United States of America
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580

Office of Commissioner
Christine S. Wilson

May 21, 2021

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington DC 20510

Dear Senator Wyden:

I write to applaud your sponsorship of the Fourth Amendment Is Not For Sale Act ("the Act"), which closes the legal loophole that allows the federal government to purchase commercial data on individuals without a warrant.

Recent press reports indicate that law enforcement and intelligence agencies increasingly choose to circumvent the Fourth Amendment by purchasing data from commercial entities rather than seeking warrants to obtain location information and other consumer records. If enacted, your proposed legislation would take an important first step in protecting the constitutional rights of Americans by outlawing the government purchase of data that otherwise would require a court order.

Your legislation also highlights the important linkage between large-scale collection of consumer data in the commercial arena and the potential for watering down Americans' civil liberties in the legal arena, an issue that I, too, have sought to highlight (see attachments). In the legal arena, the Fourth Amendment protects people from warrantless searches of places or seizures of information and objects in which they have a subjective expectation of privacy that society recognizes as reasonable.[1] An important legal corollary appears in the "third-party doctrine," which provides that people who give information to third parties, like banks, internet service providers, and email servers, have no reasonable expectation of privacy in that information.[2]

In the commercial arena, consumers have grown accustomed to surrendering extensive data through their daily use of phones, computers, digital assistants, and other connected devices – a

---

[1] *Katz v. United States*, 389 U.S. 347, 361 (1967).
[2] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (finding that the Government's use of a pen register was not a search). *See also United States v. Miller*, 425 U.S. 435, 442 (1976) (holding that bank records created no "expectation of privacy"). *But see Carpenter v. United States*, 138 S. Ct. 2206, 2217 (recognizing a narrow limit to the third-party doctrine and holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements captured through" cell-site location information).

phenomenon that raises the question of whether consumers plausibly can maintain a reasonable expectation of privacy with respect to the information they surrender. Because of the linkage created by the *Katz* test, when society loses its expectation of privacy in the commercial arena, our Fourth Amendment rights are eviscerated in the legal arena.

While the Fourth Amendment Is Not For Sale Act is a momentous and important first step in addressing troubling infringements of Americans' civil liberties, I urge you and your fellow Members of Congress to take another important step: pass comprehensive privacy legislation. Consumers currently lack transparency with respect to the types of data collected from them, and how that data is used, shared, and monetized. Only with greater transparency can they make informed decisions about the costs and benefits of using various products and services. And businesses need guidance from Congress on permitted and prohibited practices and accountable data collection and use. The growing patchwork of state and international privacy regimes is raising compliance costs, inhibiting new entry, and undermining the very innovation that makes our tech sector so unique.

Thank you again for introducing the Fourth Amendment is Not For Sale Act. I applaud your leadership on this issue, and am at your disposal to assist in advancing this legislation.

All best wishes,

Christine S. Wilson
Commissioner

Attachments

ATTACHMENTS

OPINION | COMMENTARY

Coronavirus Demands a Privacy Law

Silicon Valley's role in contact tracing and social-distancing enforcement has Americans worried.

By *Christine Wilson*
May 13, 2020 6:58 pm ET

Reopening the economy and returning to "normal life" in the absence of a Covid-19 vaccine may be possible, we are told, with a combination of widespread testing and contact tracing. But these solutions will depend heavily on technology, and Silicon Valley doesn't have the best record when it comes to protecting consumer privacy. Congress must step into the breach with federal privacy legislation establishing guardrails for tech companies' handling of our most personal information.

The Fourth Amendment protects Americans from government overreach, but the "reasonable expectation of privacy" test complicates the relationship between government action and commercial data collection. Georgetown Law professor Paul Ohm has observed that "the dramatic expansion of technologically-fueled corporate surveillance of our private lives automatically expands police surveillance too," given how "the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine."

Across the country, people are being fined and jailed for not following social-distancing guidelines. It's one thing for the cops to break up a backyard barbecue because of a neighbor's

complaint, but if police rely on data collection rather than direct observation to enforce social-distancing rules, their actions may run afoul of the Fourth Amendment. The Supreme Court has reined in warrantless tracking through Global Positioning System devices placed on vehicles and through cellphone data.

Hong Kong, Taiwan, South Korea and Poland have required people infected with or exposed to the novel coronavirus to download smartphone apps so the government can make sure they are following quarantine restrictions. India recently mandated use of a contact tracing app for office workers.

While the U.S. has yet to impose similar mandates, tech companies have begun collecting pandemic-related data. Facebook is joining with universities to distribute a symptom survey to users that will provide "precise data" that "will help governments and public health officials . . . make decisions," CEO Mark Zuckerberg has said. Apple and Google are working together to support opt-in contact-tracing apps from public health authorities.

But a Washington Post poll found that only 40% of respondents were willing and able to use such an app; half of the polled smartphone users don't trust tech companies to protect the anonymity of users who test positive for Covid-19. Moreover, a new Brookings Institution report questions the benefits of contact tracing via apps, which may be less accurate than human tracers and potentially vulnerable to hacking.

