May 2022

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

JENNIFER BROOKES, JAMES BONOMO, TIMOTHY M. BONDS

America's 5G Era

Balancing Big Data and Privacy

Fifth-generation (5G) wireless networking will increase the scale of wireless networks by an order of magnitude or more.[1] Perhaps nothing exemplifies the future of the 5G era more than the ubiquitous surveillance that is gathering more and more-diverse data on people. Even before the 5G era, data were seen as a source of new economic value. At the same time, the gathering and use of data have already raised privacy concerns, both in the United States and in Europe (Gopalakrishnan, 2020; Singer and Conger, 2019).

KEY FINDINGS

- As the volume, variety, and velocity of data gathered increase dramatically, both the value and the risk are likely to increase as well.
- In the fifth-generation (5G) wireless era, a government could expand and automate its surveillance for infectious-disease monitoring and translate that surveillance into controls of day-to-day activity.
- In the 5G era, law enforcement has more information than ever before, which it can fuse together a lot more quickly.
- The 5G era, with increased bandwidth for more-connected devices, will likely continue the trend of the collection and utilization of personal data by firms, both large and small, and could contribute to a ubiquitous mobile surveillance environment.

RAND CORPORATION

Although concerns about big data are not new, the connection between growth of the opportunities and risks associated with big data, personal privacy, and the coming 5G era are often an overlooked piece of the 5G conversation. As the volume, variety, and velocity of data gathered increase dramatically, both the value and the risk are likely to increase as well. Our focus in this report is on the implications of 5G hardware, and we assume that artificial intelligence (AI) algorithms and processing capacity will evolve to exploit the new data sources.

The challenge to U.S. policymakers and their constituents is striking a balance between the potential gains of the 5G era and the potential loss of privacy and of control over personal data. Here, we first outline current and potential problems, then discuss a general approach for balancing disparate risks and rewards, including some alternative models for the ownership and control of the data someone generates. Finally, we illustrate an alternative model through the context of countering the coronavirus disease 2019 (COVID-19) pandemic.

Abbreviations

5G	fifth generation
AI	artificial intelligence
COVID-19	coronavirus disease 2019
D2D	device to device
EU	European Union
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
RFID	radio-frequency identification
ToS	term of service
UK	United Kingdom

4G-Era Reality and 5G-Era Potential: Two Use Cases

Today, much is inferred about people using information from the devices they choose to carry, from mobile phones to fitness trackers. The 5G era—with much more reliance on machine analyses—will move from inferences to direct measurements, gathered independently of any overt choice by the user. It might be illustrative to explore the implications of these changes through the use of notional case studies. We are not advocating for these use cases but use them as a thought experiment to determine how 5G systems might affect people in the future.

Containing COVID-19 in China

Consider the case of Chinese surveillance applied to COVID-19 tracking. In 2020, people under quarantine were required to remain in their homes until they received permission to leave. If they left early or congregated outside their homes, human teams monitoring public surveillance cameras would order them to disperse or return home, via public address systems or by dispatching police (Cadell, 2020; Y. Yang et al., 2020). To access public transportation or buildings, every traveler is required to show other people their COVID code (red,

As the volume, variety, and velocity of data gathered increase dramatically, both the value and the risk are likely to increase as well.

yellow, or green) on their smartphone (Mozur, Zhong, and Krolik, 2021). In the 4G era, the smartphone provides only the COVID code.

In the 5G era, China could expand and automate its surveillance (Zhong, 2020) and translate that surveillance into controls of day-to-day activity. Cameras facing a home's doorway would communicate, to an automated control center, the face and gait of anyone leaving home (Gan, 2020). AI algorithms could identify the person leaving and check their COVID code with radio-frequency identification (RFID) devices in the doorframe. If the code were red, the center would call or text the subject's phone with an order to return home, and elevators, building doors, and public transportation would not allow the subject to pass. If the person remained outside, loudspeakers in the vicinity could announce the person's noncompliance, and law-enforcement officials would be dispatched to detain the person or return them home.

If a subject's code were green, they would be allowed access to building doors, elevators, and public transportation as usual. As the subject used or passed within a few meters of these and other portals—and each streetlight, parking meter, vehicle, or regularly spaced sensor unit—their smartphone would announce their presence and status to be checked with that of other people passing within 2 m. AI agents performing this check would confirm that the person holding the smartphone was the same person who left home and would automatically adjust their code downward to the lowest status of anyone with whom they were judged to have come into transmissible contact (i.e., if they came into transmissible contact with someone of yellow status but no one of red status, they would drop to yellow status; if they came into such contact with anyone of red status, they would drop to red status). If their status dropped to red, they would receive a call or text ordering them home—with the same compliance mechanisms described above.

Public Doxing by Anonymous Accusers

Imagine taking a bicycle ride in Gainesville, Florida, or Bethesda, Maryland, or any other city or town or along any country lane in the United States today. Just you and your smartphone and maybe a wearable device with a fitness app. A man on your route is seen

In the 5G era, local law enforcement has more information, which it can fuse together a lot more quickly.

behaving badly and maybe even criminally—perhaps he assaults someone or breaks into a house. A passerby takes pictures of the culprit and sends them to local law enforcement—which then tweets it out to 55,000 followers with a request to identify the suspect in the picture. Some of these 55,000 crowdsourcing people think they have identified the person—or perhaps several different people—because of the picture or from location information publicly shared by a fitness app. With perhaps a bit of time and social media savvy, they come up with the name, cell number, and address of one or more men who seem to match the time, date, and description of the culprit. In a process commonly known as *doxing*, the social media armchair detectives retweet the information to all 55,000—who then send thousands of threatening tweets, texts, and other social media messages (all effectively anonymous) to the supposed suspects. The problem is that they got the wrong people—but subsequent retractions from authorities do not have nearly the reach of the initial accusation. In fact, this very situation has already happened using 4G technologies (see Nuzzi, 2020, and Schuppe, 2020).

In the 5G era, local law enforcement has more information, which it can fuse together a lot more quickly. Cameras on traffic signals, streetlights, public buildings, private residences, vehicles, and wearable devices have all taken pictures. AI continuously monitors those owned by public agencies and willing private entities and those automatically scraped from social media. Advanced facial and gait recognition, cross-checked with fitness-app tracks and maybe RFID hits and accelerated by increased edge computing, has already been used to generate alerts and dispatch police ("Utah Police Look to Artificial Intelligence for Assistance," 2020). In the future, this man could probably be intercepted before he even pedals home. If needed, law-enforcement AI could ask or subpoena individuals for helpful images or hits from their Ring doorbell cameras, Bluetooth apps, RFID systems, or Wi-Fi. Of course, some perhaps well-meaning people (or less well-meaning vigilantes) might also be able to access some of the same data and systems and pursue on their own anyone who is under suspicion.

Real or Notional Issues?

The 4G-era cases mentioned above have already happened; the notional 5G cases are based on capabilities under development but not yet widely deployed. Surveillance has been possible under all previous iterations of cellular networking. Indeed, the electronic collection of

data on people's activities did not begin with the adoption of cellular phones. Electronic tracking actually began with the advent of the personal computer, and tracking of online activities began in earnest with the development of the ad-supported internet model.

Each member of society generates valuable data that they trade for otherwise-free services, such as use of an application or hardware. Often, the collection of data also serves a different purpose for the individual user. People use fitness trackers to optimize their physical training and smart thermostats to optimize efficiency. At the same time, tech firms, such as Alphabet (owner of Google) and Meta (owner of Facebook), harvest, interpret, and traffic personal data. The monetary value of the data concentrated by the app developer that accesses and aggregates the data has been deemed "more valuable than oil" ("The World's Most Valuable Resource Is No Longer Oil," 2017). The 5G era, with increased bandwidth for more-connected devices, will likely continue the trend of the collection and utilization of personal data by firms, both large and small, and could contribute to a ubiquitous mobile surveillance environment.

