

# infrastructure

Vol. 60, No. 1, Fall 2020

## Managing Critical Infrastructure During the COVID-19 Pandemic

By Kevin W. Jones

The continuing outbreak of the novel coronavirus disease (COVID-19) has upended business as usual. New cases continue to grow, and governments around the world have implemented a variety of measures in an effort to slow the spread of the virus and mitigate the strain that it has placed on healthcare systems.<sup>1</sup> Following some background and an overview of the disease characteristics of COVID-19, this article discusses measures for facilitating the continued availability of mission-critical personnel and relevant legal considerations.

### Background

To address the pandemic, governments have issued a range of mandates and official guidance regarding social distancing, face coverings, and business closures and restrictions aimed at limiting transmission among individuals in close contact. Businesses responsible



Jones

*Kevin W. Jones (kjones@HuntonAK.com) is a partner at Hunton Andrews Kurth LLP in the Energy and Infrastructure practice, and he is cochair of the firm's Energy Sector Security Team. Contributions to this article were provided by Paul M. Tiao, a partner in the firm's Privacy and Cybersecurity practice and cochair of the firm's Energy Sector Security Team; Susan F. Wiltsie, a partner in the firm's Labor and Employment practice; and Matt A. Stuart, a senior attorney in the firm's Oil, Gas & LNG practice. Special thanks to Mark A. Rausch, MD, FACEP, CEO of Secure Health, a medical testing and monitoring company, for his review of this article.*



for critical infrastructure, however, must continue certain operations in the challenging environment of the pandemic.

In recognition of this, essential critical infrastructure workers have been exempted from various “stay-at-home” orders.<sup>2</sup> This reality presents unique challenges for critical infrastructure operators, especially since many critical infrastructure workers cannot work remotely and often must work in close proximity to one another, whether in a control room, as part of a maintenance crew, or in an essential production facility. This heightens the risk of infection for individual workers and

*continued on page 12*

# infrastructure

Vol. 60, No. 1

ISSN: 1097-251X

*Infrastructure* is produced quarterly by ABA Publishing for the ABA Infrastructure and Regulated Industries Section.

©2020 by the American Bar Association. To request reprints, go to [www.americanbar.org/utility/reprint](http://www.americanbar.org/utility/reprint).

Articles reflect the views of the authors and do not necessarily represent the position of the American Bar Association or the ABA Infrastructure and Regulated Industries Section.

Readers are encouraged to send news, views, requests or suggestions to [infrastructure@americanbar.org](mailto:infrastructure@americanbar.org).

## Editor

William R. Drexel  
[billdrex@yahoo.com](mailto:billdrex@yahoo.com)

## Editorial Board

Steven C. Friend  
[sfriend@hunton.com](mailto:sfriend@hunton.com)  
David R. Hardy  
[dhardy@osler.com](mailto:dhardy@osler.com)  
J.P. Shotwell  
[j.p.shotwell@sce.com](mailto:j.p.shotwell@sce.com)  
Dena E. Wiggins  
[dena.wiggins@ngsa.org](mailto:dena.wiggins@ngsa.org)

## Section Chair

Catherine P. McCarthy  
[cathy.mccarthy@bracewell.com](mailto:cathy.mccarthy@bracewell.com)

## Section Director

Susan Koz  
[susan.koz@americanbar.org](mailto:susan.koz@americanbar.org)  
American Bar Association  
Chicago

## Managing Editor

Lisa V. Comforty  
[lisa.comforty@americanbar.org](mailto:lisa.comforty@americanbar.org)

## Senior Designer

Betsy Kulak  
[elizabeth.kulak@americanbar.org](mailto:elizabeth.kulak@americanbar.org)



## Chair's Column

By Catherine P. McCarthy

As the incoming Chair of the ABA's Infrastructure and Regulated Industries Section, I am grateful for the opportunity, and I look forward to working with Section members. Regulated industries owning infrastructure and providing service to the public are a national priority now more than ever. For example, the COVID-19 pandemic has accelerated changes in the way we rely on the communications industry, underscoring the importance of communications infrastructure, services, and providers. This year's presidential election will also highlight the importance of infrastructure. Issues central to the election include how our infrastructure will be developed, maintained, and financed, and also, how environmental considerations related to infrastructure should be weighed prospectively by government regulators, regulated service providers, and the public.

IRIS provides an invaluable opportunity to share legal knowledge and experience. Legal knowledge and experience pertaining to infrastructure and regulated industries is particularly transferable, as regulated industries (i.e., communications, energy, water, and transportation) face similar legal challenges. For example, legal issues related to physical or cyber threats are similar across various types of infrastructure and many regulated industries. IRIS members benefit from participation in IRIS through reading or writing for IRIS publications or its twitter feed, attending or presenting in IRIS CLE seminars or podcasts, attending an IRIS Young Lawyers event, or serving as a committee member. Please feel free to reach out to me directly if you have an

*continued on page 18*



## Editor's Column

By William R. Drexel

The COVID-19 pandemic has had a profound impact on our country, its economy, and its citizens. The long-term global consequences of the virus remain unclear, but it likely will affect critical infrastructure providers directly and indirectly for some time. It is thus quite appropriate that we dedicate this issue to the pandemic and how it impacts, and may be impacted by, the infrastructure sector of our economy.

In our first article, *Managing Critical Infrastructure During the COVID-19 Pandemic*, Kevin Jones explains how critical infrastructure companies and other essential businesses can take measures and develop strategies to monitor and manage the risk of exposure to COVID-19 within their workforces. The article explains the importance of contingency plans that can be implemented swiftly if an outbreak occurs within the essential employee population. Substantial advance planning is necessary because medical, legal, and other considerations must be coordinated among company management, legal and medical advisors, and critical workforce personnel.

In our second article, *Mobile Technologies and COVID-19: A Primer on Fighting the Virus with Cell Phones*, Michael Roberts explains how mobile technologies can be used by businesses and governments to manage the

*continued on page 19*

# Mobile Technologies and COVID-19: A Primer on Fighting the Virus with Cell Phones

By Michael R. Roberts

As of September 2020, the coronavirus and the disease it causes, COVID-19, had taken the lives of over 180,000 people in the United States and caused widespread economic dislocation and unemployment. Tragically, the virus also shows little sign of abating, and public health officials warn that there may be a “second wave” of infections. U.S. governments and businesses thus continue to seek ways to mitigate COVID-19’s effects, at least until a safe and effective vaccine or antiviral treatment is discovered. Mobile technologies are consistently mentioned as a piece of this mitigation puzzle, whether it be by enabling quarantine strategies through “contact tracing,” providing mobile “passports” to signify viral diagnoses or potential immunity, or assisting in health monitoring and alerting to prevent the spread of the virus.

Even as governments and businesses deploy these strategies, however, questions and controversies regarding their use persist. What data will be collected and used? How long will it be retained? And, critically, what steps should be taken to try to ensure that the COVID-19 crisis won’t permanently reset the balance between privacy and security to the detriment of civil liberties?

This article cannot definitively answer these questions and does not recommend any particular technology to respond to the pandemic. Any attempt to do so risks obsolescence given the light-speed pace of technological development and policy debates.

Instead, this article provides a short primer on key relevant privacy considerations and issues in order to assist businesses considering whether to develop or use mobile



Roberts

*Michael R. Roberts (mrroberts@sidley.com), formerly a White House intern in the Office of the Counsel to Vice President Biden, is an associate in the Sidley Austin LLP Privacy and Cybersecurity group. The author thanks Christopher C. Fonzone, a partner in the firm’s Privacy and Cybersecurity practice, for his contributions to this article. The views expressed herein are the author’s alone and do not constitute legal advice.*



technologies to fight COVID-19. It first outlines the main ways governments and businesses might use mobile technologies to fight the virus and the potential applicability of current laws to these uses. It then details how those laws might change as legislatures and regulators address the novel privacy and civil liberties issues raised by COVID-19. Finally, this article offers a checklist to capture important data privacy and security legal considerations relevant to the use of mobile technologies to combat COVID-19.

## How Mobile Technologies May Help Fight COVID-19

Although we learn more about COVID-19 on an almost daily basis, the basic ways mobile technologies might help address the pandemic are unlikely to change.

At least at the start of the pandemic, there was little understanding about whether humans had any immunity to COVID-19 because it is novel and, because the virus is also highly communicable, it spreads rapidly if infected people have sufficient contact with healthy individuals. Given this, earlier this year, the United States and various state and local jurisdictions adopted a variety of measures—including physical distancing and

statewide shutdowns—to help slow the virus’s spread. These measures helped to “flatten the curve”—i.e., mitigate the exponential growth of COVID-19 that can overwhelm health systems. Numerous jurisdictions began allowing more activity in May and June in an effort to reopen the economy, attempting to focus quarantine and self-isolation efforts on infected individuals rather than on the general population. Pervasive asymptomatic spread of COVID-19, however, complicated those efforts, and the relaxing of measures produced a resurgence of COVID-19 cases in some areas.

These developments put additional pressure on businesses and governments to determine whether there is a way to enable economic activity and increase in-person interactions without producing an unacceptable surge in COVID-19 infection rates in the absence of a safe and effective vaccine or antiviral treatment. Technologists and others have suggested three key ways that mobile technologies may help.

### **Contact Tracing**

First, mobile technologies may assist in contact tracing, which seeks to curb the spread of COVID-19 by identifying individuals who have been in “contact” with infected persons and then alerting those contacts so that they can take appropriate precautions to prevent further infections. Of course, this strategy is at best a partial mitigation approach. Contact tracing would not assist with tracing infections that may have been caused by asymptomatic carriers or carriers who do not report that they have COVID-19.<sup>1</sup> Nevertheless, contact tracing could be one tool that helps jurisdictions move away from shutdowns and physical distancing by identifying a set of individuals who need to quarantine.

An unfortunate problem with “traditional” contact tracing is that it is difficult to scale and time-consuming, and it is also subject to the vicissitudes of memory and other human factors, such as the ability to locate potential contacts for purposes of informing them of their potential exposure.<sup>2</sup> And this is where mobile technologies enter the discussion.