ILLUSTRATION: BARBARA KELLEY

The Federal Trade Commission has long used its broad consumer protection authority to safeguard Americans' privacy and data security, but its specific privacy authority is limited. I have called on Congress to pass privacy legislation that would provide more transparency to consumers and greater certainty to businesses about the types of data that can be collected and how those data can be used and shared.

Comprehensive legislation is needed to help companies navigate issues such as accountability, risk management, data minimization, deidentification and vendor management. With established legal boundaries, companies would be better equipped to determine when the government is asking them to cross the line for the public good, and whether they should require a subpoena or inform customers before turning over data.

In the absence of baseline privacy legislation, some coronavirus researchers have justified their use of mobile-device data by citing customers' prior consent to data collection. Last week, five Republican senators led by Roger Wicker of Mississippi introduced a bill that would require tech companies to get "affirmative express consent" before collecting Covid-19 data. Congress will decide whether this is the right approach, but the assumption that consumers have already given informed consent for quarantine-compliance monitoring is unsupportable. Cellphone users often don't read the fine print. They have little understanding of the actual scope of how their data are collected, analyzed and shared.

Covid-19 presents new and complex choices about information collection, dissemination and use. Care is required, because privacy and data-security missteps can cause people irrevocable harm. Companies must be transparent with consumers, assess and manage risk in collecting and using data, and share only those data necessary to achieve stated goals. Similar principles of necessity and proportionality should guide governments when seeking private industry information.

But why take chances? Samuel Johnson wrote, "When a man knows he is to be hanged in a fortnight, it concentrates his mind wonderfully." With the health, privacy and Fourth Amendment rights of Americans at stake, congressional minds should concentrate on turning draft privacy bills into comprehensive legislation, providing guidance and clarity now and in the years to come. Otherwise, with mobile devices acting as "invisible policemen," Justice William O. Douglas's warning of "a bald invasion of privacy, far worse than the general warrants prohibited by the Fourth Amendment," may come to pass.

Ms. Wilson is a commissioner of the Federal Trade Commission.

Wilson says pandemic underscores need to establish privacy rules for 'Big Tech'

Official Statement | 18 May 20 | 20:50 GMT

In Brief

MLex Summary: Christine Wilson, a Republican member of the US Federal Trade Commission said in the full text of a media opinion piece shared with MLex that the Covid-19 pandemic underscores the need for comprehensive federal privacy legislation. "Covid-19 presents new and complex choices about tech companies' collection, dissemination and application of users' data. Rather than take chances on companies' ability to intuit the appropriate course, Congress should provide the guardrails. The health, privacy, and Fourth Amendment rights of Americans are at stake," Wilson wrote.

Text of Wilson op-ed follows in full:

Covid-19 Underscores Need for Comprehensive Privacy Legislation

By Christine Wilson

After years of vilifying pharmaceutical and technology companies, the pandemic-stricken globe now looks to them with hope. The role of Big Pharma is obvious: find treatments, cures and vaccines. The role of Big Tech is less clear – and requires guidance from Congress.

Many view technology, in the form of comprehensive contact tracing, as key to safely reopening our economy and recovering a sense of normality in our social interactions. But the pandemic has not erased concerns about tech companies' handling of consumer privacy. Indeed, it heightens those concerns, as government omnipotence combines with private sector omniscience.

As a Commissioner at the Federal Trade Commission, I am familiar with Big Tech and Big Pharma. I voted to sue Facebook and YouTube for privacy violations, and Martin Shkreli for unlawful conduct that increased drug prices astronomically. While enforcing the competition and consumer protection laws is central to my FTC role, I have also sworn to support and defend the Constitution.

The Fourth Amendment protects American citizens from government overreach, but the “reasonable expectation of privacy” test applied in Fourth Amendment cases links the arenas of government action and commercial data collection. In the commercial arena, consumers have become accustomed to surrendering extensive data through their daily use of phones, computers, digital assistants and other connected devices. This phenomenon has inevitable spillover effects in the legal arena – if citizens know and accept that nothing is private, then they have no reasonable expectation of privacy, and the Fourth Amendment gets eviscerated.

The Supreme Court has limited the warrantless tracking of Americans through GPS devices placed on their cars and through cellphone data voluntarily handed over by mobile network operators. GPS data has proven helpful in fighting the spread of Covid-19; it also could be used to piece together evidence of violations of stay-at-home orders. As Chief Justice John Roberts wrote in Carpenter, “With access to [cell-site location information], the government can now travel back in time to retrace a person’s whereabouts… Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years.”

History has taught us repeatedly that sweeping security powers granted to governments during an emergency persist long after the crisis has abated. Just last week [May 13], the Senate refused to prohibit the federal government from obtaining warrantless access to third-party data collection of Americans’ web browser and search history information. This development further undermines any expectation of privacy that Americans would otherwise have in their data. As Slovak lawmaker Tomas Valasek has said, “It doesn’t just take the despots and the illiberals of this world… to wreak damage.”

Several governments around the world, from Taiwan to Poland, have required people infected with or exposed to the novel coronavirus to download smartphone apps to facilitate enforcement of quarantine restrictions.