Such commercially driven surveillance can erode individual control because these corporations are answerable to individuals only when it comes to specific types of information collected by covered entities under current laws in the United States, although protection of individual privacy is more broadly regulated in the European Union (EU) and, for Californians, under state law.[2] Although this information seems relatively harmless when it targets people with demographically relevant ads, the technology is being used in more ways and becoming more personal. In 2018, Amazon patented technology to identify coughs, presumably to sell cold medicines and soup, but this same technology could be repurposed to identify personal illnesses for beneficial or detrimental purposes (Jin and Wang, 2018). Beneficially, audio diagnostics could be useful in clinical settings in diagnosing specific illnesses, such as pertussis (Pramono, Imtiaz, and Rodriguez-Villegas, 2016). However, it is not a stretch to imagine similar diagnostics being used by companies or individuals who would not normally be allowed access to others' health information. Although Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191) regulations cover health providers and insurers, they do not cover nonmedical biometric data, even if one can use them to infer health information about an individual.

Overt data use is not confined to economic activities. Law-enforcement agencies have used some commercial data, including data collected through home video doorbells, in investigations (Harwell, 2019). Law-enforcement agencies in Utah have partnered with an AI company to monitor data streams from traffic cameras, closed-circuit television and public-safety cameras, 911 emergency systems, location data for state-owned vehicles, and social media posts to alert police to suspicious activity (Koebler, Maiberg, and Cox, 2020). As already mentioned, some law-enforcement authorities in the United States have begun to use fitness-tracking apps to identify people who might have been at crime scenes (Schuppe, 2020). The expansion of data collection in

The same data and analytic methods that produce virtuous outcomes can produce problematic outcomes as well.

daily life has coincided with an increased reliance on big data analytics for decisionmaking.

The data industry has become embedded in the basic societal structure in the United States, how people in the United States interact on social media, the news they see, and how governments recognize people. The 5G era will expand this further in two fundamental ways:

- It will incorporate the wide variety of Internet of Things sensors that will, in many cases, monitor people as a matter of course, including the devices someone might wear or carry.
- It will require and so spur the development of AI systems in order to interpret and make use of the flood of data in the data economy.

As people have adopted more-connected devices, the sheer amount of data collected will continue to increase. People in the United States have already expressed concern about their privacy. In a 2019 Pew Research Center study, 79 percent of adults were very or somewhat concerned about how the data that companies collected were used (Auxier et al., 2019). Although we cannot predict which applications will be most prevalent in the 5G era (e.g., surveillance, disease-tracking, autonomous driving, or other human-substituting intelligent agents), the changes 5G will usher in are likely to change society drastically, much as previous generations of technological innovation have. Although this change might be gradual, the final, overall technological change is likely to be drastic simply because the amount of data will be significantly larger.

Ubiquitous Surveillance

Even under 4G, there are *potential* benefits from the ubiquitous monitoring and interpretation of the coming flood of data. Indeed, some of these benefits, such as new diagnostics and contact tracing through widespread data collection, are being applied to the COVID-19 pandemic (O'Neill, Ryan-Mosley, and Johnson, 2020). An app developed by researchers in the United States and United Kingdom (UK) identified loss of taste and smell as key COVID-19 symptoms through self-identified symptoms of users in the UK (Menni et al., 2020).

But this is not an unalloyed benefit. The same data and analytic methods that produce virtuous outcomes can produce problematic outcomes as well. Already, in

China, the combination of proliferated cameras in public places, near–real-time facial recognition, and required apps on cell phones has created an ability to monitor much of the population (Mitchell and Diamond, 2018). In a report released in December 2019, researchers estimated that the number of cameras used in surveillance would increase to more than a billion in 2021, with China accounting for half of the total (Lin and Purnell, 2019). The Chinese government has used this technology extensively to track the Uighur population in Xinjiang, where the government uses proliferated sensors and information streams, along with a mandatory app, to track each person at an individual level. Although this type of technology is generally associated with authoritarian governments, democratic governments have also utilized mass surveillance and data collection to track people, both through systems those governments have developed and by utilizing the data collected by other means. The UK had already utilized automatic license-plate recognition to track and flag vehicle registration, insurance, and crime involvement, and similar technology has been used with drones to track out-of-area vehicles during the COVID-19 lockdown (Dearden, 2020).

The widespread collection and interpretation of data can also have other detrimental effects, even absent any state utilization. The 2010s were full of stories of major data breaches by malicious actors. Some, such as the hack of Office of Personnel and Management data in 2015, were the result of state-sponsored efforts; others, such as the hack of Target data in 2013, were large-scale criminal operations aimed at credit card theft (J. Yang and Jayakumar, 2014; Nakashima, 2015). Regardless of the actor, once data are lost, the people exposed become vulnerable, and once the data have been compromised, the information is "out there" on the internet, essentially impossible to remove.

Data breaches are not simply a one-way street either. Once the data have been compromised, exposure is not the only risk; there can be broader uses—against, for example, society by compromising the democratic process. The intruder might alter the data, which was a key concern with the Russian hacking of voter rolls during the 2016 election (Robles, 2019). The irreversibility of data breaches and the ways in which data can be misused will continue to motivate broad concerns about data gathering, security, and controls.

In some industries, laws have placed the liability for data theft on the data owner; such is the case with credit cards. If your credit card information is stolen and used, the credit card company is liable for the loss. For this reason, credit card companies track account usage closely in order to block fraudulent transactions, even while they also use this information to sell more services. In other industries that use personally identifiable information, there is not always the same type of preventive effort. When personally identifiable information is compromised, companies often simply provide customers with credit-monitoring services for a limited period of time. Credit-monitoring services have also been hacked but have simply put the onus on the individual subject of the data to watch for and identify fraudulent activity on their credit reports for flagging and removal.

How data-collecting industries should be incentivized to properly safeguard against data theft and misuse represents one of the most-important sets of policies that should be established in the 5G era. As more connected devices enter homes and workplaces, cybersecurity and the safeguarding of the data collected will become increasingly urgent. As we discuss in the next section, "Principles to Guide Responses," the EU has mandated some data protections as a condition for companies to operate there.

Often, some effort is made to anonymize data in order to protect privacy and prevent malicious use, but this has proved to be of limited benefit. For example, efforts have been made to decouple data from the device on which they were collected and the device owner's contact information. However, in aggregate, this information can become deanonymized. Individual people can be identified with only location data over time, as demonstrated by the *New York Times* when it purchased location data and was able to trace a senior U.S. Department of Defense official to the Women's March (Thompson and Warzel, 2019). In essence, anyone, including high-ranking officials, influential businesspeople, or politicians, can be identified by their pattern of life in anonymized location data. That information can then be used by any entity or person who is willing to buy or hack the data.

Moreover, sometimes, even anonymous data can be damaging. Location information collected and made public by the fitness-tracking app Strava might have compromised sensitive U.S. military operations when it published a heat map of users' activities even without releasing the users' identities (Sly, 2018). The initial reaction from the company was to warn users to make sure they understood the privacy settings in the app, shifting the burden of understanding the potential uses of the data from the company to each individual user.