According to the U.S. Centers for Disease Control and Prevention (CDC), there are two broad categories of ways technological tools can supplement or replace traditional contract tracing approaches. First, tools can be used for case management—i.e., to improve “the efficiency and accuracy of data management and automating tasks” and “reduce the burden of data collection on public health staff by allowing electronic self-reporting by cases and contacts.”<sup>3</sup> Here, mobile applications can automate much of the typically labor-intensive interview and tracing process, saving manpower and time. Second, and more dramatically, technology can be used to “identify community contacts unknown to the case,” which is also known as “proximity tracking.”<sup>4</sup> This second use takes advantage of the fact that individuals typically carry with them

mobile devices that can communicate with other mobile devices, making it possible for those devices to store close “contacts” so that they can be uncovered at a later time if necessary for virus prevention. (Of course, proximity tracking requires widespread community adoption and, as discussed later, raises significant privacy and civil liberties questions.)

Given these potential benefits, it is unsurprising that numerous countries have announced or implemented contact tracing apps or other app-based technologies intended to help tracing efforts.<sup>5</sup> In the United States, there is currently no comprehensive federal contact tracing system, but the CDC has been “conducting a landscape analysis and evaluation of contact tracing tools; generating preliminary tool recommendations for piloting tracing in areas with limited introduction of COVID-19; and coordinating with public health agencies, healthcare organizations, academic institutions, non-profit organizations, and private companies to maximize contact tracing effectiveness.”<sup>6</sup>

States have also adopted a range of approaches. For instance, New York State partnered with Bloomberg Philanthropies, Johns Hopkins Bloomberg School of Public Health, and Vital Strategies to launch a contact tracing program that will be implemented in coordination with New Jersey and Connecticut.<sup>7</sup> Several states have also leveraged mobile technologies and platforms for contact tracing purposes or even created their own contact tracing apps,<sup>8</sup> and others are reportedly exploring doing so.<sup>9</sup>

### **Quick Response (QR) Codes and Digital “Immunity” Passports**

A second way mobile technologies can be used to address the COVID-19 crisis is by serving as quick response (QR) codes—machine-readable tags that identify the device user or that user’s traits. The possible uses of such codes are extremely varied. For example, they can be used to track the presence of individuals at particular places to assist with contact tracing. Or the codes can serve as “digital passports” to show that individuals are symptom-free or approved to report to work.

Indeed, various countries, such as Singapore and New Zealand, are already using QR code technologies to address COVID-19.<sup>10</sup> In addition, South Korea has deployed QR codes as symptom-free electronic passports.<sup>11</sup> And on June 10, after determining that a simple sign-in system was not comprehensive, South Korea required “places at high-risk” for COVID-19, including bars, clubs, and other entertainment venues, to register patrons in a QR code-based registration system.<sup>12</sup>

### **Health Screening, Monitoring, and Alerting Systems**

A third way mobile technologies can assist is by aiding health screening, monitoring, and alerting, although experts continue to evaluate the impact of such uses.<sup>13</sup> These mobile technologies are relatively straightforward and may be used in conjunction with wearables and contactless kiosks.<sup>14</sup>

Indeed, due to government mandates for symptom screening and the speed at which such technologies can be deployed, these technologies are becoming increasingly prevalent. Many state and local governments now require or recommend that businesses conduct daily symptom screenings before employees enter a physical work location.<sup>15</sup> Businesses faced with determining how to implement such guidance are increasingly looking to mobile technologies to simplify the task.

### Existing Laws Applicable to Mobile Technologies Fighting COVID-19

As noted at the outset, the use of mobile technologies to address COVID-19 implicates important data privacy and security considerations. The technologies discussed in the prior section may collect and use various types of data that can reveal sensitive details about an individual's life. For example, contact tracing applications may track detailed movement and location information, QR code programs may also require individuals to uniquely identify their location, and all of the applications would likely collect or use sensitive health information. It is therefore understandable why privacy and civil liberties advocates want to ensure that there are appropriate protections before unleashing these technologies on COVID-19.

But it would be a mistake to assume that the calls for further legislation and regulation mean that there are no existing laws governing the most common ways technologies may be brought to bear against the virus. Indeed, to the contrary, detailing all the relevant laws would extend far beyond the scope of this article. Instead, it provides a brief tour of important existing legal regimes that might govern some of these mobile technologies.

Before turning to the legal specifics, however, it is important to note that the laws discussed in this section, even if plainly applicable during the COVID-19 pandemic, were not enacted and have not necessarily been interpreted with a global public health crisis in mind. Indeed, regulators are rapidly considering their enforcement posture and how these laws might apply to present-day facts, with the following examples representing only a small portion of their recent guidance.

- The U.S. Occupational Safety and Health Administration (OSHA), which regulates safety and health issues in the workplace and enforces the Occupational Safety and Health Act of 1970, has explained that it will evaluate community spread of COVID-19 in each geographic area when considering the frequency of workplace inspections and its enforcement priorities.<sup>16</sup>
- Similarly, the Equal Employment Opportunity Commission (EEOC), which enforces workplace antidiscrimination laws, has issued guidance concerning COVID-19 and the Americans with

Disabilities Act (ADA), the Rehabilitation Act, and other equal employment opportunity laws, which may include the Family and Medical Leave Act and the Genetic Information Nondiscrimination Act.<sup>17</sup> Importantly, this guidance asserts that employee medical information about COVID-19 symptoms and diagnosis must be maintained as a “confidential medical record” under the ADA, including when the employer receives such information in relation to a medical examination or inquiry or if the employee volunteers to provide the employer with such pandemic-related medical information.<sup>18</sup>

- The Federal Trade Commission (FTC) has also issued guidance on its enforcement posture during the pandemic, explaining that it “will be flexible and reasonable when it comes to bringing enforcement actions against companies engaged in good faith, thoughtful efforts to address the effects of the pandemic,” while cautioning that it still “doesn’t pay to be in the news for privacy and security problems, and then have to retreat to address them.”<sup>19</sup> The FTC has previously issued guidance on mobile privacy issues, including recommending that platforms provide notice to and obtain affirmative express consent from individuals before permitting apps to access geolocation information.<sup>20</sup> The FTC has also highlighted four critical “tips” for businesses using data during the pandemic, specifically that a business should (1) consider privacy and security as it develops products and services, and not after launch; (2) utilize privacy protective technologies; (3) consider using anonymous, aggregate data; and (4) delete data when the crisis ends.<sup>21</sup>

The bottom line is that, to ensure the compliance of their plans, companies that employ COVID-19 technologies should check the latest regulatory guidance applicable to their efforts.

And with that crucial message out of the way, here are some of the key laws that businesses should consider when evaluating whether to deploy any of the technologies identified above.

### Federal Laws Applicable to the Government

Businesses initially should consider whether they will work with the federal government in using mobile technology to address the COVID-19 crisis. If they will, businesses must take into account a set of laws applicable only to the government, including the Privacy Act of 1974 and the Freedom of Information Act (FOIA).<sup>22</sup>

The most important law applicable to the government is, of course, the Fourth Amendment to the U.S. Constitution, which protects people against unreasonable searches and seizures.<sup>23</sup> As a practical matter, the Supreme Court has interpreted this mandate as

prohibiting the government from gathering data without consent when individuals have a reasonable expectation of privacy unless the government has a warrant or an exception to the warrant requirement applies.<sup>24</sup> Since recent precedents make clear that individuals have such reasonable expectations regarding the contents of their cell phone and historical cell-site locational information, this means that, to engage in the sorts of contact tracing described above, the government might need a warrant or an exception to the warrant requirement.<sup>25</sup>

To that end, the Supreme Court has repeatedly recognized that the government may conduct a search without obtaining a warrant if it would be impractical to do so, the goal is not traditional law enforcement, and the search is otherwise reasonable and proportional to the facts and circumstances.<sup>26</sup> This is commonly known as the “special needs” or administrative search doctrine. While the scope and criteria for this doctrine are not well-defined, the Court has used the doctrine to allow certain public health and safety initiatives, and it may be applicable here.<sup>27</sup>

Moreover, the Fourth Amendment likely does not apply to location data that is sufficiently de-identified and aggregated,<sup>28</sup> which may be relevant if the government is using aggregated data to understand compliance with quarantine orders.

In short, if businesses are providing applications or information to the government, they should evaluate whether the Fourth Amendment applies and, if it does, whether the provision of information is consistent with it.

### **Generally Applicable Federal Laws**

Although the United States does not have a comprehensive cross-sectoral privacy regime like the European Union’s General Data Protection Regulation (GDPR), it does have various legal regimes that focus on particular sectors or interests. While a complete tour of this landscape is beyond this article’s scope, the following highlights three of the legal regimes most likely relevant to the technological applications identified above.<sup>29</sup>

#### *Wiretap and Stored Communications Acts*

The Wiretap Act and the Stored Communications Act (SCA) are the primary federal laws protecting the privacy of electronic communications. The Wiretap Act, among other things, generally prohibits the nonconsensual “interception” of electronic communications, absent lawful process.<sup>30</sup> The SCA generally prohibits service providers from knowingly disclosing the contents of communications to any person or entity<sup>31</sup> and also bars providers from sharing with any governmental entity certain information, specifically a customer record or other information regarding a subscriber.<sup>32</sup>

While it is unlikely that the technological uses outlined here would implicate the Wiretap Act, many uses could leave businesses in possession of information

covered by the SCA. Businesses thus should carefully evaluate any disclosure of such information, particularly if they are disclosing the information to a governmental entity. As previously noted, businesses are not barred from disclosing customer records to private parties as long as those records do not reflect the content of communications.<sup>33</sup>

#### *The Federal Trade Commission Act*

Section 5 of the Federal Trade Commission Act (FTC Act) prohibits “unfair or deceptive acts or practices in or affecting commerce,”<sup>34</sup> and the FTC has frequently taken enforcement action for various “deceptive” or “unfair” acts or practices related to data privacy and security. For instance, the FTC has brought enforcement actions against companies for failing to reasonably secure personal information, adequately disclose data collection practices, and operate in accordance with the representations made in their privacy policies.<sup>35</sup>

Because all of the COVID-19 technologies identified previously could implicate any of these areas, businesses should review their data practices and privacy policies and notices with respect to such technologies to ensure compliance with FTC standards and guidance.

#### *The Health Insurance Portability and Accountability Act of 1996 and Health Information Technology for Economic and Clinical Health Act of 2009*

Health-related data is, of course, at the core of many of the forms of data collection and use discussed above. A key initial question is whether the data that businesses collect or process is protected under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 (together, with their implementing regulations, HIPAA) and state laws relating to health data, which are discussed further below.