State action has not gone entirely unchallenged; Israel’s Supreme Court ruled late last month that the country’s parliament must pass legislation for the internal security service to use individuals’ mobile data for contact tracing. “The state’s choice to use its preventative security service for monitoring those who wish it no harm, without their consent, raises great difficulties and a suitable alternative, compatible with the principles of privacy, must be found,” the court said. “We must take every precaution to ensure that the extraordinary developments with which we are dealing these days do not put us on a slippery slope in which extraordinary and harmful toolsare used without justification.”

The UK government on May 4 introduced the National Health Service’s home-grown contacttracing app to the Isle of Wight. Mobile device users choose whether to install the app and to inform it if they have symptoms or a diagnosis of Covid-19. The NHS COVID-19 app relies on Bluetooth technology to determine if one user has been in close proximity for a certain amount of time with another user who has reported possible or confirmed infection.

The U.S. has not yet taken similar steps in its fight against COVID-19, but tech companies are collecting relevant data. As part of its “Data for Good” initiative, Facebook has partnered with universities to distribute a symptom survey to users, with the company’s knowledge of their demographics used to correct for sample bias. Apple and Google are introducing interoperability between iOS and Android devices to support decentralized contact tracing apps from

public health authorities. But a Washington Post poll found that half of the polled smartphone users do not trust tech companies to protect the anonymity of app users who test positive for Covid-19. Voluntary measures will fail if a critical mass of Americans do not participate – which should incentivize both the public and private sectors to demonstrate their trustworthiness.

The FTC recommended that Congress pass comprehensive federal privacy legislation in its first major report on privacy in 2012. I have echoed this long-standing call – in testimony before the US Senate and House, in public speeches, and in articles. The FTC recently confronted the significant limits to its authority in bringing its enforcement action against Facebook. As the district court noted when entering the consent order, “these concerns are largely for Congress.”

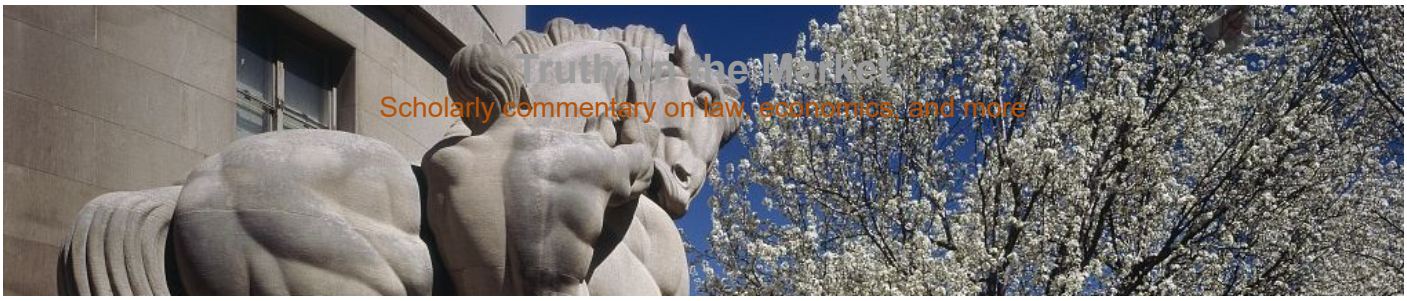
Congress’s failure to pass legislation is mystifying: in a toxic political environment infused with strident partisanship, the need for a comprehensive privacy regime is one issue on which both parties and all stakeholders agree. In recent months, Congressional drafts were released with fanfare. None was perfect, but for too long, on data security and privacy, we have let the perfect be the enemy of the good.

In the absence of comprehensive privacy legislation, coronavirus researchers have justified using mobile device data provided by companies by citing prior customer consent. But the assumption that consumers have given informed consent – particularly for quarantine compliance monitoring during a pandemic – is undermined by studies showing users have little understanding of the actual scope of data collection and deployment. Moreover, click-through consent does not end the conversation about privacy rights. Lengthy fine-print disclosures are insufficient, especially if assent is framed as altruism to aid public health.

To address at least the current pandemic, five Republican senators on May 7 introduced coronavirus-specific privacy legislation. A week later, two Democratic senators offered their own version of such a law. These bills agree on some core issues, including the need to obtain affirmative express consent rather than infer consent from inaction; the obligation to provide an effective way to revoke consent; and enforcement by the FTC under its authority against unfair or deceptive practices and by state attorneys general.

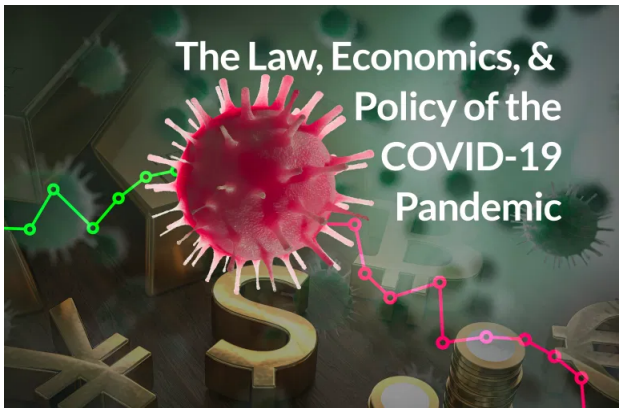
But the proposals diverge on some of the same points that previously held up passage of a baseline privacy law: whether the federal law preempts state law; whether consumers should have a private right of action to obtain damages; and whether this right can be subject to binding arbitration. That these bills are not bipartisan does not inspire confidence in their likelihood of getting passed. In any event, a narrow privacy bill dealing only with the conditions of the pandemic, which we pray will soon pass, is far less preferable than comprehensive legislation that will provide broad guidance for years to come.