The use of data and modeling also has the potential to change people's behavior in real time. Some undesired outcomes from earlier cellular generations might give insights into potential effects of the 5G era. For example, Google Maps and Waze have measurably changed traffic patterns all over the world by showing where traffic is and where it is not (Littman, 2019). These apps change human behavior but are relatively easy to trick (Barrett, 2020). Unfortunately, reliance on rapid interpretation can lead to more-consequential outcomes than a longer commute or much busier residential side streets (Macfarlane, 2019). The 2010 flash crash was driven in part by high-frequency trading algorithms (Gara, 2015). In 2019, the hacking of smart cameras allowed malicious actors to look inside private homes and broadcast to children (Brown, 2019). Data collected by wellness devices can be used to determine whether someone has a health condition, but the data are not generally protected under HIPAA (Pub. L. 104-191, 1996), in part because the data are collected for personal use and not linked to a HIPAA-covered entity, such as a provider of insurance coverage or medical care (Federal Trade Commission [FTC], 2016).

A different problem can arise through the AI engines using the approaching flood of data. The poten-

Who is responsible if the government uses an opaque algorithm to make decisions that affect people's rights, such as equal protection under the law? The application of advanced AI to analyze and interpret data streams will only increase the potential for unintended, biased, or even malicious uses of data, which will often be opaque to the affected parties.

tial use of opaque algorithmic decisions that affect individuals, such as health care, insurance rates, and hiring and firing decisions, all raise questions of equity and democratic control. In 2018, a study reported in *Science Advances* showed that a model that several states used in sentencing proceedings to calculate recidivism rates was no more accurate than decisions by people with no criminal justice background (Dressel and Farid, 2018). Worse, although the algorithm did not use race as a criterion, other factors that were correlated with race were used, leading to racial bias in sentencing. This raises a question: Who is responsible if the government uses an opaque algorithm to make decisions that affect people's rights, such as equal protection under the law? The application of advanced AI to analyze and interpret data streams will only increase the potential for unintended, biased, or even malicious uses of data, which will often be opaque to the affected parties.

Many of the technologies used now and many more projected for the 5G era rely on device-to-device (D2D) communication (Cisco, 2020). The uses for these D2D communications are vast. For many years, there has been a push for vehicle-to-vehicle, vehicle-to-infrastructure, and any number of other vehicle-to-something communications. If road vehicles can talk to each other, they can minimize their energy use, as well as overall congestion, based on road conditions and traffic flow. Surveillance from other D2D communications will also permeate into all rooms of U.S. homes. Wearable devices, such as smart watches and fitness trackers, are already common, as are smart assistants, such as Alexa. In the 5G era, these devices will increasingly

talk to each other and to additional smart devices in the home. Today, the user must connect devices though Wi-Fi; in the 5G future, smart devices will automatically connect directly to the 5G network without a guarantee of an off switch. They already listen to conversations—even when users have not asked them to or acted to turn them on—again raising privacy concerns (Haselton, 2019).

The ability to analyze someone's intimate pattern of life based on their connected devices already exists, but it is unclear whether the firms gathering the information currently have the capacity to analyze and make full use of all of the existing data. In the current legal and policy structure, a company may repurpose all of the data collected in one's home, and one's continued use of the device implies consent to the terms of service (ToS), including that repurposing. This is an essential part of the current economics of app development: A free app is not free to produce and support—apps are free because the maker can monetize the data that the app collects. And, of course, discontinuing use of a device or app does nothing to get the already-collected data back. The changes that the 5G era creates are the volume and nature of the data to be collected and exploited. Each new type of Internet of Things sensor with increased bandwidth and interconnectivity will create new dimensions to the information collected.

The question is whether this onrushing technology is akin to a force of nature that societies must simply endure the best they can or whether it is something societies can and should channel and control. We found that some clear choices are available, even when a society is under a pervasive, unfamiliar threat like they are today with the COVID-19 pandemic. A country can explicitly decide on the limits of data collection, the rules for holding and analyzing data, and the potential uses for the results of those analyses.

Principles to Guide Responses

In recent history, the ethos of the technology industry, as made famous by Facebook, has been to "move fast and break things." Companies have moved forward with minimally viable products, introduced new features, and allowed accidents to happen while seeking forgiveness later. An example of this ethos is the history of adjustments to Facebook's functionality and privacy policies (Romm, 2019).

With the increasing volume of personal information available for exploitation by a large number of more-diverse organizations, it is important that communities and governments make decisions now about the trade-offs they are willing to accept—between the potential benefits and the risks associated with widespread mobile surveillance—ideally before the information is collected because, once out there, data cannot be taken back. To date, most privacy regulations in the United States have been applied to specific types of data in certain contexts. For example, HIPAA created rules and regulations for insurance and service providers governing the protection of health information, while the Privacy Act of 1974 (Pub. L. 93-579) prohibited transmission of

We propose a basic principle: that the beneficial uses be identified, well defined, and agreed upon *before* data are collected or new analysis is conducted.

personal information between federal agencies without the person's permission. So far, there have been no broad federal-level decisions on what privacy protections consumers should have, aside from a few specific data types, such as credit, financial, and health information, and often these laws cover only specific entities, with the same data collected by other entities or means not covered.

In light of the forthcoming 5G era and, with it, the increased collection of data covering all aspects of people's lives, we propose a more structured approach. Specifically, we propose a basic principle: that the beneficial uses be identified, well defined, and agreed upon *before* data are collected or new analysis is conducted. This principle also allows—and, in fact, demands—that the related ethical questions be broadly discussed in some structured manner before a system is implemented.

For new applications and exploratory research, some initial simultaneity of data protections and collection might be possible. The COVID-19 contact-tracing algorithms we discuss in this report are a particularly salient case. Other important examples include other medical and law-enforcement research. Google is now mining millions of patient records with the goal of improving patient care and is developing an AI-based system to improve cancer diagnoses (Abbott, 2020). And, as previously mentioned, AI companies have prototyped systems to generate alerts for law-enforcement agencies ("Utah Police Look to Artificial Intelligence for Assistance," 2020). The current status quo favors very little in terms of safeguards of exploratory research with personal data, but such applications should be testable with limited data sets, carefully established safeguards to protect privacy, and appropriate human supervision of algorithm operations and uses. Most importantly, these limits and applications should then be reevaluated once their benefits and risks become better understood, in order to perhaps ease the limitations or add further restrictions. We see this as a framing of the questions of costs, risks, and benefits of the use of data, so we must immediately confront the two very different sorts of judgments: the ethical ones that determine which costs, risks, and benefits are relevant and the scientific ones for estimating the chosen factors (Fischhoff, 2015).

Although typically much attention is focused on scientific or technical analyses for 5G, the ethical issues

This approach with a diverse public can be possible only if the burden of proof is explicitly—and continually—on those proposing to gather and use data for some purpose that is beneficial or financially advantageous to them.

are far more complicated. The ethical issues surrounding privacy and data use are not new, but the adoption of 5G and the increased bandwidth for connected devices in combination with edge computing and an increase in the use of algorithms to make decisions create a turning point in the magnitude of the data available. Many questions are important to consider, including what privacy users should have and what rights they have over information about them, their movements, and their activities. Although these concerns apply most directly to the devices someone chooses to use themselves, the implications extend to the decisions the people around them make. In May 2020, a judge found that one does not have a right to not have one's image taken in public by someone else (Cramer, 2020). If someone else's device is tracking you, without your consent, did you imply consent by being in public? These issues are difficult, not only because analysts thinking about such issues must explicitly explain their choices and rationales for what is of concern—although they do need to do that—but also because of the related need to involve diverse stakeholders in reaching a decision.

The imperative to involve the relevant stakeholders in any assessment of risks, costs, and benefits is now simply a part of the process, even embedded within the relevant global standard, International Organization for Standardization 31000 (International Organization for Standardization, 2018). The problem for the risks and benefits associated with the 5G era is that the stakeholders include the general populace, increasing the challenges involved in having meaningful consultation to define the "right" choices and even communication about those choices.