Importantly, HIPAA does not apply to all health data; instead, it applies only to protected health information (PHI) held by either “covered entities” or “business associates.” Covered entities include health-care providers, health plans (including employer health plans), and healthcare clearinghouses that engage in certain electronic transactions involving PHI.<sup>36</sup> Business associates are entities with which a covered entity contracts to perform a function for or on behalf of the covered entity that involves PHI, or to provide services to a covered entity that involve the use or disclosure of PHI.<sup>37</sup>

If HIPAA does apply, its compliance requirements can be substantial. HIPAA requires covered entities to adhere to certain privacy standards, including limitations on disclosure, absent authorization. HIPAA also requires covered entities and their business associates to engage in certain security measures to ensure PHI is properly protected.

The U.S. Department of Health and Human Services has announced that it intends to exercise enforcement discretion with respect to limited aspects of HIPAA, including with respect to certain uses of telehealth, in light of the pandemic.<sup>38</sup>

### **State Laws and Regulations**

Every state has numerous laws and regulations potentially applicable to the use of COVID-19 technologies. Many of these laws mirror federal laws outlined above; for example, every state or nearly every state has a state-constitution equivalent to the Fourth Amendment, a Wiretap Act analogue (with many also having an SCA analogue), and an “unfair and deceptive practices” statute mirroring the FTC Act. But there are also unique state laws that have no exact federal analogue, with key examples of such state laws as follows.

- First, as mentioned previously, many states have medical privacy laws, which may be different in material respects from HIPAA. Although many of these laws do not apply to employers performing return-to-work health screenings for their employees, they do contain provisions that must be tracked on a state-by-state level, including such provisions as those contained in the Alabama and Illinois codes, which mandate information security protections for health information.<sup>39</sup>
- Second, state laws may require businesses to disclose their collection and use practices and also grant consumers rights with respect to their personal information. The most important of these is the California Consumer Privacy Act of 2018 (CCPA), which gives California residents important rights regarding their “personal information.”<sup>40</sup> Among other things, the CCPA requires business to provide consumers with the rights to access and delete their personal information, as well as opt out of its “sale.”<sup>41</sup> The CCPA also requires businesses to detail privacy practices in a publicly accessible privacy policy; the personal information that they collect, use, store, and share; and how consumers may exercise their CCPA rights.<sup>42</sup>
- Third, as particularly relevant to contact tracing applications with a geolocation component, several states have laws that regulate location tracking of individuals.<sup>43</sup>
- Fourth, certain states, such as Illinois, Texas, and Washington, have laws that specifically regulate the collection of biometric information.<sup>44</sup> These laws may require businesses to obtain explicit consent to collect such information, and the Illinois Biometric Information Privacy Act (BIPA) provides a private right of action with statutory damages.<sup>45</sup>
- Fifth, it is also important to note that all states grant their governors and/or public health

authorities emergency powers, which may allow them to suspend otherwise operative laws during a public health crisis or to implement emergency regulations.<sup>46</sup> It is thus important to be aware of any invocation of these authorities, particularly if a business is working with the government.

The key point is that businesses should consider the legal regime of each applicable state based on the locations of their operations, employees, and consumers.

### **International Regulators and Governments**

Finally, if operating internationally, a business should consider the laws, regulations, and standards of relevant jurisdictions, as well as regulator guidance and statements related to the use of technologies in the fight against COVID-19. Key international regulators may include the European Data Protection Board and the United Kingdom Information Commissioner’s Office (ICO). Both of these regulators have evaluated data processing and sharing practices relevant to the COVID-19 response.<sup>47</sup> Additionally, the ICO continues to issue public assessments of COVID-19 technologies and the national contact tracing system sponsored by the British government and health authorities.<sup>48</sup>

### **How COVID-19 Might Change Data Privacy and Security Law**

The COVID-19 pandemic raises numerous privacy challenges. Asymptomatic spread requires prophylactic measures; the wide range of potential symptoms associated with COVID-19 makes identifying cases of concern more difficult; and employers, schools, and other institutions may be placed in roles that they do not ordinarily play in order to keep spaces safe.

Although numerous privacy laws potentially apply to the use of mobile technologies to combat COVID-19, these laws were not designed to apply particularly to the use of information to fight a public health crisis of the current magnitude. This fact has led to concerns from both sides of the privacy spectrum. Privacy advocates fear that the existing laws do not sufficiently protect civil liberties during this time of crisis, while others believe that the existing laws may restrict too much activity that would help combat the virus’s spread. It is thus unsurprising that legislators and regulators are considering whether new laws and regulations are necessary to specifically address how governments and businesses may use data during the pandemic.

Two draft bills recently introduced in Congress may serve as a good indication of the issues central to the current debate on COVID-19 privacy legislation. First, the COVID-19 Consumer Data Protection Act (CDPA) was introduced by Senate Republicans on May 7, and second, the Public Health Emergency Privacy Act (PHEPA) was introduced by Senate Democrats on May 14. The table below provides several key elements of these bills.

	CDPA	PHEPA
<b>Scope</b>	<p>Applies to a “covered entity,” defined to include any organization subject to the FTC Act, as well as any common carrier or nonprofit organization defined per federal law.</p> <p>Includes exemption for service providers.</p>	<p>Applies to a “Covered Organization,” which broadly includes any person subject to de minimis and household exceptions, including any governmental entity that is not a public health authority.</p> <p>Includes exemption for service providers and healthcare providers.</p>
<b>Authorized Purposes for Processing</b>	<p>Prohibits covered entities from collecting, processing, or transferring data of an individual unless (1) the covered entity is processing the data for a “covered purpose” or (2) the covered entity satisfies specified notice and consent protocols.</p> <p>Defines <i>covered purpose</i> to include (i) tracking the spread, signs, or symptoms of COVID-19; (ii) measuring compliance with social distancing guidelines and requirements; and (iii) contact tracing of COVID-19 cases. Explicitly prohibits certain types of data processing, including those related to (i) commercial advertising; (ii) marketing, soliciting, or selling activities in targeted areas such as housing, education, and finance; and (iii) discriminating or disadvantaging an individual in a place of public accommodation.</p>	<p>Requires processing only be performed for a good faith public health purpose and, like the CDPA bill, permits processing if it is otherwise required by law.</p> <p>Does not include a “notice and consent” safe harbor but, rather, requires that consent be obtained in all instances in which emergency health data is collected, unless a particular exception applies, with such exceptions limited to purposes related to guarding against fraud, protecting against data breaches, and adhering to legal requirements.</p>
<b>Notice Obligations</b>	<p>Requires covered entity to publish a special public-facing privacy policy within 14 days of the law’s enactment, disclosing the categories of recipients who receive covered data and the entity’s data retention and data security practices.</p> <p>Further requires entities to issue a report within 30 days of the law’s enactment, (i) stating the number of individuals whose covered data has been collected, and (ii) describing the categories, purposes, and recipients of such covered data.</p>	<p>Contains requirements similar to the CDPA, although (i) there is no specific requirement that the privacy notice be public-facing; (ii) the privacy policy must include a summary of individual rights; and (iii) the public reporting obligation only applies to entities that collect the data of 100,000 individuals or more, but it requires that such organizations issue a public report every 90 days, rather than just once.</p>
<b>Affirmative Private Rights and Obligations</b>	<p>Requires covered entities to (i) provide an effective opt-out mechanism to revoke consent and otherwise restrict processing of covered data; (ii) delete all covered data when it is no longer being used; (iii) ensure the accuracy of covered data and provide a mechanism for individuals to report inaccuracies; (iv) implement data-minimization processes in accordance with guidelines to be issued by the FTC; and (v) establish reasonable administrative, technical, and physical data security policies and practices to protect covered data.</p>	<p>Apart from a specific data-minimization obligation, contains the other privacy rights and obligations found in the CDPA: an opt-out mechanism, data destruction requirement, data accuracy obligation, and a mandate to establish reasonable safeguards for the protection of emergency health data.</p> <p>Also requires reasonable safeguards to protect against discrimination and to ensure that data is disclosed to governments only for public health reasons.</p>
<b>Enforcement</b>	<p>Delegates primary enforcement authority to the FTC under section 5 of the FTC Act; secondary enforcement authority given to state attorneys general.</p>	<p>Delegates primary enforcement authority to the FTC under section 5 of the FTC Act; secondary enforcement authority given to state attorneys general.</p> <p>Includes private right of action with maximum statutory damages of \$5,000 per violation, as well as reasonable attorney fees and other fees that the court deems appropriate.</p>

While these two bills are not likely to be the last word on this subject, as this table shows, there is substantial overlap between these two bills—overlap that provides a good overview of the areas where legislators believe that existing law should be supplemented. These areas include gathering health information for public health purposes to combat the COVID-19 pandemic while requiring additional protections—such as use restrictions, data-minimization requirements, retention limits, and individual rights protections—to ensure that the data are used properly and for more targeted purposes.<sup>49</sup>

### Checklist of Privacy and Security Considerations for COVID-19 Technologies

As the foregoing discussion demonstrates, the technological landscape for using mobile applications to fight COVID-19 is constantly evolving and legally dense. While this article does not seek to comment on or evaluate any particular application of technology, below please find a basic checklist of privacy-related considerations for use of these technologies.<sup>50</sup>

- Take privacy into account when developing plans for using the mobile technologies by, for example, using “privacy by design” principles to develop the technology; ensuring that data collection, particularly of sensitive information (such as biometrics), is necessary and proportionate, including by evaluating whether it would be possible to use de-identified or aggregate data; procuring affirmative user consent; and conducting a privacy impact assessment of the plan.
- Assess what legal requirements apply, including by evaluating the jurisdictions in which the technology will be used (to see what international, federal, state, and local laws might apply); the types of entities that will be gathering or using the information and the type of information that will be gathered (to determine the applicability of any sector-specific or category-specific regimes, such as HIPAA); and whether any relevant regulators have recently issued guidance on how those rules apply with respect to COVID-19.
- Review disclosures regarding data collection, use, and privacy practices to ensure that they are consistent with any legal requirements and provide sufficient and accurate information about how data will be collected and used to combat COVID-19. Consider whether additional communications to data subjects about the technology used or the data collected are helpful and appropriate.
- Review existing information security policies and procedures to ensure that they are consistent with applicable regulations and guidance and contain appropriate security and handling protections.
- Establish appropriate and lawful protocols for data retention, including with respect to its destruction after its retention is no longer necessary and/or the COVID-19 pandemic has ended.
- Evaluate relevant contracts with suppliers, vendors, and clients to ensure that privacy and information security issues, and the allocation of liability among the parties, are appropriately addressed.
- Review existing or, if necessary, establish new governance structures and monitoring protocols for evaluating and auditing the effectiveness of the technological use and privacy safeguards, as well as compliance with any internal policies or procedures.