Covid-19 presents new and complex choices about tech companies’ collection, dissemination and application of users’ data. Rather than take chances on companies’ ability to intuit the appropriate course, Congress should provide the guardrails. The health, privacy, and Fourth Amendment rights of Americans are at stake.



Privacy in the Time of Covid-19

Christine Wilson — 15 April 2020



[*TOTM: The following is part of a blog series by TOTM guests and authors on the law, economics, and policy of the ongoing COVID-19 pandemic. The entire series of posts is available here.*

This post is authored by Christine S. Wilson (Commissioner of the U.S. Federal Trade Commission).[1] *The views expressed here are the author's and do not necessarily reflect those of the Federal Trade Commission or any other Commissioner.*]

I type these words while subject to a stay-at-home order issued by West Virginia Governor James C. Justice II. "To preserve public health and safety, and to ensure the healthcare system in West Virginia is capable of serving all citizens in need," I am permitted to leave my home only for a limited and precisely enumerated set of reasons. Billions of citizens around the globe are now operating under similar shelter-in-place directives as governments grapple with how to stem the tide of infection, illness and death inflicted by the global Covid-19 pandemic. Indeed, the first response of many governments has been to impose severe limitations on physical movement to contain the spread of the novel coronavirus. The second response contemplated by many, and the one on which this blog post focuses, involves the extensive collection and analysis of data in connection with people's movements and health. Some governments are using that data to conduct sophisticated contact tracing, while others are using the power of the state to enforce orders for quarantines and against gatherings.

The desire to use modern technology on a broad scale for the sake of public safety is not unique to this moment. Technology is intended to improve the quality of our lives, in part by enabling us to help ourselves and one another. For example, cell towers broadcast wireless emergency alerts to all mobile devices in the area to warn us of extreme weather and other threats to safety in our vicinity. One well-known type of broadcast is the Amber Alert, which enables community members to assist in recovering an abducted child by providing descriptions of the abductor, the abductee and the abductor's vehicle. Citizens who spot individuals and vehicles that meet these descriptions can then provide leads to law enforcement authorities. A private nonprofit organization, the National Center for Missing and Exploited Children, coordinates with state and local public safety officials to send out Amber Alerts through privately owned wireless carriers.

The robust civil society and free market in the U.S. make partnerships between the private sector and government agencies commonplace. But some of these arrangements involve a much more extensive sharing of Americans' personal information with law enforcement than the emergency alert system does.

For example, Amazon's home security product Ring advertises itself not only as a way to see when a package has been left at your door, but also as a way to make communities safer by turning over video footage to local police departments. In 2018, the company's pilot program in Newark, New Jersey, donated more than 500 devices to homeowners to install at their homes in two neighborhoods, with a big caveat. Ring recipients were encouraged to share video with police. According to Ring, home burglaries in those neighborhoods fell by more than 50% from April through July 2018 relative to the same time period a year earlier.

Yet members of Congress and privacy experts have raised concerns about these partnerships, which now number in the hundreds. After receiving Amazon's response to his inquiry, Senator Edward Markey highlighted Ring's failure to prevent police from sharing video footage with third parties and from keeping the video permanently, and Ring's lack of precautions to ensure that users collect footage only of adults and of users' own property. The House of Representatives Subcommittee on Economic and Consumer Policy continues to investigate Ring's police partnerships and data policies. The Electronic Frontier Foundation has called Ring "a perfect storm of privacy threats," while the UK surveillance camera commissioner has warned against "a very real power to understand, to surveil you in a way you've never been surveilled before."

Ring demonstrates clearly that it is not new for potential breaches of privacy to be encouraged in the name of public safety; police departments urge citizens to use Ring and share the videos with police to fight crime. But emerging developments indicate that, in the fight against Covid-19, we can expect to see more and more private companies placed in the difficult position of becoming complicit in government overreach.

At least mobile phone users can opt out of receiving Amber Alerts, and residents can refuse to put Ring surveillance systems on their property. The Covid-19 pandemic has made some other technological intrusions effectively impossible to refuse. For example, online proctors who monitor students over webcams to ensure they do not cheat on exams taken at home were once something that students could choose to accept if they did not want to take an exam where and when they could be proctored face to face. With public schools and universities across the U.S. closed for the rest of the semester, students who refuse to give private online proctors access to their webcams – and, consequently, the ability to view their surroundings – cannot take exams at all.