Another way to conceive of this is that, in the 5G era, the public needs to view these decisions as having what we call *perceptible legitimacy*. Otherwise, the decision risks being seen as the product of isolated elites—technical or economic—and so risk rejection by large parts of the public. This means that the public must meaningfully be involved in deciding the ethical

questions—notably, what is included as risks and benefits and how they are defined.

One way of handling this, described in the literature, involves an explicit plan for iterating with the stakeholders at each stage in the process (in which formal elections and voting are one example of an iteration). This is inherently in contrast to the "move fast and break things" ethos the technology industry has adopted. This approach is admittedly complex and onerous, which might not be easily implemented. We describe this methodology to illustrate a counterpoint to the current approach to data collection and use in the private sector, not to imply that it is the only or best approach.

We believe that this approach with a diverse public can be possible only if the burden of proof is explicitly—and continually—on those proposing to gather and use data for some purpose that is beneficial or financially advantageous to them. If that is explicitly true from the initiation of the analysis through to the monitoring of the use of the data, members of the public can see that their interests, however defined, can be protected. A key characteristic of this type of iterative risk assessment is clear communication of assumptions, limitations, and associated risks.

Most importantly, this up-front shifting of the burden of proof requires articulation and agreement on the ethical questions about what potential risks should be considered. The alternative, allowing data use and waiting to adjust once a problem arises, risks a familiar pattern in which the ethical questions are not faced until someone notes a problem. The fact that some use would then be established, presumably with gains for some party, could produce either a time-consuming disagreement on the ethical questions, frustrating those who see a problem and threatening the perceived legitimacy of the entire process, or the imposition of an ill-considered, draconian "solution" that sacrifices all the economic gain. Neither is even close to ideal, but steering between these two options takes care and attention.

In a sense, this is much like environmental regulation, in which a community demands some consideration of detrimental environmental effects of a development before committing to a project. Of course, this could also lead to delays that threaten a project, even if it eventually obtains permission. In one such example, the construction contractor threatening a potential stoppage in construction of the Purple Line mass-transit system in Maryland, claiming that this is in part because of the costs of delays in obtaining environmental permits (Shaver, 2020). The potential for such delays, and the presumably accompanying economic loss, is another one of the risks that must be considered in this process.

Potential Outcomes

The process described in the previous section can produce a wide variety of outcomes to be monitored. Here, we sketch a few to illustrate the breadth of potential outcomes.

One option that could be adopted would be having industry self-regulate. This would rely on voluntary guidelines adopted by the industry that is gathering and using the data—a form of self-governance.

Self-Governance by Technology Companies

The model of evaluation of technology described previously is a model in which the federal government would take the leading role in convening stakeholders and setting privacy norms. One option that could be adopted would be having industry self-regulate. This would rely on voluntary guidelines adopted by the industry that is gathering and using the data—a form of self-governance. Indeed, there have already been some attempts at these sorts of arrangements.

The FTC has previously recommended legislation that would allow consumers access to the information that data brokers collect and that would improve transparency for consumers while urging industry to implement self-regulatory measures (FTC, 2014). In the further development for a model in which the primary mover is technology companies' self-governance, a different risk framework might be necessary. One example of such a risk framework for self-governance is described in *Ethics and Data Science* (Loukides, Mason, and Patil, 2018). In it, the authors identify five categories, or five Cs, as guidelines to consider before building a data product: consent, clarity, consistency, control (and transparency), and consequences (and harm).

Consent refers to building trust with the people who are providing the data. The current standard operating procedure is to use acceptance of ToS as evidence of consent. Mistrust in ToS is not misguided: ToS are not the product of a negotiation but rather a one-sided agreement in which each user consents to let the product maker do what it wants with the data it collects.[3] And product makers can and often do unilaterally change these agreements. Because full participation in modern U.S. society relies on access to these technologies, consumers do not usually have a true choice about whether to use a particular product. This assumes that consumers even *give* consent; in fact, currently, many companies profit by collecting, using, and selling data without ever obtaining explicit consent. Credit reporting agencies are an example of companies that collect, use, and sell personal information without explicit consent.[4]

Five Cs are guidelines to consider before building a data product: consent, clarity, consistency, control, and consequences.

Related to consent is clarity about the activity (and consequences) to which one is consenting. In the current framework, the ToS to which a consumer agrees is written in legalese, and studies have shown that only 9 percent of people bother to even read ToS prior to installing an app—presumably, even fewer fully understand what is written (Deloitte, 2017). A party cannot obtain meaningful consent if the party consenting does not understand the terms to which it is agreeing.

Consistency and trust are tied together because, if a company is not consistent, it does not build trust with its consumers. An example of a company that has lost trust because of its lack of consistency is Facebook, which, through several scandals, including Cambridge Analytica's use of its data and lack of consistency in addressing misinformation campaigns, has damaged the trust consumers place in it (Weisbaum, 2018).

Control and transparency refers to the amount of control the user has over their data; what data, control, and transparency are provided and collected; and how the data are used. Laws, including the GDPR in the EU and the California Consumer Privacy Act (Cal. Civ. Code Title 1.81.5), have made efforts to legislate the control consumers have over their data.

The final C is *consequences*. There have been innumerable consequences for the collection and use of data, most of which had not been considered by the original technology developer, nor were the associated risks considered in the planning of the technology. It is also worth noting that, historically, the organizations with the economic incentive to move ahead have not done the best self-policing of their products, as seen with Facebook.

An important aspect of adopting this or any form of self-government is the explicit monitoring step above, the last in the organized process. Compliance monitoring is properly a governmental function and, because of the interstate and international nature of networks, one most appropriate for the federal government to perform. The federal government must continue to monitor the agreed-upon set of ethical issues and report regularly and transparently to all stakeholders, including members of the public who use or are affected by the technologies. This monitoring both provides an incentive for firms to abide by the guidelines and reassures all stakeholders that the outcomes are acceptable—or that, if they

In one model of data ownership, people could continuously own their data but be able to grant permission, for only certain uses, to a firm or firms.

are not, the government will revisit the process above to consider other outcomes.

Alternative Models of Data Ownership

Another potential outcome would be a policy change for who "owns" the data collected on individuals, likely requiring some legal and regulatory changes. This could be accomplished in any of a wide variety of ways, with differing implications for the firms and for individuals, particularly in the context of the control and transparency described in the discussion of self-governance. Currently, a firm owns the data it has gathered on an individual, largely with few restrictions and little responsibility to the people involved. But this is not the only possible framework.

In one model of data ownership, people could continuously own their data but be able to grant permission, for only certain uses, to a firm or firms.[5] This could be combined with requirements limiting the further dissemination of the information and with security requirements for holding the information. The latter might even be backed up by insurance against economic losses if, for example, financial information were used to steal someone's retirement accounts or social security benefits. In this case, all earnings from the use of the data would continue to accrue to the firm. One important complication of this model is an owner's right to withdraw permission for the use of their data. This would be a difficult and expensive rule for firms to implement—a risk that the overall process must consider alongside privacy concerns. The data would have been aggregated in different ways and used for other purposes already.

Alternatively, perhaps people could sell some or all of their data, granting some broader rights, such as allowing ads from many firms but for some (probably micro) payment. This would then again be combined with binding restrictions on other uses of the data, on security, and so forth, as in the prior example. Also as with the previous example, the potential loss of economic value if too few people sell their data should be acknowledged and considered.

Rights for People to Know About and Control Their Data

Another framework for data ownership could be a larger change in the basic legal structure involving personal

Another framework for data ownership could be one in which people have fundamental rights to know about the data collected about themselves and have some power over the use of those data.

data. The most sweeping change would be one in which people have fundamental rights to know about the data collected about themselves and have some power over the use of those data. For example, the United States could adopt a framework similar to the EU's GDPR. The GDPR requires that some personal data be deleted upon request of the subject of the data (Wolford, undated). However, the GDPR has proved difficult to enforce, in part because the lead regulator is the EU country in which the data-holding company is headquartered.