A current legal obligation may not be linked to each of these considerations. However, by entertaining these considerations, businesses could reduce other privacy and reputational risks that might arise. And, importantly, by incorporating these suggestions, businesses will be better prepared in the event that such considerations do become applicable—a likely occurrence as the law in this area is evolving rapidly. 

### Endnotes

1. *Interim Clinical Guidance for Management of Patients with Confirmed Coronavirus Disease (COVID-19)*, CTRS. FOR DISEASE CONTROL & PREVENTION (updated July 22, 2020).
2. See, e.g., Matt Richtel, *Contact Tracing with Your Phone: It's Easier but There Are Tradeoffs*, N.Y. TIMES (updated July 20, 2020), <https://www.nytimes.com/2020/06/03/health/coronavirus-contact-tracing-apps.html>
3. *Digital Contact Tracing Tools for COVID-19*, CTRS. FOR DISEASE CONTROL & PREVENTION (updated May 26, 2020).
4. *Id.*
5. See, e.g., *Help Speed Up Contact Tracing with TraceTogether*, SINGAPORE GOV'T AGENCY (Mar. 21, 2020), <https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogogether>. Based on a survey of online sources, the list of countries with contact tracing technologies at the national, state, or province level includes Australia, Azerbaijan, Bahrain, Bangladesh, Canada, China, Colombia, Czech Republic, Denmark, France, Germany, Ghana, Hungary, Iceland, India, Israel, Italy, Japan, Jordan, Latvia, Malaysia, New Zealand, North Macedonia, Norway, Qatar, Saudi Arabia, Singapore, Spain, and Switzerland.
6. *Digital Contact Tracing Tools for COVID-19*, *supra* note 3.
7. New York State Contact Tracing, STATE OF N.Y., <https://coronavirus.health.ny.gov/new-york-state-contact-tracing> (last visited July 15, 2020).
8. Several states, notably South Dakota and Utah, chose to deploy their own contact tracing apps. David Ingram, *Coronavirus Contact Tracing Apps Were Tech's Chance to Step Up. They Haven't*, NBC NEWS (June 12, 2020), <https://www.nbcnews.com/tech/tech-news/coronavirus-contact-tracing-apps-were-tech-s-chance-step-they-n1230211>. Other states—Alabama, North Dakota (CARE19 app), and South

Carolina (SC-Safer-Together app)—have said that they will use existing technology in their contact tracing apps. Kif Leswing, *Three States Will Use Apple-Google Contact Tracing Technology for Virus Tracking Apps*, CNBC NEWS (May 20, 2020), <https://www.cnbc.com/2020/05/20/three-states-commit-to-apple-google-technology-for-virus-tracking-apps.html>.

9. See, e.g., Amit Syal & Sam Burdette, *Campus Reentry Update: University of Arizona Begins Testing Phase for New Contact Tracing App*, DAILY WILDCAT (June 18, 2020), <https://www.wildcat.arizona.edu/article/2020/06/sc-tracing-app>; Amy Wadas, *Pennsylvania Health Department Working to Hire More Coronavirus Contact Tracers*, CBS PITTSBURGH (June 8, 2020), <https://pittsburgh.cbslocal.com/2020/06/08/covid-19-contact-tracing-hiring-in-pennsylvania/>; *Case Investigations and Contact Tracing*, WASH. STATE DEP'T OF HEALTH (2020), <https://www.doh.wa.gov/Emergencies/NovelCoronavirusOutbreak2020COVID19/CaseInvestigationsandContactTracing>; David Gutman, *Why You Might Now Get a Phone Call to Tell You You've Been Exposed to the Coronavirus*, SEATTLE TIMES (updated May 21, 2020), <https://www.seattletimes.com/seattle-news/health/washington-trains-more-than-2100-callers-as-it-expands-contact-tracing-to-battle-coronavirus/>; Frank Witsil, *New Contracts Restart Volunteer Contact Tracing, but Epidemiologist Takes Aim at Effort*, DETROIT FREE PRESS (updated May 14, 2020), <https://www.freep.com/story/news/local/michigan/2020/05/12/volunteer-contact-tracing-michigan-rock-connections-deloitte/3107351001>; Kelly House & Riley Beggin, *Michigan Launches Coronavirus Contact Tracing. Here's What You Need to Know*, BRIDGE MAG. (May 9, 2020), <https://www.bridgemi.com/michigan-health-watch/michigan-launches-coronavirus-contact-tracing-heres-what-you-need-know/>; *Maine Expands Contact Tracing to Limit the Spread of COVID-19*, STATE OF ME. OFFICE OF GOVERNOR JANET T. MILLS (May 26, 2020), <https://www.maine.gov/governor/mills/news/maine-expands-contact-tracing-limit-spread-covid-19-2020-05-26>.

10. GovTech, *Responding to COVID-19 with Tech*, SINGAPORE GOV'T AGENCY (last updated July 6, 2020), <https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech> (providing overview of SafeEntry, “national digital check-in system” that “is used for contact tracing and data verification through (1) scanning of QR codes or (2) scanning of [National Registration Identity Cards] at hotspots and high traffic locations”); *NZ COVID Tracer QR Codes*, GOV'T OF N.Z. MINISTRY OF HEALTH (updated Aug. 27, 2020), <https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-novel-coronavirus-resources-and-tools/nz-covid-tracer-app/nz-covid-tracer-qr-codes>.

11. Victoria Kim, *Welcome, Please Scan Your QR Code: In South Korea, a High-Tech Registry for Nightlife amid Coronavirus*, L.A. TIMES (June 10, 2020), <https://www.latimes.com/world-nation/story/2020-06-10/welcome-please-scan-your-qr-code-in-south-korea-a-high-tech-registry-for-nightlife-amid-coronavirus>.

12. U.S. Mission Korea, *Health and Travel Alert—U.S. Embassy Seoul, Republic of Korea*, U.S. EMBASSY & CONSULATE IN THE REPUBLIC OF KOR. (June 12, 2020), <https://kr.usembassy.gov/061220-health-and-travel-alert-u-s-embassy-seoul-republic-of-korea>.

gov/061220-health-and-travel-alert-u-s-embassy-seoul-republic-of-korea.

13. See, e.g., Natasha Singer, *Employers Rush to Adopt Virus Screening. The Tools May Not Help Much*, N.Y. TIMES (May 11, 2020), <https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html>.

14. For example, some businesses are deploying mobile technologies and wearables to monitor for COVID-19 symptoms and enhance their ability to identify potential cases and limit exposure to the virus. See, e.g., Geoffrey A. Fowler, *Wearable Tech Can Spot Coronavirus Symptoms Before You Even Realize You're Sick*, WASH. POST (May 28, 2020), <https://www.washingtonpost.com/technology/2020/05/28/wearable-coronavirus-detect>. Businesses are also deploying technologies such as temperature-checking applications and contactless temperature-checking kiosks. See, e.g., Sarah Whitten, *Contactless Temperature-Checking Kiosks Are Coming, Here's What It's Like to Use One*, CNBC (May 21, 2020), <https://www.cnbc.com/2020/05/21/contactless-temperature-checking-kiosks-are-coming-amid-coronavirus.html>.

15. See, e.g., *COVID-19: RESTART Guidance for Businesses*, GOV'T OF N.Y. CITY HEALTH (July 2020), <https://www1.nyc.gov/site/doh/covid/covid-19-businesses-and-facilities.page>; *Reopening New York City: Frequently Asked Questions (FAQs)*, GOV'T OF N.Y. CITY HEALTH (updated Aug. 21, 2020), <https://www1.nyc.gov/assets/doh/downloads/pdf/imm/covid-19-reopening-nyc-faq.pdf>; *Reopening New York—Office-Based Work Guidelines for Employers and Employees*, GOVERNOR OF N.Y. (June 2020), <https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/OfficesSummaryGuidelines.pdf>; *Reopening NYC Phase 2: Offices*, GOV'T OF N.Y. CITY (June 17, 2020), <https://www1.nyc.gov/assets/coronavirus/downloads/phase2/offices.pdf>; *Reopening New York City: Frequently Asked Questions—What Offices Need to Know*, GOV'T OF N.Y. CITY (updated Aug. 17, 2020), <https://www1.nyc.gov/assets/doh/downloads/pdf/imm/covid-19-reopening-offices-guidance.pdf>.

16. See OSHA, INTERIM ENFORCEMENT RESPONSE PLAN FOR CORONAVIRUS DISEASE 2019 (COVID-19), U.S. DEP'T OF LAB. (April 13, 2020), [www.osha.gov/memos/2020-04-13/interim-enforcement-response-plan-coronavirus-disease-2019-covid-19](http://www.osha.gov/memos/2020-04-13/interim-enforcement-response-plan-coronavirus-disease-2019-covid-19); OSHA, UPDATED INTERIM ENFORCEMENT RESPONSE PLAN FOR CORONAVIRUS DISEASE 2019 (COVID-19), U.S. DEP'T OF LAB. (May 19, 2020), <https://www.osha.gov/memos/2020-05-19/updated-interim-enforcement-response-plan-coronavirus-disease-2019-covid-19>.

17. *Coronavirus and COVID-19*, U.S. EQUAL EMP'T OPPORTUNITY COMM'N, <https://www.eeoc.gov/coronavirus> (last visited July 6, 2020); U.S. EQUAL EMP'T OPPORTUNITY COMM'N, WHAT YOU SHOULD KNOW ABOUT COVID-19 AND THE ADA, THE REHABILITATION ACT, AND OTHER EEO LAWS (June 17, 2020), <https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws>.