Existing technology and data practices already have made the Federal Trade Commission sensitive to potential consumer privacy and data security abuses. For decades, this independent, bipartisan agency has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices. It brought its first privacy and data security cases nearly 20 years ago, while I was Chief of Staff to then-Chairman Timothy J. Muris. The FTC took on Eli Lilly for disclosing the e-mail addresses of 669 subscribers to its Prozac reminder service – many of whom were government officials, and at a time of greater stigma for mental health issues – and Microsoft for (among other things) falsely claiming that its Passport website sign-in service did not collect any personally identifiable information other than that described in its privacy policy.

The privacy and data security practices of healthcare and software companies are likely to impact billions of people during the current coronavirus pandemic. The U.S. already has many laws on the books that are relevant to practices in these areas. One notable example is the Health Insurance Portability and Accountability Act, which set national standards for the protection of individually identifiable health information by health plans, health care clearinghouses and health care providers who accept non-cash payments. While the FTC does not enforce HIPAA, it does enforce the Health Breach Notification Rule, as well as the provisions in the FTC Act used to challenge the privacy missteps of Eli Lilly and many other companies.

But technological developments have created gaps in HIPAA enforcement. For example, HIPAA applies to doctors' offices, hospitals and insurance companies, but it may not apply to wearables, smartphone apps or websites. Yet

sensitive medical information is now commonly stored in places other than health care practitioners' offices. Your phone and watch now collect information about your blood sugar, exercise habits, fertility and heart health.

Observers have pointed to these emerging gaps in coverage as evidence of the growing need for federal privacy legislation. I, too, have called on the U.S. Congress to enact comprehensive federal privacy legislation – not only to address these emerging gaps, but for two other reasons. First, consumers need clarity regarding the types of data collected from them, and how those data are used and shared. I believe consumers can make informed decisions about which goods and services to patronize when they have the information they need to evaluate the costs and benefits of using those goods. Second, businesses need predictability and certainty regarding the rules of the road, given the emerging patchwork of regimes both at home and abroad.

Rules of the road regarding privacy practices will prove particularly instructive during this global pandemic, as governments lean on the private sector for data on the grounds that the collection and analysis of data can help avert (or at least diminish to some extent) a public health catastrophe. With legal lines in place, companies would be better equipped to determine when they are being asked to cross the line for the public good, and whether they should require a subpoena or inform customers before turning over data. It is regrettable that Congress has been unable to enact federal privacy legislation to guide this discussion.

Understandably, Congress does not have privacy at the top of its agenda at the moment, as the U.S. faces a public health crisis. As I write, more than 579,000 Americans have been diagnosed with Covid-19, and more than 22,000 have perished. Sadly, those numbers will only increase. And the U.S. is not alone in confronting this crisis: governments globally have confronted more than 1.77 million cases and more than 111,000 deaths. For a short time, health and safety issues may take precedence over privacy protections. But some of the initiatives to combat the coronavirus pandemic are worrisome. We are learning more every day about how governments are responding in a rapidly developing situation; what I describe in the next section constitutes merely the tip of the iceberg. These initiatives are worth highlighting here, as are potential safeguards for privacy and civil liberties that societies around the world would be wise to embrace.

Some observers view public/private partnerships based on an extensive use of technology and data as key to fighting the spread of Covid-19. For example, Professor Jane Bambauer calls for contact tracing and alerts "to be done in an automated way with the help of mobile service providers' geolocation data." She argues that privacy is merely "an instrumental right" that "is meant to achieve certain social goals in fairness, safety and autonomy. It is not an end in itself." Given the "more vital" interests in health and the liberty to leave one's house, Bambauer sees "a moral imperative" for the private sector "to ignore even express lack of consent" by an individual to the sharing of information about him.

This proposition troubles me because the extensive data sharing that has been proposed in some countries, and that is already occurring in many others, is not mundane. In the name of advertising and product improvements, private companies have been hoovering up personal data for years. What this pandemic lays bare, though, is that while this trove of information was collected under the guise of cataloguing your coffee preferences and transportation habits, it can be reprocessed in an instant to restrict your movements, impinge on your freedom of association, and silence your freedom of speech. Bambauer is calling for detailed information about an individual's every movement to be shared with the government when, in the United States under normal circumstances, a warrant would be required to access this information.

Indeed, with our mobile devices acting as the "invisible policeman" described by Justice William O. Douglas in *Berger v. New York*, we may face "a bald invasion of privacy, far worse than the general warrants prohibited by the Fourth Amendment." Backward-looking searches and data hoards pose new questions of what constitutes a "reasonable" search. The stakes are high – both here and abroad, citizens are being asked to allow warrantless searches by the government on an astronomical scale, all in the name of public health.

Abroad

The first country to confront the coronavirus was China. The World Health Organization has touted the measures taken by China as "the only measures that are currently proven to interrupt or minimize transmission chains in humans." Among these measures are the "rigorous tracking and quarantine of close contacts," as well as "the use of big data and artificial intelligence (AI) to strengthen contact tracing and the management of priority populations." An ambassador for China has said his government "optimized the protocol of case discovery and management in multiple ways like backtracking the cell phone positioning." Much as the Communist Party's control over China enabled it to suppress early reports of a novel coronavirus, this regime vigorously ensured its people's compliance with the "stark" containment measures described by the World Health Organization.