All these cases, and others that one can imagine, need to resolve some common questions, such as the allowed access for law enforcement to any personal information and the conditions for that access; the allowed access of the news media to some information, such as images of protests that might allow people to be identified; and the nature of any penalties for failure to secure personal data, perhaps dependent on the use or misuse of the data. All of these should be uncovered and identified early on, in the preliminary analysis and risk-estimation steps of the process, and this fact illustrates only some of the wide variety of stakeholders who must be involved.

For this report, we cannot determine the "right" or "best" outcome because that will necessarily be a societal decision, driven fundamentally by the ethical issues of privacy and overall societal well-being. Without a broad, societal decision, any outcome will lack the necessary base of support to be sustainable. And without a sustainable policy, the United States risks policy uncertainty and perhaps instability—forfeiting the economic promise of the 5G era while still incurring damaging uses of the data.

COVID-19 as a Case Study

There is a particular relevance to this process because the United States now faces both an urgent challenge and a unique opportunity. As of December 28, 2021, COVID-19 is known to have sickened nearly 53 million people in the United States and killed more than 818,000, with the threat of future mutations and waves

pending and the numbers probably being higher than those given because of testing scarcity and undiagnosed deaths and cases (CNN, 2021). When in crisis, people are often more willing than they might be otherwise to accept extreme measures for safety and security, so the trade-offs that a community is willing to make during the pandemic will have long-lasting effects on how it implements technology. Because the United States is currently in a time of upheaval, it is likely to enter the 5G era with even more-intrusive surveillance and fast-changing technology than it otherwise might have. This is a fast-moving area of public policy, with many recent reports and analyses (e.g., Mello and Wang, 2020; Darby, Louie, and Matheny, 2020). Our work emphasizes that these concerns should be addressed in the broader context of the 5G era, with the current pandemic serving as both an urgent reason to consider the issues and a striking example of the general problems that society will soon face.

The pandemic has already had direct effects on the gathering and use of personal data—notably, in China and Europe. At the same time, the enormous effects and uncertainty induced by the pandemic have made this a time of unusual fluidity in social and political behavior. The pandemic has shaped how people view the roles of these technologies. As the virus rapidly spread across the globe, people increasingly moved their work and social lives online. For many people, every interaction with someone else, every exercise class, every purchase has moved to an electronic device. Information collected by phones already shows whether populations and individuals are complying with mandatory stay-at-home and shelter-in-place orders.

The COVID-19 pandemic is a particularly important turning point, not just because of the threat but also because of the unprecedented executive powers available by the declaration of both a national health emergency and a national emergency. This could be the most consequential time in modern history to use risk assessment with stakeholders to make decisions about the implementation of technology.

Beyond their uses of existing technology, countries and companies have rapidly invested in ways to track COVID-19 using surveillance and data. The use of this technology might well be an example of people being willing to give up privacy concerns for the greater good, to allow the weakening of isolation measures and to prevent themselves from becoming ill. In hopes of tracking COVID-19 outbreaks, countries all over the world have implemented various forms of electronic technologies to first track and then enforce quarantining and self-isolation measures, as well as to trace contacts of infectious people when lockdowns are not in effect. All these options are natural ones for the United States to consider as well.

Beyond the initial lockdown in Wuhan, China quickly implemented a strict mobile app requirement. To engage in normal activities, such as entering a hotel or taking a train, each person must present their phone to show their color-coded status of green, yellow, or red. The app tracks the user's location and purchase history and changes their status based on possible contact

In hopes of tracking COVID-19 outbreaks, countries all over the world track, enforce quarantining and self-isolation measures, and trace contacts of infectious people.

with COVID-19 cases. The algorithms underlying the Chinese app are opaque, and it is unclear how the information is collected and how a color status is assigned (Mozur, Zhong, and Krolik, 2021). In Hong Kong, international travelers arriving in the country are required to wear electronic wristbands that also interface with an app and so monitor compliance with a two-week quarantine order (Saiidi, 2020).

The Republic of Korea has utilized data from electronic transactions, mobile phone location, and surveillance video streams to contact trace (Fendos, 2020). Detailed information about the locations, activities, and behavior of confirmed-positive patients are made public to allow others to assess their risk. The system has been successful in identifying and isolating outbreaks but at the cost of personal privacy. The system has been criticized for the level of personal detail provided in publicly released information. An outbreak in the Seoul party district highlights important privacy concerns; the information released about positive cases could identify members of sexual- and gender-minority communities, which could deter potentially exposed people from seeking COVID-19 testing (Kim, 2020).

How might contact tracing have been implemented more impactfully in the United States? Even putting aside the issues of privacy, duration of storage, and use of the information collected, other, quite practical issues remain. One in six Americans does not have a smartphone, and, of those who do, only 70 percent say they are willing to use a contact-tracing app; many cite privacy concerns. Another limitation to widespread adoption of this type of contact-tracing technology is the uneven levels of concern in different groups (e.g., ideological, racial). All of these represent sorts of ethical issues that need to be squarely and explicitly addressed to have a sustainable, effective policy in the United States.

Although contact tracing might be the most publicized, many health-related technologies have refocused to track COVID-19. Some existing networked devices, including health and fitness trackers, have turned to

Now is the time when people should rethink and more thoughtfully balance concepts of privacy, anonymity, safety, well-being, and fundamental freedoms.

using their data to track the COVID-19 outbreak. Examples include

- Kinsa QuickCare Bluetooth Smart Thermometers and Kinsa Smart Ear Bluetooth Thermometers, tools that connect to an app that contributes data to maps tracking fevers across the country (McNeil, 2020; "Social Distancing May Already Be Working to Slow Coronavirus Spread," 2020)
- the Oura Ring, which tracks heart rate and body temperature, has partnered with the University of California, San Francisco, to study whether the device can track COVID-19 outbreak patterns (Oura, 2020; Landi, 2020).

These examples are striking because they are repurposing data collected from users, are using health information that is not subject to HIPAA restrictions, and potentially link the user with a disease.

For the purpose of analyzing what a thoughtful assessment of a technology could look like, we used the example of the COVID-19 contact-tracing apps. Countries around the world have used the unprecedented Apple/Google partnership to develop contact tracing, which utilizes Bluetooth signals to measure proximity and duration of contact between people. At the time of this writing, Apple and Google have prohibited the development of apps that use location data to trace contacts. Several government organizations have said that the prohibition limits the usefulness of electronic contact tracing (Bond, 2020).

The underlying technology of Apple/Google tracking allows Bluetooth-enabled phones to ping each other when in proximity to each other; the duration of that contact would be collected. Each phone will collect a "key" for the devices with which it has had contact. If someone tests positive for COVID-19 *and* provides that information to the app, everyone who has been in contact with that person is notified. Health authorities have access to this information for contact tracing. The intention was for local health authorities to use the application programming interface developed by Google and Apple to develop their own apps with which users could interact and for participation to be voluntary for individuals.

Now is the time when people should rethink and more thoughtfully balance concepts of privacy, anonymity, safety, well-being, and fundamental freedoms. Emer-

gencies have a habit of suspending democratic norms, and many short-term emergency measures become permanent. The longest current national emergency declaration in the United States is from 1979 in response to the Iran hostage crisis (Trump, 2020b), and many of the measures taken following the attacks on September 11, 2001, also still remain in effect (Trump, 2020a). Many of the provisions first passed in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act (Pub. L. 107-56, 2001), including pen-register exceptions to wiretap laws,[6] have been broadly applied to internet communications and use. This provision allows the government to view some information, such as email subject lines and metadata, without a warrant. This is all to say that the decisions made during crisis have long-lasting effects, so people should consider this when deciding what norms they are willing to accept.

