national security crisis of this magnitude, the strain between privacy and security in the COVID-19 era today presents many of the same challenges as a generation ago.

We explore below the tensions policymakers and the public face and the changed conditions from that era, both here and across the globe.

Emerging Battle Lines

Dr. Anthony Fauci, Director of the National Institute of Allergy and Infectious Diseases, recently posed this question during a live Snapchat interview: “Do you give up a little liberty to get a little protection?” As occurred after 9/11, large segments of the public might make the same choice again.

But we could see a potential middle ground develop or a generational divide in how the public responds. With the launch of an “exposure notification” tool on May 20 by Apple and Google, this well-developed and privacy-protecting technology is now available to aid in contact tracing by helping individuals learn whether they have been in contact with someone who had (or who later tests positive for) the coronavirus. In fact, this is a great example of businesses applying “privacy by design” principles into a product before launching it. The two traditional rivals worked together to build an app that uses Bluetooth technology that would provide an alert to a user of the technology that he or she has been in close proximity to or
in contact with someone who voluntarily uploads that information to his or her mobile device. Importantly, they designed the app so that the data would only stay on the recipient’s phone for 14 days and then would disappear. Moreover, they specifically designed the app so it would not mark the location where the contact occurred. With the privacy concerns of their users in mind, they quite purposefully designed the technology so that the data would not be available to the government or local health authorities. Additionally, they designed the app so that the data couldn’t be shared with employers or insurers.

By putting the privacy of their users first in designing the app, there could be a tension with the desire of some governmental authorities to obtain the data (even anonymized) that such apps produce, which could be a very powerful tool in fighting the pandemic. The companies clearly understood this, but they nonetheless put the interests of users ahead of others, much as Apple, Android and others have done in designing phones that give them no access to the data on a phone.

At the moment, at least in the United States, polling suggests that a majority of Americans are not willing to use the technology, even with these limitations having been built in to protect their privacy. Moreover, the app is of no utility to people who do not own a smart phone. Should re-opening of the economy here and abroad lead to a second surge of infections, however, attitudes might well shift towards greater adoption and use of the technology. On the other hand, as weeks of social distancing turn into months, and potentially years, it seems quite possible that real generational schisms will develop with respect to the emphasis placed on privacy versus security. One could foresee a scenario where tech-savvy millennials and Gen-Z value privacy more than Gen-X and boomers, who are far more concerned than younger generations about contracting the virus themselves. And it’s anyone’s guess just how all of this will be affected by heightened surveillance in the aftermath of recent social unrest in response to the tragic death of George Floyd in Minneapolis.

New apps are being developed in the EU as well, but with a difference. Some of what governments are doing now indicates a willingness to stretch things more in order to deliver a public good than in the past. For example, a number of European governments are using anonymized mobile network data to understand how lockdown measures are working in practice, and to plot the links between population mobility and virus propagation. That some governments (such as the UK and French) are trying to centralize the contract tracing approach, with the central government being the repository of all the data and directing the app functionality (such as how and when the device’s Bluetooth connectivity is turned on/off), brings these concerns to the fore.

The European Commission has invited telecommunications companies to make their metadata available. EU Commissioner Thierry Breton wants to receive mobile data from EU telecoms companies during the coronavirus outbreak. He said that obtaining certain data sets would allow “the impact of the containment measures taken by member states” to be more clearly seen. The commission called on the telecommunications companies to “hand over anonymized mobile metadata to help analyze the patterns of coronavirus spread.” To date, EU members have been using apps based on different methods. Justice Didier Reynders told the European
Parliament that he preferred a “decentralized approach.” Recently, the EU’s justice chief threw his weight behind the app developed by Apple and Google.

South Korea, one of the most successful at dealing with Coronavirus, has made extensive use of mobile network data and has linked app-sourced data with CCTV in order to get as comprehensive as possible a picture of someone’s potential infection. That success comes with a price, which we doubt many Americans are yet willing to accept: For many years, the Korean government has tracked massive amounts of transaction data, such as every credit card purchase or mobile payment purchase, in order to ferret out tax fraud. The technology has now been re-purposed to monitor the movement of the entire population when using a credit card or electronic payment app. So, it knows, for example, where its citizens purchased a cup of coffee or hopped on a bus. Very effective, no doubt, in helping to stamp out a virus; not so good if you cherish your freedom to go about your business without cameras and other technology monitoring your every move in public.

In contrast, Germany – the most successful of the large European countries at tackling the pandemic – has put privacy ahead of analytics, and is following the Google/Apple approach. Although it had initially supported the centralized approach to data gathering, it reversed its approach in reaction to widespread privacy concerns. This change of direction marked a major blow to a homegrown-standardization effort, called PEPP-PT, that had been aggressively backing centralization while insisting it was preserving privacy by not tracking location data. Nonetheless, concerns had been raised by privacy advocates about governmental authorities having access to an individual’s “social graph” and the potential for function creep and potentially state surveillance, of the kind that appears to have been accepted willingly in South Korea.