Before the Covid-19 pandemic, Hong Kong already had been testing the use of "smart wristbands" to track the movements of prisoners. The Special Administrative Region now monitors people quarantined inside their homes by requiring them to wear wristbands that send information to the quarantined individuals' smartphones and alert the Department of Health and Police if people leave their homes, break their wristbands or disconnect them from their smartphones. When first announced in early February, the wristbands were required only for people who had been to Wuhan in the past 14 days, but the program rapidly expanded to encompass every person entering Hong Kong. The government denied any privacy concerns about the electronic wristbands, saying the Privacy Commissioner for Personal Data had been consulted about the technology and agreed it could be used to ensure that quarantined individuals remain at home.

Elsewhere in Asia, Taiwan's Chunghwa Telecom has developed a system that the local CDC calls an "electronic fence." Specifically, the government obtains the SIM card identifiers for the mobile devices of quarantined individuals and passes those identifiers to mobile network operators, which use phone signals to their cell towers to alert public health and law enforcement agencies when the phone of a quarantined individual leaves a certain geographic range. In response to privacy concerns, the National Communications Commission said the system was authorized by special laws to prevent the coronavirus, and that it "does not violate personal data or privacy protection." In Singapore, travelers and others issued Stay-Home Notices to remain in their residency 24 hours a day for 14 days must respond within an hour if contacted by government agencies by phone, text message or WhatsApp. And to assist with contact tracing, the government has encouraged everyone in the country to download TraceTogether, an app that uses Bluetooth to identify other nearby phones with the app and tracks when phones are in close proximity.

Israel's Ministry of Health has launched an app for mobile devices called HaMagen (the shield) to prevent the spread of coronavirus by identifying contacts between diagnosed patients and people who came into contact with them in the 14 days prior to diagnosis. In March, the prime minister's cabinet initially bypassed the legislative body to approve emergency regulations for obtaining without a warrant the cellphone location data and additional personal information of those diagnosed with or suspected of coronavirus infection. The government will send text messages to people who came into contact with potentially infected individuals, and will monitor the potentially infected person's compliance with quarantine. The Ministry of Health will not hold this information; instead, it can make data requests to the police and Shin Bet, the Israel Security Agency. The police will enforce quarantine measures and Shin Bet will track down those who came into contact with the potentially infected.

Multiple Eastern European nations with constitutional protections for citizens' rights of movement and privacy have superseded them by declaring a state of emergency. For example, in Hungary the declaration of a "state of danger" has enabled Prime Minister Viktor Orbán's government to engage in "extraordinary emergency measures" without parliamentary consent. His ministers have cited the possibility that coronavirus will prevent a gathering of a sufficient quorum of members of Parliament as making it necessary for the government to be able to act in the absence of legislative approval.

Member States of the European Union must protect personal data pursuant to the General Data Protection Regulation, and communications data, such as mobile location, pursuant to the ePrivacy Directive. The chair of the European Data Protection Board has observed that the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security. But if those measures allow for the processing of non-anonymized location data from mobile devices, individuals must have safeguards such as a right to a judicial

remedy. “Invasive measures, such as the ‘tracking’ of individuals (i.e. processing of historical non-anonymized location data) could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing.” The EDPB has announced it will prioritize guidance on these issues.

EU Member States are already implementing such public security measures. For example, the government of Poland has by statute required everyone under a quarantine order due to suspected infection to download the “Home Quarantine” smartphone app. Those who do not install and use the app are subject to a fine. The app verifies users’ compliance with quarantine through selfies and GPS data. Users’ personal data will be administered by the Minister of Digitization, who has appointed a data protection officer. Each user’s identification, name, telephone number, quarantine location and quarantine end date can be shared with police and other government agencies. After two weeks, if the user does not report symptoms of Covid-19, the account will be deactivated — but the data will be stored for six years. The Ministry of Digitization claims that it must store the data for six years in case users pursue claims against the government. However, local privacy expert and Panoptykon Foundation cofounder Katarzyna Szymielewicz has questioned this rationale.

Even other countries that are part of the Anglo-American legal tradition are ramping up their use of data and working with the private sector to do so. The UK’s National Health Service is developing a data store that will include online/call center data from NHS Digital and Covid-19 test result data from the public health agency. While the NHS is working with private partner organizations and companies including Microsoft, Palantir Technologies, Amazon Web Services and Google, it has promised to keep all the data under its control, and to require those partners to destroy or return the data “once the public health emergency situation has ended.” The NHS also has committed to meet the requirements of data protection legislation by ensuring that individuals cannot be re-identified from the data in the data store.

Notably, each of the companies partnering with the NHS at one time or another has been subjected to scrutiny for its privacy practices. Some observers have noted that tech companies, which have been roundly criticized for a variety of reasons in recent years, may seek to use this pandemic for “reputation laundering.” As one observer cautioned: “Reputations matter, and there’s no reason the government or citizens should cast bad reputations aside when choosing who to work with or what to share” during this public health crisis.