We believe that a thorough assessment of contact-tracing apps could and should use the above framework to help policymakers decide whether the potential benefit of a technology outweighs the associated risks. The assessment should, as above, include all relevant stakeholders from the companies developing the apps, government agencies, public health officials, and users, as well as those who might be negatively affected by the technology.

To illustrate the difficult issues that the process must confront and distinguish, we applied the five-C framework described above to a few alternative approaches for contact-tracing apps. For purposes of illustration, this analysis need not be specific to the current COVID-19 pandemic. Consider how public perception of risk—and emergency measures taken by government authorities—might change with higher infection and mortality rates. Indeed, this framework could also be applied to diseases that would pose substantially higher risks to life and health, not just to a potential second or third wave of COVID-19.

Consent and Clarity

A user cannot legally consent without understanding the terms to which they are consenting. Contact-tracing apps should therefore be explicit with users about the information collected, how it is used, and how their privacy is or is not protected. Clarity of this information for the user will likely affect public trust in adoption of apps and thus the effectiveness of electronic contact tracing.

Consistency (and Trust)

So that users can trust that information is being used in the way in which they have agreed, an app's purpose and description should not be changed without prior notification to those users. For example, various concerns would arise with contact tracing. Information about the people with whom each of us comes into contact and the duration of the contact is sensitive. It reveals the identities of people with whom one works and socializes. For example, one could imagine that a corporation that seeks to prevent its employees from unionizing might use

information from apps that track the people with whom organizers interact. By knowing the duration of the interaction, a corporation could know who is interested in unionizing. For public health officials, though, who are responsible for stay-at-home and physical-distancing orders, the data could be used to track people who have broken pandemic-related laws.

Can a user sufficiently trust Apple and Google, as well as their local health authorities, to use the information for only the intended purpose, for the data to be protected, and the data to sunset (i.e., to be deleted) when no longer needed? These are all examples of the questions that we believe must be addressed before a technology is adopted.

Control (and Transparency)

In a voluntary contact-tracing program, users could have control over their own data. They could even have the power to see and delete their own information. Alternatively, public health officials could argue that the government needs to maintain such records, at least for the duration of a pandemic wave.

Consequences

The efficacy of app-based contact tracing is not a given, in that success is dependent on adoption rates and test availability. If too few people are using the apps or not enough tests are performed to identify COVID-19 cases, the technology might not be useful. There is thus no guarantee of apps' efficacy, which will also likely vary by location.

The reason a deliberate approach to risk is so essential to COVID-19 contact-tracing apps is that the potential for negative consequences is vast. The apps specifically track everyone with whom a user has contact and their disease statuses. Each of these pieces of information is of a private nature, and each could be misused to harm someone. And in a future wave or an entirely different pandemic, this information could be even more harmful to someone.

If the mortality rate of a subsequent wave of the COVID-19 pandemic were higher, if for some other disease, if the spread of the illness were associated with specific behaviors or with marginalized groups, the misuse of information collected by contact-tracing apps would become more deleterious. Consideration of such consequences is particularly relevant during the COVID-19 pandemic because the pandemic has been coupled with civil unrest. Government misuse of contact information for identifying demonstrators could further erode public trust, decreasing the likely adoption of the technology and so rendering it less useful.

This example of contact tracing is only one example of the rapidly developing mobile technologies that will have a significant impact on future personal privacy and security. The applications of these technologies for coping with the COVID-19 pandemic are likely to be seen as urgent by some and threatening by others. Society will need to make choices.

The 5G era brings the promise of real economic gains but also the threat of great losses of privacy, anonymity, safety, and general well-being.

Final Observations

The 5G era, with its ubiquitous surveillance, brings the promise of real economic gains but also the threat of great losses of privacy, anonymity, safety, and general well-being. Most, if not all, the privacy issues discussed in this report predate the 5G era but will become more pressing with the adoption of 5G. Balancing legitimate but often-competing demands is a challenge—but one that appears ripe for meeting. Moreover, we believe that it can be met in a way that establishes the legitimacy of the result, producing a lasting resolution of this competition. Fundamentally, revenue is important, but it must not be the only metric by which technology is measured.

The federal government has the convening authority to organize a focused effort around a process of setting rules and guidelines governing the collection and use of data. It also has the ability to implement whatever result is determined, from monitoring a set of voluntary standards to large changes in law and regulation. Coping with the COVID-19 pandemic provides both new potential uses for this information and a window of time during which significant changes can be entertained—changes that might, in less eventful times, be viewed as too difficult or not urgent. The pandemic also highlights the need for public trust in information and processes.

What is needed is a decision to address issues related to data and privacy directly and not to simply wait to see what happens. We believe that adopting an explicit principle for widespread use during this 5G era—that any potential uses of data be identified, well defined, and agreed upon *before* data are collected and analyzed—can provide the rationale for the process and be a powerful incentive to participate for those wishing to make use of the data.

The resulting process described here, involving an intense focus on risk communication to the diverse stakeholders, then offers a path to a decision that has legitimacy across the country. Without such solid support, we feel that the competing risks and benefits of the 5G era could cause great dissent and indecision—resulting in losses of the benefits while still permitting some harms. We hope, and believe, that following this course of action can do the opposite, gaining benefits and avoiding most harms.

Notes

[1] This section draws heavily on Bonds et al., 2021.

A 5G network has data rates of up to 10 gigabits per second and 1 millisecond of latency and can accommodate up to 1 million devices per square kilometer; a 4G network has data rates of up to 100 megabits per second and 20 milliseconds of latency and can accommodate up to 60,000 devices per square kilometer.

[2] Companies operating in Europe must abide by the General Data Protection Regulation (GDPR). See European Commission, undated, and Palmer, 2019. California residents have data privacy rights under the California Consumer Privacy Act of 2018 (Cal. Civ. Code Title 1.81.5).

[3] We focus here on ToS because they are included in the millions of apps available for Apple and Android devices. The discussion might also apply equally to end-user license agreements.

[4] Most people never interact directly with a credit reporting agency except when requesting a free credit report. Although an agency checks the credit of a credit applicant, and accountholder information is reported regularly to those agencies, the consumer has no way to opt out of that system except to entirely forgo any type of credit. These agencies also collect public information, such as court judgments against consumers. The agencies sell this information to banks as part of credit checks, but some of that information is also sold for marketing purposes (hence people with good credit receiving credit offers in the mail).

[5] Senator John Kennedy of Louisiana introduced a bill stating, "Each individual owns and has an exclusive property right in the data that an individual generates on the internet under section 5 of the Federal Trade Commission Act (15 U.S.C. 45)" (U.S. Senate, 2019, § 2[a]). The EU grants individuals the right to be forgotten under GDPR Article 17. Also known as the *right to erasure*, it means that people have the right to demand that their personal data be erased. This right arises in specific circumstances, such as when "[t]he personal data is no longer necessary for the purpose an organization originally collected or processed it" (see Wolford, undated).

[6] A pen register collects all phone numbers dialed from a telephone line. The definition has expanded to include any technology that collects similar information, including the monitoring of internet communications.

References

Abbott, Brianna, "Google AI Beats Doctors at Breast Cancer Detection—Sometimes," *Wall Street Journal*, January 1, 2020.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Information," Washington, D.C.: Pew Research Center, November 15, 2019. As of June 5, 2020: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Barrett, Brian, "An Artist Used 99 Phones to Fake a Google Maps Traffic Jam," *Wired*, February 3, 2020.