Although Australia has been relatively successful in mitigating the widespread health impacts of COVID-19, the federal government has encouraged all Australians to download its COVIDSafe digital contact-tracing app, indicating that the relaxation of COVID-19 restrictions may depend on the app’s take-up by the Australian public. Not surprisingly, due to privacy concerns, support for a contact-tracing app has been mixed, even within the government itself. Australia is not the first country to offer contact-tracing apps as a solution to the current pandemic. In fact, the app is based on Singapore’s TraceTogether app, which launched in late March 2020 and has been released as “open-source” code so that it can be used by other countries. Perhaps surprisingly, the app has not been widely embraced by the Singaporean population. If it won’t be used there, it is hard to see it being adopted on a voluntary basis more widely throughout the world.

What Next?

We have seen a great deal of commentary about the extent to which this or that use of the apps would be legally allowable. This, however, ignores two important considerations: European governments are all operating using one or another form of emergency legislation. They have ample legislative power to ensure that whatever they want to do is lawful. And there are many different approaches to safeguards to ensure compatibility with human rights legislation. One advantage – in precedent setting terms – of using emergency powers is that they, and the measures they have
put in place, lapse when the emergency is over. All apps will come with consents built into their provision. As suggested above, in current circumstances the public might well be willing to consent to quite a lot.

There are many different approaches and open questions:

- Will apps be mandatory or voluntary? Most likely they will be voluntary, but strongly encouraged – possibly mandatory in some circumstances. The consent issue is therefore highly significant.

- Will apps store data on peoples’ phones or centrally? Both are being produced. As noted above, the app developed by Apple and Google keeps the data on the phone, and then only for a limited time. Phone storage has obvious advantages for privacy, but public health authorities get no data. Moreover, the effectiveness at individual level is entirely dependent on whether recipients of alerts do anything about them.

- Will health service “track and trace” capability have any access to app data of someone who tests positive? If they do, it could partially assist with the inefficacy issue identified above. But if they do, the privacy argument in favor of decentralized data will be substantially eroded.

- Will sufficient numbers of individuals use the technology for it to have any value? Studies suggest that at least 50-60% of the population, if not substantially more, must use a contact tracing app for it to have any utility. As a recent report from Oxford University demonstrated, if 56% of the population used an app (or 80% of smartphone users), its use could bend the curve below the threshold for further spread of the virus, but then only if individuals over age 70 remained in lock down and the public engaged in social distancing. And even when a sufficient percentage of the public agree to use it, will there be enough individuals engaged to actually do the contact tracing necessary to bend or flatten the curve and will they make the other sacrifices necessary to bend the curve, such as self-isolation and social distancing?

- As a related question, can the contact tracers be effective if they don’t have access to the data? And if governmental authorities mandate that access, what is to stop them from sharing the data more widely among other health officials?

If the effect of absolute adherence to the very important civil liberty of privacy is that governmental authorities have to deprive you of other very important civil liberties such as leaving your house when you want to, or earning your living, you might be more willing to accept a strictly limited and controlled reduction to your privacy in order to secure the other rights you want to exercise.

Other issues abound: Will employers have any access to app data, or the ability to require employees to use them? There is a great deal of concern among both employers and employees about safety at the workplace, and employers have obligations to their employees which are extremely difficult to meet in some circumstances. If – as in many countries – employers can effectively compel employees to have temperatures monitored or to wear personal protective equipment, why should they not be able to compel them also to use apps which can
help to indicate the potential to be infectious? Employers have “track and trace”
equivalent obligations at the workplace, and some are looking at putting in place
their own apps to enable them to fulfill these obligations. For the employer, it is a
fine balance between the duty of care for the workforce as a whole, and the duty of
care for the individual within the workplace. Not many countries have taken a
position on this yet. Australia has decided against allowing employers access to the
government sponsored app.

Some employers are however taking matters into their own hands, and providing
track and trace devices to their employees to use in the workplace. Early anecdotal
evidence suggests that employees welcome them, as something which will help to
keep them safe. Such workplace apps obviously raise a host of privacy issues.

Other employer-employee confrontations are on the horizon as well, as employers
seek to use Artificial Intelligence, security technology, and other technologies to
enforce social distancing and safe work environments as they re-open for business. A
major debate is now underway in the United States about whether employers should
be shielded from liability for choices they make in re-opening for business. Just as
technology can be used to help workers do their jobs remotely, so too can it be used
to determine whether those same employees are actually working as they shelter in
place. As a result, we are likely to hear greater concerns expressed about mission
creep, of the type that caused the German government to move away from a
centralized to a decentralized approach to data collection.

We end where we began, but with a sense of foreboding. We have long been
proponents of advances in technology for the benefit of consumers. Will they and
governments make the right choice? What indeed is the “right” choice? That day of
reckoning is now upon us.

© Copyright 2021 Squire Patton Boggs (US) LLP

National Law Review, Volume X, Number 164

Source URL: https://www.natlawreview.com/article/privacy-vs-security-post-pandemic-world