At home

In the U.S., the federal government last enforced large-scale isolation and quarantine measures during the influenza (“Spanish Flu”) pandemic a century ago. But the Centers for Disease Control and Prevention track diseases on a daily basis by receiving case notifications from every state. The states mandate that healthcare providers and laboratories report certain diseases to the local public health authorities using personal identifiers. In other words, if you test positive for coronavirus, the government will know. Every state has laws authorizing quarantine and isolation, usually through the state’s health authority, while the CDC has authority through the federal Public Health Service Act and a series of presidential executive orders to exercise quarantine and isolation powers for specific diseases, including severe acute respiratory syndromes (a category into which the novel coronavirus falls).

Now local governments are issuing orders that empower law enforcement to fine and jail Americans for failing to practice social distancing. State and local governments have begun arresting and charging people who violate orders against congregating in groups. Rhode Island is requiring every non-resident who enters the state to be quarantined for two weeks, with police checks at the state’s transportation hubs and borders.

How governments discover violations of quarantine and social distancing orders will raise privacy concerns. Police have long been able to enforce based on direct observation of violations. But if law enforcement authorities identify violations of such orders based on data collection rather than direct observation, the Fourth Amendment may be implicated. In *Jones* and *Carpenter*, the Supreme Court has limited the warrantless tracking of Americans through GPS devices placed on their cars and through cellphone data. But building on the longstanding practice of contact tracing in fighting infectious diseases such as tuberculosis, GPS data has proven helpful in fighting the spread of

Covid-19. This same data, though, also could be used to piece together evidence of violations of stay-at-home orders. As Chief Justice John Roberts wrote in *Carpenter*, "With access to [cell-site location information], the government can now travel back in time to retrace a person's whereabouts… Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years."

The Fourth Amendment protects American citizens from government action, but the "reasonable expectation of privacy" test applied in Fourth Amendment cases connects the arenas of government action and commercial data collection. As Professor Paul Ohm of the Georgetown University Law Center notes, "the dramatic expansion of technologically-fueled corporate surveillance of our private lives automatically expands police surveillance too, thanks to the way the Supreme Court has construed the reasonable expectation of privacy test and the third-party doctrine."

For example, the COVID-19 Mobility Data Network – infectious disease epidemiologists working with Facebook, Camber Systems and Cubiq – uses mobile device data to inform state and local governments about whether social distancing orders are effective. The tech companies give the researchers aggregated data sets; the researchers give daily situation reports to departments of health, but say they do not share the underlying data sets with governments. The researchers have justified this model based on users of the private companies' apps having consented to the collection and sharing of data.

However, the assumption that consumers have given informed consent to the collection of their data (particularly for the purpose of monitoring their compliance with social isolation measures during a pandemic) is undermined by studies showing the average consumer does not understand all the different types of data that are collected and how their information is analyzed and shared with third parties – including governments. Technology and telecommunications companies have neither asked me to opt into tracking for public health nor made clear how they are partnering with federal, state and local governments. This practice highlights that data will be divulged in ways consumers cannot imagine – because no one assumed a pandemic when agreeing to a company's privacy policy. This information asymmetry is part of why we need federal privacy legislation.

On Friday afternoon, Apple and Google announced their opt-in Covid-19 contact tracing technology. The owners of the two most common mobile phone operating systems in the U.S. said that in May they would release application programming interfaces that enable interoperability between iOS and Android devices using official contact tracing apps from public health authorities. At an unspecified date, Bluetooth-based contact tracing will be built directly into the operating systems. "Privacy, transparency, and consent are of utmost importance in this effort," the companies said in their press release.

At this early stage, we do not yet know exactly how the proposed Google/Apple contact tracing system will operate. It sounds similar to Singapore's TraceTogether, which is already available in the iOS and Android mobile app stores (it has a 3.3 out of 5 average rating in the former and a 4.0 out of 5 in the latter). TraceTogether is also described as a voluntary, Bluetooth-based system that avoids GPS location data, does not upload information without the user's consent, and uses changing, encrypted identifiers to maintain user anonymity. Perhaps the most striking difference, at least to a non-technical observer, is that TraceTogether was developed and is run by the Singaporean government, which has been a point of concern for some observers. The U.S. version – like finding abducted children through Amber Alerts and fighting crime via Amazon Ring – will be a partnership between the public and private sectors.

Recommendations

The global pandemic we now face is driving data usage in ways not contemplated by consumers. Entities in the private and public sector are confronting new and complex choices about data collection, usage and sharing. Organizations with Chief Privacy Officers, Chief Information Security Officers, and other personnel tasked with managing privacy programs are, relatively speaking, well-equipped to address these issues. Despite the extraordinary circumstances, senior management should continue to rely on the expertise and sound counsel of their CPOs and CISOs, who should continue to make decisions based on their established privacy and data

security programs. Although developments are unfolding at warp speed, it is important – arguably now, more than ever – to be intentional about privacy decisions.