Bond, Shannon, "Apple, Google Coronavirus Tool Won't Track Your Location. That Worries Some States," NPR, May 13, 2020. As of June 5, 2020: https://www.npr.org/2020/05/13/855064165/apple-google-coronavirus-tech-wont-track-your-location-that-worries-some-states

Bonds, Timothy M., James Bonomo, Daniel Gonzales, C. Richard Neu, Samuel Absher, Edward Parker, Spencer Pfeifer, Jennifer Brookes, Julia Brackup, Jordan Willcox, David R. Frelinger, and Anita Szafran, *America's 5G Era: Gaining Competitive Advantages While Securing the Country and Its People*, Homeland Security Operational Analysis Center operated by the RAND Corporation, PE-A435-1, 2021. As of December 27, 2021: https://www.rand.org/pubs/perspectives/PEA435-1.html

Brown, Dalvin, "How to Secure Your Home Surveillance Cameras from Getting Hacked," *USA Today*, December 13, 2019. As of June 5, 2020: https://www.usatoday.com/story/tech/2019/12/13/how-secure-your-home-surveillance-cameras-getting-hacked/4407914002/

Cadell, Cate, "China's Coronavirus Campaign Offers Glimpse into Surveillance System," Reuters, May 25, 2020. As of January 24, 2021: https://www.reuters.com/article/us-health-coronavirus-china-surveillance/chinas-coronavirus-campaign-offers-glimpse-into-surveillance-system-idUSKBN2320LZ

California Civil Code, Division 3, Obligations; Part 4, Obligations Arising from Particular Transactions; Title 1.81.5, California Consumer Privacy Act of 2018. As of December 27, 2021: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Cisco, *Cisco Annual Internet Report (2018–2023)*, updated March 9, 2020. As of April 20, 2020: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

CNN, "Tracking COVID-19 Cases in the US," last updated December 28, 2021. As of September 14, 2021: https://www.cnn.com/interactive/2020/health/coronavirus-us-maps-and-cases/

Cramer, Maria, "Trailing Women with a Camera Was Legal, Appeals Court Rules," *New York Times*, May 12, 2020.

Darby, Chris, Gilman Louie, and Jason Matheny, "Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence," National Security Commission on Artificial Intelligence, White Paper on Pandemic Response and Preparedness 2, May 6, 2020.

Dearden, Lizzie, "Coronavirus Lockdown Causing 'Creeping' Expansion of Intrusive Surveillance Tactics, Campaigners Warn," *The Independent*, April 26, 2020. As of June 5, 2020: https://www.independent.co.uk/news/uk/home-news/coronavirus-lockdown-surveillance-uk-nhs-app-drones-anpr-4g-a9484566.html

Deloitte, *2017 Global Mobile Consumer Survey: US Edition—The Dawn of the Next Era in Mobile*, 2017. As of June 5, 2020: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf

Dressel, Julia, and Hany Farid, "The Accuracy, Fairness, and Limits of Predicting Recidivism," *Science Advances*, Vol. 4, No. 1, January 17, 2018, p. eaao5580.

European Commission, "Data Protection in the EU," webpage, undated. As of December 27, 2021: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, May 2014. As of January 24, 2021: https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

———, "Sharing Consumer Health Information? Look to HIPAA and the FTC Act," October 2016. As of July 22, 2020: https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act

Fendos, Justin, "How Surveillance Technology Powered South Korea's COVID-19 Response," *TechStream*, Washington, D.C.: Brookings Institution, April 29, 2020. As of June 5, 2020: https://www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/

Fischhoff, Baruch, "The Realities of Risk–Cost–Benefit Analysis," *Science*, Vol. 350, No. 6260, October 30, 2015.

FTC—*See* Federal Trade Commission.

Gan, Nectar, "China Is Installing Surveillance Cameras Outside People's Front Doors . . . and Sometimes Inside Their Homes," CNN, April 28, 2020. As of January 24, 2021: https://www.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html

Gara, Antoine, "British Trader Navinder Sarao Arrested over 2010 Flash Crash," *Forbes*, April 21, 2015. As of December 27,2021: https://www.forbes.com/sites/antoinegara/2015/04/21/british-trader-navinder-sarao-arrested-over-2010-flash-crash/?sh=2d74cf872e35

Gopalakrishnan, Chandu, "Google Faces GDPR Violation Complaint: Privacy Expert Finds Merit in Move," SC Media UK, March 20, 2020.

Harwell, Drew, "Police Can Keep Ring Camera Video Forever and Share with Whomever They'd Like, Amazon Tells Senator," *Washington Post*, November 19, 2019. As of June 5, 2020: https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/

Haselton, Todd, "Apple Apologizes for Listening to Siri Conversations," CNBC, August 28, 2019. As of June 5, 2020: https://www.cnbc.com/2019/08/28/apple-apologizes-for-listening-to-siri-conversations.html

International Organization for Standardization, "Risk Management—Guidelines," ISO 31000:2018(en), 2018. As of June 5, 2020: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Jin, Huafeng, and Shuo Wang, "Voice-Based Determination of Physical and Emotional Characteristics of Users," U.S. Patent 10,096,319, filed March 13, 2017, and granted October 9, 2018. As of December 27, 2021: https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=10096319.PN.&OS=PN/10096319&RS=PN/10096319

Kim, Min Joo, "Tracing South Korea's Latest Virus Outbreak Shoves LGBTQ Community into Unwelcome Spotlight," *Washington Post*, May 11, 2020.

Koebler, Jason, Emanuel Maiberg, and Joseph Cox, "This Small Company Is Turning Utah into a Surveillance Panopticon," *Vice*, March 4, 2020. As of June 5, 2020: https://www.vice.com/en_us/article/k7exem/banjo-ai-company-utah-surveillance-panopticon

Landi, Heather, "UCSF Partners with Oura Smart Ring to Study Early Detection of COVID-19," FierceHealthcare, March 27, 2020. As of June 5, 2020: https://www.fiercehealthcare.com/tech/ucsf-launches-study-to-use-wearable-data-from-oura-ring-for-early-covid-19-detection

Lin, Liza, and Newley Purnell, "A World with a Billion Cameras Watching You Is Just Around the Corner," *Wall Street Journal*, December 6, 2019.

Littman, Jonathan, "Waze Hijacked L.A. in the Name of Convenience. Can Anyone Put the Genie Back in the Bottle?" *Los Angeles Magazine*, August 20, 2019. As of June 5, 2020: https://www.lamag.com/citythinkblog/waze-los-angeles-neighborhoods/

Loukides, Mike, Hilary Mason, and D. J. Patil, *Ethics and Data Science*, Sebastopol, Calif.: O'Reilly Media, 2018.

Macfarlane, Jane, "Your Navigation App Is Making Traffic Unmanageable," *IEEE Spectrum*, September 19, 2019.

McNeil, Donald G., Jr., "Can Smart Thermometers Track the Spread of the Coronavirus?" *New York Times*, March 18, 2020.

Mello, Michelle M., and C. Jason Wang, "Ethics and Governance for Digital Disease Surveillance," *Science*, Vol. 368, No. 6494, May 29, 2020, pp. 951–954.

Menni, Cristina, Ana M. Valdes, Maxim B. Freidin, Carole H. Sudre, Long H. Nguyen, David A. Drew, Sajaysurya Ganesh, Thomas Varsavsky, M. Jorge Cardoso, Julia S. El-Sayed Moustafa, Alessia Visconti, Pirro Hysi, Ruth C. E. Bowyer, Massimo Mangino, Mario Falchi, Jonathan Wolf, Sebastien Ourselin, Andrew T. Chan, Claire J. Steves, and Tim D. Spector, "Real-Time Tracking of Self-Reported Symptoms to Predict Potential COVID-19," *Nature Medicine*, Vol. 26, May 11, 2020, pp. 1037–1040.