18. See, e.g., U.S. EQUAL EMP'T OPPORTUNITY COMM'N, PANDEMIC PREPAREDNESS IN THE WORKPLACE AND THE AMERICANS WITH DISABILITIES ACT (rev. Mar. 21, 2020), <https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities->

act; U.S. EQUAL EMP'T OPPORTUNITY COMM'N, WHAT YOU SHOULD KNOW ABOUT COVID-19, *supra* note 17.

19. Elisa Jillson, *Privacy During Coronavirus*, FTC BUS. BLOG (June 19, 2020, 10:32 AM), <https://www.ftc.gov/news-events/blogs/business-blog/2020/06/privacy-during-coronavirus> (citing the FTC's recent enforcement action against smart-lock manufacturer Tapplock as an example of a business that "rush[ed] to get a product to market without considering privacy and security issues").

20. FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15 (Feb. 2013) ("[C]onsistent with the Commission's Privacy Report, before allowing apps to access sensitive content through APIs, such as geolocation information, platforms should provide a just-in-time disclosure of that fact and obtain affirmative express consent from consumers." (citations omitted)).

21. *Id.*

22. The Privacy Act regulates federal agencies' collection, use, and sharing of systems of records that store personal information, not only providing individuals with a way to access and correct information that an agency maintains about the individual, but also mandating certain restrictions for how federal agencies manage and disclose that information. *See* 5 U.S.C. § 552a(b)–(e) (2012). FOIA permits members of the public to submit formal requests in order to access federal executive agencies' records, although certain exceptions do apply. *See id.* § 552. The important point here is that if businesses are working with the government, it is possible that either or both of these laws could apply in certain circumstances.

23. U. S. CONST. amend. IV.

24. *See* Katz v. United States, 389 U.S. 347 (1967).

25. *See, e.g.,* Carpenter v. United States, 138 S. Ct. 2206 (2018) (finding that the Fourth Amendment protects an individual's historical cell-site locational information (CSLI) even if the information is in the possession of a wireless carrier). For a more detailed analysis of *Carpenter* and its potential implications for Fourth Amendment jurisprudence, see Christopher C. Fonzone, Kate Heinzelman & Michael R. Roberts, *Carpenter and Everything After: The Supreme Court Nudges the Fourth Amendment into the Information Age*, 58(4) A.B.A. INFRASTRUCTURE & REGULATED INDUS. (Summer 2019).

26. *See, e.g.,* Ferguson v. City of Charleston, 532 U.S. 67, 74 (2001) (applying "special needs" doctrine and upholding warrantless search to "serve non-law-enforcement ends").

27. *See, e.g.,* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (applying special needs doctrine and finding that Michigan police sobriety checkpoints were reasonable searches and did not violate the Fourth Amendment).

28. Businesses should understand that de-identified or aggregated data could be reidentified, and, in certain circumstances, the Fourth Amendment could be applicable to such reidentified data.

29. Depending on the technology platform, the intended users of the technology, and the types of personal information collected, other applicable laws may include the Communications Act, 47 U.S.C. § 222 *et seq.*; Family Educational Rights

and Privacy Act (FERPA), 20 U.S.C. § 1232g *et seq.*; Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq.*; and Federal Food, Drug, and Cosmetic Act (FDCA), 21 U.S.C. § 301 *et seq.*

30. 18 U.S.C. § 2511.

31. *Id.* § 2702(a)(1)–(2).

32. *Id.* § 2702(a)(3).

33. *Id.* § 2702(c)(6).

34. 15 U.S.C. § 45(a)(1).

35. *See* FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 3 (June 18, 2020) (citing enforcement actions and settlements, including *In re Info-Trax Systems, L.C.*, FTC File No. 162 3130, Docket No. C-4696 (2019), in which the FTC alleged that the company and its former CEO failed to use reasonable security measures to safeguard clients' personal information).

36. *Id.* § 160.102.

37. *Id.* § 160.103.

38. *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, U.S. DEPT. OF HEALTH & HUMAN SERV., <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html> (Mar. 20, 2020).

39. *See, e.g.,* ALA. CODE § 8-38-2(6); 815 ILL. COMP. STAT. 530/5.

40. CAL. CIV. CODE § 1798.100 *et seq.*

41. *See id.* §§ 1798.100(d), 1798.105, 1798.110.

42. *Id.* § 1798.130 *et seq.*

43. CAL. PENAL CODE § 637.7 *et seq.* (prohibiting any person or entity in California from using "an electronic device to determine the location or movement of a person," absent several exemptions including "the lawful use of an electronic tracking device by a law enforcement agency").

44. *See* 740 ILL. COMP. STAT. 14; TEX. BUS. & COM. CODE ANN. § 503.001; WASH. REV. CODE ANN. §19.375.020.

45. *See* 740 ILL. COMP. STAT. 14/20.

46. *See* Benjamin Della Rocca et al., *State Emergency Authorities to Address COVID-19*, LAWFARE (May 4, 2020, 3:03 PM), <https://www.lawfareblog.com/state-emergency-authorities-address-covid-19> (providing an overview of state emergency authorities available to governors in their response to the pandemic).

47. *See* EUROPEAN DATA PROT. BD., GUIDELINES 04/2020 ON THE USE OF LOCATION DATA AND CONTACT TRACING TOOLS IN THE CONTEXT OF THE COVID-19 OUTBREAK (Apr. 21, 2020), [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_20200420\\_contact\\_tracing\\_covid\\_with\\_annex\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf) (providing guidance on the use of location data and contact tracing tools related to COVID-19).

48. *See, e.g.,* *Collecting Customer and Visitor Details for Contact Tracing*, INFO. COMM'RS OFFICE, <https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/collecting-customer-and-visitor-details-for-contact-tracing> (last visited July 7, 2020); *Contact Tracing—Protecting Customer and Visitor Details*, INFO. COMM'RS OFFICE, <http://ico.org.uk/global/data-protection-and->

coronavirus-information-hub/contact-tracing-protecting-customer-and-visitor-details (last visited July 7, 2020); Dep't of Health & Soc. Care, *Maintaining Records of Staff, Customers and Visitors to Support NHS Test and Trace*, GOV.UK (updated Aug. 28, 2020), <https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace>; Elizabeth Denham, *Blog: Combatting COVID-19 Through Data: Some Considerations for Privacy*, INFO. COMM'RS OFFICE (Apr. 17, 2020), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combating-covid-19-through-data-some-considerations-for-privacy>; INFO. COMM'RS OFFICE, INFORMATION COMMISSIONER'S OPINION: APPLE AND GOOGLE JOINT INITIATIVE ON COVID-19 CONTACT TRACING TECHNOLOGY (Apr. 17, 2020), <https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf>; Paul Arnold, *Statement on the Publication of ICO Guidance to Businesses Collecting Personal Data for Contact Tracing*, INFO. COMM'RS OFFICE, <http://ico.org.uk/>

global/data-protection-and-coronavirus-information-hub/statement-on-the-publication-of-ico-guidance-to-businesses-collecting-personal-data-for-contact-tracing (last visited July 7, 2020).

49. Of course, just like the ongoing debates over comprehensive federal privacy legislation, there are also divergent views on certain issues. See, e.g., Cameron Kerry, *Keeping the Fires Burning for Federal Privacy Legislation*, IAPP PRIVACY PERSP. (June 3, 2020), <https://iapp.org/news/a/keeping-the-fires-burning-for-federal-privacy-legislation> (observing that, similar to prior congressional efforts to pass privacy legislation, the CDPA and PHEPA “both display the same gulf on preemption and private right of action”).

50. A number of regulators and commentators have provided similar sets of considerations that companies should take into account in addressing this fast-moving area. For a good example, see Denham, *supra* note 48.

## Managing Critical Infrastructure During the COVID-19 Pandemic

*continued from page 1*

creates the potential for groups of essential workers to become infected at the same time, potentially threatening continuous operations of critical infrastructure functions.<sup>3</sup>

Accordingly, critical infrastructure companies and other essential businesses need to take measures and develop strategies to monitor and manage the risk of exposure to the virus that causes COVID-19 within their workforces.<sup>4</sup> They also should develop contingency plans that can be implemented swiftly if an outbreak occurs within the essential employee population. These response measures require substantial advance planning because a range of medical, legal, and other considerations must be coordinated among company management, legal and medical advisors, and critical workforce personnel.

### COVID-19 Disease Characteristics

Due to the novel and emergent nature of COVID-19, employers must establish a basic understanding about the disease in order to develop appropriate measures tailored to their company's needs. While the medical community's understanding of the virus is still evolving, some important points of consensus relevant to critical infrastructure workforce management have emerged.

First, COVID-19 is highly transmissible and spreads more efficiently than many other respiratory diseases.<sup>5</sup> This is due, in part, to the relatively long incubation period and duration of asymptomatic transmission seen with COVID-19. In addition, the multiple modes of transmission of COVID-19 create challenges for controlling the spread in many workplace environments.<sup>6</sup>

Transmission occurs primarily through direct, indirect, or close contact with an infected individual through droplets created by coughing, sneezing, or talking. Droplets expelled by an infected individual can also contaminate surfaces and objects, leading to fomite transmission to other individuals. Researchers are also studying the possibility that COVID-19 can be transmitted by smaller, aerosolized particles that have the potential to remain in the air longer and to travel farther than with droplet transmission.<sup>7</sup>

Second, while the lethality of COVID-19 has been difficult to determine with precision, due to its novelty and the lack of sufficient testing to determine the total number of infections, it is significantly more deadly than the seasonal flu. Current estimates suggest that COVID-19 has an overall fatality rate of between 0.5 percent and 1 percent, which is 5–10 times higher than the seasonal flu with its average fatality rate of approximately 0.1 percent.<sup>8</sup> Fatality rates have been observed to increase with age, including in working-age populations of those 45–54 years old and those 55–64 years old.<sup>9</sup> Furthermore, while the vast majority of those who contract COVID-19 survive the disease, evidence suggests that it can have significant and lasting health impacts on those who contract it.<sup>10</sup>

Third, while some clinical trials have shown promise, development of a safe and effective vaccine remains elusive. Even with expedited development and approval protocols, the likely timelines for testing, development, and deployment of a vaccine will require critical infrastructure companies to continue managing through the pandemic for the foreseeable future.