For organizations that lack experience with privacy and data security programs (and individuals tasked with oversight for these areas), now is a great time to pause, do some research and exercise care. It is essential to think about the longer-term ramifications of choices made about data collection, use and sharing during the pandemic. The FTC offers easily accessible resources, including Protecting Personal Information: A Guide for Business, Start with Security: A Guide for Business, and Stick with Security: A Business Blog Series. While the Gramm-Leach-Bliley Act (GLB) applies only to financial institutions, the FTC's GLB compliance blog outlines some data security best practices that apply more broadly. The National Institute for Standards and Technology (NIST) also offers security and privacy resources, including a privacy framework to help organizations identify and manage privacy risks. Private organizations such as the Center for Information Policy Leadership, the International Association of Privacy Professionals and the App Association also offer helpful resources, as do trade associations. While it may seem like a suboptimal time to take a step back and focus on these strategic issues, remember that privacy and data security missteps can cause irrevocable harm. Counterintuitively, now is actually the *best* time to be intentional about choices in these areas.

Best practices like accountability, risk assessment and risk management will be key to navigating today's challenges. Companies should take the time to assess and document the new and/or expanded risks from the data collection, use and sharing of personal information. It is appropriate for these risk assessments to incorporate potential benefits and harms not only to the individual and the company, but for society as a whole. Upfront assessments can help companies establish controls and incentives to facilitate responsible behavior, as well as help organizations demonstrate that they are fully aware of the impact of their choices (risk assessment) and in control of their impact on people and programs (risk mitigation). Written assessments can also facilitate transparency with stakeholders, raise awareness internally about policy choices and assist companies with ongoing monitoring and enforcement. Moreover, these assessments will facilitate a return to "normal" data practices when the crisis has passed.

In a similar vein, companies must engage in comprehensive vendor management with respect to the entities that are proposing to use and analyze their data. In addition to vetting proposed data recipients thoroughly, companies must be selective concerning the categories of information shared. The benefits of the proposed research must be balanced against individual protections, and companies should share only those data necessary to achieve the stated goals. To the extent feasible, data should be shared in de-identified and aggregated formats and data recipients should be subject to contractual obligations prohibiting them from re-identification. Moreover, companies must have policies in place to ensure compliance with research contracts, including data deletion obligations and prohibitions on data re-identification, where appropriate. Finally, companies must implement mechanisms to monitor third party compliance with contractual obligations.

Similar principles of necessity and proportionality should guide governments as they make demands or requests for information from the private sector. Governments must recognize the weight with which they speak during this crisis and carefully balance data collection and usage with civil liberties. In addition, governments also have special obligations to ensure that any data collection done by them or at their behest is driven by the science of Covid-19; to be transparent with citizens about the use of data; and to provide due process for those who wish to challenge limitations on their rights. Finally, government actors should apply good data hygiene, including regularly reassessing the breadth of their data collection initiatives and incorporating data retention and deletion policies.

In theory, government's role could be reduced as market-driven responses emerge. For example, assuming the existence of universally accessible daily coronavirus testing with accurate results even during the incubation period, Hal Singer's proposal for self-certification of non-infection among private actors is intriguing. Thom Lambert identified the inability to know who is infected as a "lemon problem;" Singer seeks a way for strangers to verify each other's "quality" in the form of non-infection.

Whatever solutions we may accept in a pandemic, it is imperative to monitor the coronavirus situation as it improves, to know when to lift the more dire measures. Former Food and Drug Administration Commissioner Scott Gottlieb and other observers have called for maintaining surveillance because of concerns about a resurgence of the virus later this year. For any measures that conflict with Americans' constitutional rights to privacy and freedom of movement, there should be metrics set in advance for the conditions that will indicate when such measures are no longer justified. In the absence of pre-determined metrics, governments may feel the same temptation as Hungary's prime minister to keep renewing a "state of danger" that overrides citizens' rights. As Slovak lawmaker Tomas Valasek has said, "It doesn't just take the despots and the illiberals of this world, like Orbán, to wreak damage." But privacy is not merely instrumental to other interests, and we do not have to sacrifice our right to it indefinitely in exchange for safety.

I recognize that halting the spread of the virus will require extensive and sustained effort, and I credit many governments with good intentions in attempting to save the lives of their citizens. But I refuse to accept that we must sacrifice privacy to reopen the economy. It seems a false choice to say that I must sacrifice my Constitutional rights to privacy, freedom of association and free exercise of religion for another's freedom of movement. Society should demand that equity, fairness and autonomy be respected in data uses, even in a pandemic. To quote Valasek again: "We need to make sure that we don't go a single inch further than absolutely necessary in curtailing civil liberties in the name of fighting for public health." History has taught us repeatedly that sweeping security powers granted to governments during an emergency persist long after the crisis has abated. To resist the gathering momentum toward this outcome, I will continue to emphasize the FTC's learning on appropriate data collection and use. But my remit as an FTC Commissioner is even broader – when I was sworn in on Sept. 26, 2018, I took an oath to "support and defend the Constitution of the United States" – and so I shall.

---

[1] Many thanks to my Attorney Advisors Pallavi Guniganti and Nina Frant for their invaluable assistance in preparing this article.

In consumer protection, COVID-19-Response-Series, ftc, privacy, truth on the market big data, coronavirus, COVID, covid-19, data collection, Data Protection Regulation, Fourth Amendment, GDPR, privacy, privacy regulation

Previous Next