Mitchell, Anna, and Larry Diamond, "China's Surveillance State Should Scare Everyone," *The Atlantic*, February 2, 2018.

Mozur, Paul, Raymond Zhong, and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags," *New York Times*, March 1, 2020, updated January 28, 2021.

Nakashima, Ellen, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, July 9, 2015.

Nuzzi, Olivia, "What It's Like to Get Doxed for Taking a Bike Ride," *Intelligencer*, June 8, 2020. As of January 24, 2021: https://nymag.com/intelligencer/2020/06/what-its-like-to-get-doxed-for-taking-a-bike-ride.html

O'Neill, Patrick Howell, Tate Ryan-Mosley, and Bobbie Johnson, "A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them," *MIT Technology Review*, May 7, 2020.

Oura, "UCSF TemPredict Study," news release, August 31, 2020. As of June 5, 2020: https://ouraring.com/ucsf-tempredict-study

Palmer, Danny, "What Is the GDPR? Everything You Need to Know About the New General Data Protection Regulations," *ZDNet*, May 17, 2019. As of January 24, 2021: https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Pramono, Renard Xaviero Adhi, Syed Anas Imtiaz, and Esther Rodriguez-Villegas, "A Cough-Based Algorithm for Automatic Diagnosis of Pertussis," *PLoS ONE*, Vol. 11, No. 9, September 1, 2016, p. e0162128. As of June 5, 2020: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0162128

Public Law 93-579, Privacy Act of 1974, December 31, 1974. As of February 7, 2021: https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf

Public Law 104-191, Health Insurance Portability and Accountability Act of 1996, August 21, 1996. As of February 6, 2021: https://www.govinfo.gov/app/details/PLAW-104publ191/summary

Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, October 26, 2001. As of February 7, 2021: https://www.govinfo.gov/app/details/PLAW-107publ56/summary

Robles, Frances, "Russian Hackers Were 'in a Position' to Alter Florida Voter Rolls, Rubio Confirms," *New York Times*, April 29, 2019.

Romm, Tony, "U.S. Government Issues Stunning Rebuke, Historic $5 Billion Fine Against Facebook for Repeated Privacy Violations," *Washington Post*, July 24, 2019.

Saiidi, Uptin, "Hong Kong Is Putting Electronic Wristbands on Arriving Passengers to Enforce Coronavirus Quarantine," CNBC, March 18, 2020. As of June 5, 2020: https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html

Schuppe, Jon, "Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect," NBC News, March 7, 2020. As of June 5, 2020: https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

Shaver, Katherine, "Purple Line Consortium Says It Will Dissolve Public–Private Partnership with State If It Can't Reach a Deal on Cost Overruns," *Washington Post*, June 23, 2020.

Singer, Natasha, and Kate Conger, "Google Is Fined $170 Million for Violating Children's Privacy on YouTube," *New York Times*, September 4, 2019.

Sly, Liz, "U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging," *Washington Post*, January 29, 2018.

"Social Distancing May Already Be Working to Slow Coronavirus Spread, Smart Thermometer Data Suggest," *Boston Globe*, March 31, 2020.

"The World's Most Valuable Resource Is No Longer Oil, but Data," *The Economist*, May 6, 2017. As of June 5, 2020: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Thompson, Stuart A., and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times*, December 19, 2019. As of June 5, 2020: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Trump, Donald J., President, "Continuation of the National Emergency with Respect to Certain Terrorist Attacks," *Federal Register*, Vol. 85, No. 177, September 11, 2020a, p. 56467. As of March 12, 2021: https://www.federalregister.gov/documents/2020/09/11/2020-20312/continuation-of-the-national-emergency-with-respect-to-certain-terrorist-attacks

———, "Continuation of the National Emergency with Respect to Iran," *Federal Register*, Vol. 85, No. 220, November 13, 2020b, p. 72895. As of March 12, 2021: https://www.federalregister.gov/documents/2020/11/13/2020-25310/continuation-of-the-national-emergency-with-respect-to-iran

U.S. Code, Title 15, Commerce and Trade; Chapter 2, Federal Trade Commission; Promotion of Export Trade and Prevention of Unfair Methods of Competition; Subchapter I, Federal Trade Commission; Section 45, Unfair Methods of Competition Unlawful; Prevention by Commission. As of December 28, 2021: https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title15-section45&num=0&edition=prelim

U.S. Senate, Own Your Own Data Act, Senate Bill 806, 116th Congress, introduced March 4, 2019, referred to Committee on Commerce, Science, and Transportation on March 14, 2019. As of December 28, 2020: https://www.govtrack.us/congress/bills/116/s806

"Utah Police Look to Artificial Intelligence for Assistance," *Salt Lake Tribune*, January 14, 2020. As of January 24, 2021: https://www.sltrib.com/news/2020/01/15/utah-police-look/

Weisbaum, Herb, "Trust in Facebook Has Dropped by 66 Percent Since the Cambridge Analytica Scandal," NBC News, April 18, 2018. As of July 27, 2020: https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011

Wolford, Ben, "Everything You Need to Know About the 'Right to Be Forgotten,'" Proton Technologies, undated. As of June 5, 2020: https://gdpr.eu/right-to-be-forgotten/

Yang, Jia Lynn, and Amrita Jayakumar, "Target Says Up to 70 Million More Customers Were Hit by December Data Breach," *Washington Post*, January 10, 2014. As of June 5, 2020: https://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html

Yang, Yuan, Nian Liu, Sue-Lin Wong, and Qianer Liu, "China, Coronavirus and Surveillance: The Messy Reality of Personal Data," *Financial Times*, April 1, 2020.

Zhong, Raymond, "China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears," *New York Times*, May 26, 2020.

About the Authors

Jennifer Brookes is a physical scientist at the RAND Corporation. Her professional interests include wargaming, emerging technology, and strategic planning. She has a Ph.D. in physical chemistry.

James Bonomo is a senior physical scientist at RAND. Most of his research focuses on system development or acquisition, primarily for the military or other national security sponsors. He has a Ph.D. in physics.

Timothy M. Bonds is a senior fellow at RAND. His areas of research emphasis include the economic, technical, and social impacts of the 5G era; forces and capabilities needed to meet national security objectives and commitments; command-and-control capabilities; personnel mission-day metrics; and military employment of commercial space systems and services. He has an M.S. in aero/astro engineering and an M.B.A.

About This Perspective

This report is one of a set of publications that examine the United States' fifth-generation (5G) wireless future across a variety of dimensions that include data privacy. As noted in the first in the set,

> The latest generation of wireless networks, called 5G (for "fifth generation"), has launched with great expectations and amid significant concerns. A theme running through discussions of the 5G era is that this is a race, that first movers will dominate all others, and that this dominance will provide enduring economic and technical benefits to those first movers' home countries and people. (Bonds et al., 2021, p. 1)

This framework of 5G technology adoption as a race might tend to blind the public and policymakers to some of the dangers of rushing into the 5G era without carefully considering its potential downsides.

Concurrently with the adoption of 5G technology, the number of automated sensors and devices connected to wireless networks will grow in the next few years by an order of magnitude or more. Increasingly, these networks will inform artificial-intelligence algorithms, which will then autonomously make decisions and take actions—with human decisionmakers directly involved only infrequently. In this report, we describe how the United States should seek to balance the potential gains of the 5G era with the potential loss of privacy and of control over personal data. The findings should be of interest to policymakers and researchers with an interest in the broader impacts of the implications for the 5G era.

Funding

Funding for this research was made possible by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

www.rand.org