### **Developing Workforce Management Protocols**

Current understanding of COVID-19 points to a range of measures that companies can take to protect essential employees and support continued business operations. These risk-based approaches vary depending on the nature of the organization, as there is no one-size-fits-all solution. The expense and difficulty of implementing safeguards also vary, depending on the measures chosen.

Factors to consider in developing a COVID-19 workforce management program to ensure continuity of essential operations include: the minimum number of employees needed to operate mission-critical functions, the number of trained and licensed personnel qualified to conduct those functions, the ability to isolate or distance essential employees from nonessential personnel, and opportunities for early detection of infections within the workforce and effective response measures.

Assessment of these and other company-specific factors can help guide the choice of measures that will best support business continuity for a critical workforce. Basic, straightforward measures focused on vigilant workplace and at-home hygiene, consistent use of masks, and disciplined social distancing, for example, may be sufficient for organizations with large workforce reserves and controlled-access facilities, while more extensive measures may be necessary for those with less margin for error. Legal considerations and the extent of medical supervision required also vary based on the measures taken and should be carefully considered when developing workforce management protocols.

### **Basic Protective Measures**

Basic protective measures are widely familiar by now. These require minimal effort and expense but can provide meaningful safeguards against exposure to and transmission of the COVID-19 virus. Basic protective measures include symptom monitoring, workplace social distancing and hygiene, education, reduced employee density and cohort staffing, and off-site/off-shift measures.

#### *Symptom Monitoring*

Daily temperature checks and symptom monitoring can help identify potentially infected individuals and prevent spread of disease to other employees, though the prevalence of asymptomatic transmission strongly indicates that symptom monitoring should be combined with other measures. The details of such a program should be developed with input from medical advisers and labor and employment counsel.

#### *Workplace Social Distancing and Hygiene*

These measures include social distancing practices within the workplace, mandatory masking requirements and use of other personal protective equipment (PPE) where appropriate, good personal hygiene

practices, and enhanced cleaning and disinfecting in the workplace.<sup>11</sup>

#### *Education*

While information about COVID-19 is readily available, education still plays an important role in effective workforce management. Effective education programs, with a focus not only on the “what” but also the “why,” can improve employee compliance both on and off the job. Written materials are important, but they are most effective when supplemented by other modes of communication, including briefings from management or expert advisers. Video training modules can provide further detail to reinforce and explain written policies and guidance. Live, interactive formats can facilitate deeper understanding through question-and-answer sessions and provide valuable insights into what measures work best in practice.

#### *Reduced Employee Density and Cohort Staffing*

Approaches to reducing employee density and the risk of spread of COVID-19 among employees include returning employees in stages, staggering days or shifts on-site, dividing returning employees into groups and minimizing interaction among different groups (cohort staffing), and physically separating critical workforce from the general employee population. These measures can help limit the spread of infection in the event of COVID-19 cases within the workplace. Effective cohort staffing often requires changes to current practices and can be supported through a tailored testing program, as discussed further below.

#### *Off-Site/Off-Shift Measures*

Measures implemented in the workplace are an important first step, but most employees spend between half to two-thirds of each workday outside the workplace. It is important for critical infrastructure companies to take steps to promote employee behavior off the job that reduces the risk of infection that could lead to an outbreak on the job.

### **Advanced Protective Measures**

Critical infrastructure companies may also need to consider more advanced protective measures, especially for essential personnel. These are generally more complex to design and implement, and they present logistical, medical, and legal considerations that need to be addressed.

These measures can be divided into two categories: those implemented on-site at the workplace and those implemented off-site, including within the employee’s household. Some of these measures may call for medical consultation or supervision. Advanced measures may also implicate important legal considerations, some of which are addressed below.

Advanced measures include medical screening, workspace alterations, COVID-19 testing, preventative isolation, isolation from exposed or potentially sick family members, and on-site sequestration.

#### *Medical Screening*

A screening questionnaire to assess individual employee risk factors for exposure outside the workplace can be used as a tool to guide formation of employee cohort groups. While potentially useful, this presents legal issues that should be evaluated by labor and employment counsel.

#### *Workspace Alterations*

Changes to the physical workspace can also provide potential benefits. HVAC system upgrades such as high-efficiency particulate air (HEPA) filtration and UV-C ultraviolet light treatment systems may help reduce the likelihood of transmission within the workplace.<sup>12</sup> Companies also should consider using clear plastic shields or other physical barriers between employees; restricting access to spaces where mission-critical employees work; and reducing maximum-occupancy limits for shared workspaces, elevators, break rooms, and other common areas.

#### *COVID-19 Testing*

Tailored use of COVID-19 testing is an important tool for critical infrastructure workforce management. Two primary options are available to employers to screen for infected individuals: laboratory-based testing and point-of-care testing. These tests use different technologies, and they offer different advantages and disadvantages. Both are used to identify an active infection and are distinguishable from antibody tests, which can indicate a prior infection.

Laboratory-based testing uses a nasal/throat swab or saliva sample that is collected at an employer's location, at a healthcare provider's facility, or by telemedicine appointment and then transported to a laboratory for analysis, with results generally available within 48 to 72 hours. The laboratory-based COVID-19 test identifies genetic material of the virus using a reverse transcription polymerase chain reaction (PCR) process. Saliva-based samples can be collected remotely by a telemedicine appointment, allowing for sample collection at home. When administered properly, PCR tests are highly accurate.<sup>13</sup>

Point-of-care testing uses a nasal or throat swab taken by a healthcare provider at the employer's location or at a healthcare provider's facility using a portable diagnostic machine that provides results within 15–20 minutes. Point-of-care testing uses one of two approaches to identify COVID-19 infection: antigen testing to detect proteins on the surface of the virus, or a real-time variant of the traditional PCR process that identifies genetic material of the virus. Recent findings indicate a high level of accuracy with the latest point-of-care testing technologies.<sup>14</sup>

The best choice of a testing method depends on how testing will be integrated into a workforce management program. In some cases, more than one method may be indicated. Point-of-care tests are generally less expensive than laboratory-based PCR tests, and the rapid results offer a clear advantage, though they have a slightly lower accuracy rate.<sup>15</sup> Laboratory tests are slightly more accurate, and the ability to provide a sample by telemedicine visit is a benefit in some circumstances, but the tests are somewhat more expensive and results generally take 48–72 hours.

The Food and Drug Administration has approved “batch testing” to allow multiple individuals to be tested together with a combined sample, thereby reducing costs, though this practice introduces an increased likelihood of false negative test results due to sample dilution. For this reason, batch testing is still in a developmental stage and is not widely used in practice.

COVID-19 testing can be incorporated into a comprehensive workforce management program in a number of ways. Some employers may elect to test all employees before they return to work in order to establish a baseline, though this provides only a single snapshot in time and does not substitute for ongoing measures. Testing can also be used in conjunction with contact tracing to facilitate case management following a known or suspected exposure, and it may facilitate more rapid return to work for individuals who have been confirmed negative.<sup>16</sup> In addition, COVID-19 tests can be used to facilitate in-person meetings, to periodically screen mission-critical personnel required to work on-site, to check employees returning from travel or other high-risk scenarios, to conduct point-prevalence survey (random sample) testing, and in other applications that can be designed to meet individual organizational needs with the assistance of a medical advisor.<sup>17</sup>

Companies incorporating testing into their COVID-19 workforce management programs should consider contracting with a private provider offering testing to ensure consistent availability and timely results. These providers have experience working with a number of industrial applications and can tailor a testing program to a company's specific needs and budget.

#### *Preventative Self-Isolation*

This measure ranges from relatively minor steps, such as recommending that essential employees limit activities outside their household to the extent possible, to more aggressive steps, such as recommending that essential employees self-isolate within their households depending on potential exposure risk factors present.

#### *Isolation from Exposed or Potentially Sick Family Members*

In addition to education and guidance regarding measures to minimize contact with family members who have potentially been exposed or who exhibit possible

symptoms, employers should consider providing temporary alternative housing arrangements for critical employees when circumstances warrant.

#### *On-Site Sequestration*

Among advanced measures, one of the most intensive is an on-site sequestration program for mission-critical personnel. Several utilities undertook sequestration programs for control-room operator personnel at the outset of the COVID-19 outbreak.<sup>18</sup> Such programs are inherently complex and resource intensive and need to be designed around the company's particular circumstances, including workforce needs, head count, and the configuration of facilities.

Critical infrastructure companies, in coordination with their medical and legal advisors, will need to identify and address a wide range of potential risk factors and other issues prior to implementation of an on-site sequestration or quarantine program. They will need to consider, for example:

- selection criteria for assessing the technical, managerial, legal, and medical personnel who may participate in quarantine;
- entry and exit protocols, both for quarantine rotations and for unquarantined personnel who require access to quarantined facilities (e.g., for critical maintenance);
- lodging, meals, supplies, and receiving protocols needed in order to provide living accommodations for sequestered personnel;
- medical screenings, supervision, and support needed to conduct initial screenings prior to entry into sequestration, as well as for ongoing screenings, wellness checks, mental health assessments and support, and emergency medical care;
- ongoing preventative measures, including continued social distancing, use of masks, hygiene, cleaning, etc., as well as preparations for self-isolation within quarantine or removal from quarantine if indicated; and
- wage and hour considerations needed to assess compensation and related matters for special staffing protocols to ensure compliance with applicable laws.

#### **Medical Input and Supervision**

Many of the measures described above have medical components or significance. It is advisable for critical infrastructure companies to consult with an appropriate medical advisor to ensure that the measures are consistent with the latest medical guidance and administered or supervised by licensed medical professionals where required.

A medical advisor can provide valuable assistance in the

- initial assessment to identify available resources and determine how best to allocate those

resources to serve program objectives;

- development of detailed program protocols in consultation with management and legal advisors;
- implementation of the program with adjustments as necessary in response to changes in relevant underlying facts (e.g., the availability of testing, staffing rotations, and potential exposures); and
- oversight, periodic review, and adjustment by management of program details in consultation with medical and legal advisors to ensure that the program remains consistent with current information and guidance.

#### **Key Legal Considerations**

Because critical infrastructure companies play a vitally important role in the functioning of society, they cannot cease operations during a crisis, and their mission-critical functions must continue operating even when the general public is subject to stay-at-home orders or similar restrictions. Any critical workforce management program that addresses COVID-19 should be developed with an understanding of relevant legal considerations. Many of the measures that a company may adopt alter the workplace environment or other employment conditions in ways that are legally significant. Below is representative sampling of legal considerations when developing a COVID-19 workforce management program for critical infrastructure.

#### **Labor, Employment, and Compensation**

Labor, employment, and compensation is perhaps the most obvious legal subject matter area implicated by changes to the work environment implemented as part of a pandemic workforce management program. In general, there are three primary authorities that need to be considered when developing such a program.

First, laws and regulations that govern workplace health and safety, including the Occupational Health and Safety Act (OSHA) and the equivalent law in OSHA-state-plan states, apply to the working conditions on-site—thus, employers have a legal obligation to keep employees free from health and safety hazards. Moreover, OSHA requirements extend to the living conditions of any employees quarantined on-site, which means that any on-site quarantine protocol must be developed in a manner consistent with employers' obligations under OSHA and other applicable laws and regulations.

Second, protocols need to be developed in a manner consistent with guidance provided by the Centers for Disease Control (CDC). For example, the CDC has published guidance regarding the circumstances in which a critical infrastructure worker may continue to work in the event of potential exposure to COVID-19,<sup>19</sup> which requires, among other things, that such employees maintain social

distance as work duties permit, be regularly monitored for temperature and other symptoms, and wear a mask at all times for 14 days after their last exposure. A workforce management protocol should include a mechanism that directly or indirectly incorporates such guidance, and that incorporates any changes to such guidance that the CDC and other authorities may implement over time. CDC guidance is not required by law unless it is incorporated into a state's executive orders or similar mandates, but CDC guidance will be the standard of care in any negligence case related to COVID-19 exposure.

Third, state and local health departments have police power to enforce government quarantines, stay-at-home orders, mask orders, and the like. Workforce management protocols must therefore comply with any obligations imposed by these authorities and also should comply with nonmandatory guidance for the same reasons stated above.

In addition to applicable health and safety requirements, employers must also comply with applicable federal, state, and local law relating to employee compensation. At the federal level, the Fair Labor Standards Act includes certain obligations relating to pay for work assignments that are 24 hours or more (in addition to ordinary overtime pay obligations). The Families First Coronavirus Response Act also contains pay and job security obligations. Further, changes to the wages, benefits, and other terms and conditions of bargained employees may be subject to collective bargaining agreements and negotiations with union representatives. Finally, a number of states and localities also have passed and implemented COVID-19–related sick pay laws. Thus, the compensation payable to mission-critical employees may need to be adjusted to comply with federal law—as well as any similar or other relevant state law requirements.

#### **Data Privacy and Security**

Protocols developed to maintain critical workforce continuity in the face of COVID-19 (or other infectious diseases) may, depending on the healthcare and working arrangements included in the protocol, result in the flow of sensitive personal information and protected health information in and among employees and third parties in ways that are not typical for the company. Some of the potential measures described above, for example, involve regular temperature checks and collection of other information regarding symptoms, the results of which need to be periodically communicated either to the employer or the employer's medical advisory team. This flow of data has privacy and cybersecurity implications. Although the company may already have systems in place to collect, transfer, communicate, process, store, and destroy sensitive or protected personal information in compliance with federal and state law and consistent with cybersecurity best

practices, those existing systems might not work effectively with the efficient administration of the workforce management protocol.

Consequently, data privacy and cybersecurity procedures should be developed with an understanding of various issues associated with the potential flow of sensitive and protected personal information. What information needs to be collected? Who needs to see it and how often? How should it be transferred and stored? Are there any privacy or security risks, and, if so, how can they be mitigated? To the extent that the company's existing information systems will not suffice to appropriately handle that information in compliance with applicable law and corporate policies, the workforce management protocol should account for the need to implement appropriate information-handling procedures.

In order to ensure that all program participants—management, mission-critical employees, medical supervisors, and others—fully understand and accept the information and privacy implications of the workforce management protocol, it is advisable to develop brief information-management procedures for program participants and to review them with each participant. Additionally, weekly reviews during the course of the program are advisable to enable appropriate adjustments to the information-handling protocols.

#### **Insurance**

Critical infrastructure companies typically maintain a variety of insurance coverages, many of which are potentially implicated by the COVID-19 pandemic and a company's response to it. Those coverages include, among others, commercial property policies, business interruption insurance, worker's compensation and employer's liability policies, employment liability, director's and officer's liability policies, event cancellation policies, and trade disruption policies.

Insurance coverages that are most likely to be affected by COVID-19 are those with a "time element" to them: business interruption, contingent business interruption, extra expense coverage, preservation of property, and contamination/communicable disease coverage.

As part of the process of developing a workforce management protocol in response to COVID-19, companies should be aware of potential impacts to these and any other potentially relevant policies that they maintain and should take appropriate steps to maximize their rights under those policies. For example, a given insurance policy might require the policyholder to issue one or more notices in order to preserve the right to claim under the policy (e.g., a notice of circumstances). Companies should thoroughly review all existing policies to understand any applicable deadlines and notice requirements to avoid potential insurers' defenses, and they should carefully review and consider those policies in any upcoming

policy renewals. Further, new coverages or coverage features may be needed in connection with the implementation of a COVID-19 workforce management program. Such policies should be carefully reviewed to ensure adequate coverage and a full understanding of exclusions.

## Conclusion

Despite significant efforts to control the spread of COVID-19 and to develop effective prevention and treatment measures, the highly contagious disease remains an ongoing global pandemic. As the outbreak continues to spread through different areas of the country, with the possibility of another surge this fall, critical infrastructure companies must manage through the crisis. The nature of the disease presents unique workforce management challenges because many critical infrastructure workers cannot work remotely and often must work in close proximity to one another. A significant threat to be managed is the potential for a group of essential workers to become infected at the same time, possibly threatening continuous operations of critical infrastructure functions.

Critical infrastructure companies and other essential businesses must therefore develop robust business continuity plans for pandemics generally and take meaningful steps to monitor and manage the risk of COVID-19 within their workforces and mitigate any internal spread of the disease, especially within critical employee populations. These measures require substantial effort because a range of management, logistical, medical, legal, and other considerations must be addressed to ensure continued operational readiness. 

## Endnotes

1. See Liz Sly, Simon Denyer & Ruth Eglash, *Coronavirus Makes a Comeback Around the World*, WASH. POST (July 29, 2020), [https://www.washingtonpost.com/world/a-coronavirus-comeback-around-the-world/2020/07/28/8ddd9e64-d043-11ea-826b-cc394d824e35\\_story.html](https://www.washingtonpost.com/world/a-coronavirus-comeback-around-the-world/2020/07/28/8ddd9e64-d043-11ea-826b-cc394d824e35_story.html).

2. The Cybersecurity and Infrastructure Security Agency (CISA) has provided guidance relating to the identification and management of essential critical infrastructure workers during the COVID-19 pandemic, including a list of workers that are considered “essential.” See CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, IDENTIFYING CRITICAL INFRASTRUCTURE DURING COVID-19 (rev. May 28, 2020), <https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19>; Advisory Memorandum from Christopher C. Krebs, Dir., Cybersec. & Infrastructure Sec. Agency, on Identification of Essential Critical Infrastructure Workers During COVID-19 Response (May 19, 2020), [https://www.cisa.gov/sites/default/files/publications/Version\\_3.1\\_CISA\\_Guidance\\_on\\_Essential\\_Critical\\_Infrastructure\\_Workers.pdf](https://www.cisa.gov/sites/default/files/publications/Version_3.1_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers.pdf).

3. Electric utilities and grid operators, for example, “rely on a small number of highly trained operators for their control rooms”; and experienced operators “are essential for reliable grid operations,” which, in turn, are critical for keeping electricity flowing not only to the general public but also to

hospitals and other critical businesses. See THOMAS S. POPIK ET AL., PRESERVING OPERATIONAL CONTINUITY FOR ELECTRIC UTILITY CONTROL ROOMS DURING THE COVID-19 PANDEMIC (Mar. 25, 2020).

4. The official name for the virus that causes COVID-19 is “severe acute respiratory syndrome coronavirus 2,” or “SARS-CoV-2.” See *Naming the Coronavirus Disease (COVID-19) and the Virus That Causes It*, WORLD HEALTH ORG. (2020), [https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-\(covid-2019\)-and-the-virus-that-causes-it](https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it).

5. See, e.g., Annelies Wilder-Smith et al., *Can We Contain the COVID-19 Outbreak with the Same Measures as for SARS?*, 20 LANCET (May 1, 2020), [https://www.thelancet.com/journals/laninf/article/PIIS1473-3099\(20\)30129-8/fulltext](https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30129-8/fulltext).

6. See WORLD HEALTH ORG., TRANSMISSION OF SARS-CoV-2: IMPLICATIONS FOR INFECTION PREVENTION PRECAUTIONS (July 9, 2020), <https://www.who.int/news-room/commentaries/detail/transmission-of-sars-cov-2-implications-for-infection-prevention-precautions>.

7. See Joshua L. Santarpia et al., *Aerosol and Surface Contamination of SARS-CoV-2 Observed in Quarantine and Isolation Care*, NATURE RESEARCH (July 29, 2020), <https://www.nature.com/articles/s41598-020-69286-3>.

8. See Brianna Abbott & Jason Douglas, *How Deadly Is COVID-19? Researchers Are Getting Closer to an Answer*, WALL ST. J. (July 21, 2020), <https://www.wsj.com/articles/how-deadly-is-covid-19-researchers-are-getting-closer-to-an-answer-11595323801>.

9. See NAT’L CTR. FOR HEALTH STATISTICS, CTRS. FOR DISEASE CONTROL & PREVENTION, WEEKLY UPDATES BY SELECT DEMOGRAPHIC AND GEOGRAPHIC CHARACTERISTICS (Aug. 5, 2020), [https://www.cdc.gov/nchs/nvss/vsrr/covid\\_weekly/index.htm](https://www.cdc.gov/nchs/nvss/vsrr/covid_weekly/index.htm).

10. See, e.g., Mark W. Tenforde et al., *Symptom Duration and Risk Factors for Delayed Return to Usual Health Among Outpatients with COVID-19 in a Multistate Health Care Systems Network—United States, March–June 2020*, CDC MORBIDITY & MORTALITY WKLY. REP. (July 31, 2020), <https://www.cdc.gov/mmwr/volumes/69/wr/mm6930e1.htm> (setting out the results of a recent study in which 35 percent of symptomatic patients reported not having returned to their usual state of health roughly two to three weeks after initial testing); see also Kara Manke, *From Lung Scarring to Heart Damage , COVID-19 May Leave Lingering Marks*, BERKELEY NEWS (July 8, 2020), <https://news.berkeley.edu/2020/07/08/from-lung-scarring-to-heart-damage-covid-19-may-leave-lingering-marks>.

11. See *Cleaning and Disinfecting Your Facility*, CTRS. FOR DISEASE CONTROL & PREVENTION (July 28, 2020), <https://www.cdc.gov/coronavirus/2019-ncov/community/disinfecting-building-facility.html>.

12. See Will Stone, *Coronavirus Sparks New Interest in Using Ultraviolet Light to Disinfect Indoor Air*, NPR (July 13, 2020), <https://www.npr.org/sections/health-shots/2020/07/13/890387205/coronavirus-sparks-new-interest-in-using-ultraviolet-light-to-disinfect-indoor-a>.

13. See *How Do COVID-19 Antibody Tests Differ from Diagnostic Tests*, MAYO CLINIC (2020), <https://www.mayoclinic.org/diseases-conditions/coronavirus/expert-answers/covid-antibody-tests/faq-20484429>.

14. *Id.*

15. *Id.*

16. See *Implementing Safety Practices for Critical Infrastructure Workers Who May Have Had Exposure to a Person with Suspected or Confirmed COVID-19*, CTRS. FOR DISEASE CONTROL & PREVENTION (Apr. 20, 2020) [hereinafter *Implementing Safety Practices*], <https://www.cdc.gov/coronavirus/2019-ncov/community/critical-workers/implementing-safety-practices.html>.

17. Guillermo V. Sanchez et al., *Initial and Repeated Point Prevalence Surveys to Inform SARS-CoV-2 Infection Prevention in 26 Skilled Nursing Facilities—Detroit, Michigan, March–May*

2020, CDC MORBIDITY & MORTALITY WKLY REP. (July 10, 2020), <https://www.cdc.gov/mmwr/volumes/69/wr/mm6927e1.htm>. Random sample testing of a small portion of the employee population on a regular basis can discover asymptomatic carriers, allowing them to be removed from the population and informing contract tracing initiatives.

18. Jimmy Vielkind, *New York Utility Workers Live at Job Site During Coronavirus Crisis*, WALL ST. J. (Apr. 5, 2020), <https://www.wsj.com/articles/new-york-utility-workers-live-at-job-site-during-coronavirus-crisis-11586098801>.

19. See *Implementing Safety Practices*, *supra* note 16.

## Chair's Column

*continued from page 2*

interest in writing or speaking for IRIS, joining a committee, or virtually attending a Young Lawyers event.

This issue of *Infrastructure* provides timely commentary on the COVID-19–related challenges facing regulated industries. One article explores managing critical essential infrastructure while mitigating risk during the pandemic. Another article examines the use of cellphone technology to curb the spread and adverse effects of the pandemic. We anticipate that over the next few years, IRIS will maintain an ongoing discussion of business-continuity planning challenges faced by regulated industries.

IRIS is continuing its online programming and intends to provide more programs than typical while in-person meetings are not an option. IRIS will host webinars (at no cost for Section members) on October 21 (3:30–5 pm ET) and October 22 (1–2:30 pm ET). On October 21, our panel will discuss the growing issue of restrictions or outright prohibitions on natural gas as the next targeted fossil fuel. We will hear from a state regulatory commissioner, the chief executive officer of a national natural gas association, and a senior attorney from the Southern Environmental Law Center.

On October 22, our program's panelists will discuss the rapid increase in renewable generation in the United States. Speakers include a senior energy policy advisor who will discuss what a Biden administration may mean for federal climate change policy, a member of the New York State Climate Action Council who will update us on the steps New York is taking to increase its reliance on clean energy and reduce greenhouse gas emissions, a Columbia Law professor who will assess the role that carbon capture and sequestration might play in coming years, and the climate policy director of a major U.S. utility holding company. As a reminder, our past CLE

programs, such as the recent IRIS webinar on trends in water industry M&A, are available on the ABA website at no charge for Section members.

I also want to remind you about the ABA's efforts on diversity and inclusion. The ABA website includes a Diversity and Inclusion Center that provides a useful roadmap to available ABA programming, resources, and information addressing bias, racism, and prejudice in the justice system and society. IRIS has a Diversity Plan that is also available on the ABA website. This year, IRIS plans to combine our efforts to reach out to law students and young lawyers to introduce them to IRIS with an effort to increase diversity in the pipeline of attorneys interested in working on regulated industry matters.

I especially want to thank Christian Binnig, the Section's outgoing Chair, for his work for the Section and its members. Along with the help of our Section Director Susan Koz and other ABA staff, Chris' efforts allowed IRIS to move through pandemic-related challenges smoothly. Most recently, Chris organized and hosted a very well-attended virtual Section meeting as part the ABA's annual meeting. That IRIS meeting included an inspiring presentation by Trish Refo, the current ABA President, as well as a presentation and Q&A with the general counsel of a large utility holding company. While Chair, Chris also continued to produce written material for IRIS; for example, a recent *Infrastructure* publication included a Binnig article on the FCC's media ownership rules.

In closing, I want to remind you that we recently began Section podcasts and plan to move more content online, so please consider visiting the IRIS webpage and following IRIS on Twitter (@AmericanBarIRIS). Very best wishes for continued good health. 

## Editor's Column

*continued from page 2*

pandemic. Mobile technologies offered by infrastructure companies, for example, can facilitate contact tracing and enable quick response (QR) codes that serve as digital immunity passports and provide health screening, monitoring, and alerting systems. The use of such digital technologies is positively correlated with more effective pandemic management across the globe. The author identifies the opportunities and legal issues surrounding the use of such technology.

I want to take this opportunity on behalf of the entire Section to congratulate Cathy McCarthy on her election as Chair of IRIS for the upcoming year. Cathy has served our Section for many years and thus is well-equipped to lead us through the continued uncertainty arising from the pandemic. Like many of our clients, we will need to

remain flexible and adapt to the changing needs of our members, our clients, and their customers.

We hope you enjoy this issue. As noted in our last issue, we have begun regular podcasts focusing on topics in *Infrastructure*. Our first podcast was on net neutrality, which was the subject of an article in the Winter 2020 *Infrastructure* issue, and we have had more recent podcasts on the Safety Act and renewable energy. Other topics should be covered in additional podcasts by the time this article is printed. Follow us on twitter (@AmericanBarIRIS) or connect with me on LinkedIn to get timely notices of new podcasts as they are released.

If you have other suggested topics for future issues or would like to submit an article for consideration, please contact me at [billdrex@yahoo.com](mailto:billdrex@yahoo.com). 

## Introducing: The *Infrastructure* Podcast!

Featuring conversations between Editor Bill Drexel and *Infrastructure* authors about developments in infrastructure law and technology

<https://www.americanbar.org/groups/infrastructure-regulated-industries/>

### Net Neutrality: Take Four!

Bill Drexel, Editor of *Infrastructure*, and Joe Cosgrove Jr., Adjunct Professor at the University of Texas Law School in Austin, discuss Joe's Winter 2020 *Infrastructure* article on Net Neutrality and its current status.

### The SAFETY Act: An Important Risk Mitigation Tool for Critical Infrastructure Companies

*Infrastructure* Editor Bill Drexel and Kevin Jones, a partner with Hunton Andrews Kurth LLP, discuss Kevin's Fall 2019 *Infrastructure* article on why the Support Anti-Terrorism by Fostering Effective Technologies Act is a powerful tool to help infrastructure companies manage cyber risks.

### The Paradigm Shift in Renewable Energy

Mark Strain and Stephanie Green, partner and associate, respectively, with Duggins, Wren, Mann & Romero, recently authored *Electric Resource Planning in an Era of Burgeoning Renewables*. Together with *Infrastructure* Editor Bill Drexel, they discuss why we have entered this era of renewables and how that's critically important for the industry.

### The 9th Circuit *City of Portland* Case and Its Impact on 5G Wireless Deployment

*Infrastructure* Editor Bill Drexel talks with Andrew Emerson, partner with Porter Wright Morris & Arthur LLP, author of *Removing Barriers for 5G Wireless Infrastructure Deployment*, and Vice-Chair of IRIS and its Communications Committee. They discuss the two FCC orders designed to facilitate deployment of next-generation 5G wireless services, the Small Cell Infrastructure Order and the Moratoria Order, and the Ninth Circuit's August 2020 response to challenges to them in *City of Portland v. United States*.

# infrastructure

## **ABA Infrastructure and Regulated Industries Section**

American Bar Association  
321 N. Clark Street  
Chicago, IL 60654-7598

Nonprofit Organization  
U.S. Postage  
PAID  
American Bar Association

## **Save the Date!**

### **Upcoming IRIS CLE Webinars**

### **Free to Section Members**

October 21, 2020, 3:30–5:00 PM ET

#### **Natural Gas Faces the Future: More, Less, Green, or None at All?**

Laws, regulations, and requirements applicable to the use of natural gas continue to develop rapidly. Learn more about the federal, state, and local laws that may restrict or prohibit the use of natural gas now and in the future. Panelists will include a state regulatory commissioner. They will discuss, among other things, local laws prohibiting utility connections and some states' ban of those connections, as well as federal, state, and local laws that apply to interstate natural gas pipelines.

October 22, 2020, 1:00–2:30 PM ET

#### **Climate Change and the Changing Generation Mix: Environmental Effects, Technological Advances, and Policy Options for 2021 and Beyond**

Panelists will discuss the state and federal laws that have contributed to the recent historic changes in generation mix along with potential upcoming changes in the law that will likely further affect the mix. The program will also cover how technological advances may affect the range of legal options available for lowering greenhouse gas emissions and the legal challenges already being posed by recent changes in the generation mix..

Registration for the webinars is available on the Section website: [https://www.americanbar.org/groups/infrastructure-regulated-industries/events\\_cle/](https://www.americanbar.org/groups/infrastructure-regulated-industries/events_cle/)