May 1, 2020

Going Back to Work: Employer Use of "Apps" on Employee PDAs/Smart Phones for COVID-19 Contact Tracing

Attorneys
Mark Barnes
Megan Bisk
Edward R. McNicholas
Sarah Blumenthal
Samantha M. Brennan
Stephanie A. Bruce
Fran Faircloth
Josiah Irvin

As new cases of COVID-19 begin to plateau and decline in some places, governors, municipalities, retailers, employers, and others are considering when and how to reopen safely. Public health officials caution, however, that reopening too quickly and without the right public health protections in place risks a COVID-19 resurgence.[1] One traditional method of public health prevention is a robust practice of contact assessment and contact tracing, in which the close contacts of an infected person are identified, tracked, warned of exposure, and then directed to test, self-quarantine, and/or receive treatment. Tech companies are developing contact-tracing applications ("apps") that utilize smart phone and mobile phone technology in the hope that technology can be used to conduct electronic contact assessment and notification, and that such a system would be more rapid, more accurate, and more effective than "shoe leather" person-to-person contact tracing methods traditionally used by public health departments.[2]

With mobile technology near ubiquitous in major swaths of society, employers are considering use of these contact-tracing apps to determine when to reopen their businesses and how to keep their workforce healthy once the workplace has been reopened. This alert reviews these apps' technical development, where and how they are currently in use, and the legal and practical framework necessary for employers to deploy this technology within acceptable legal and ethical parameters. The alert ends with FAQs that summarize the lengthier analysis and offer best practices for employers considering using contact-tracing apps.

Technology-Enabled Contact Tracing

Mobile phones and smart phones have different means of tracking locations and logging their users' movement. For example, location is tracked both by a phone's interaction with nearby cell towers and antennae and by its embedded GPS; a phone's Bluetooth technology can exchange information with nearby Bluetooth-enabled devices such that the devices register the presence of each other. In a contact-tracing app, a user (voluntarily, or otherwise if made mandatory by a government or employer) downloads an app to his/her phone into which the user (or a third party like a health care provider or testing lab) inputs the user's known or presumed COVID-19 status, and the app interacts with other contact-tracing apps on other phones in whose vicinity the first phone has been. The app communicates to its user if he/she had been in close, sustained contact with someone who had tested positive for (or was diagnosed with) COVID-19 and communicates to other phones if its user registers as COVID-19 positive. Specific users who are identified by the app's algorithmic logic, which works by calculating close exposures using geolocation data, are instructed by the app to self-quarantine and/or seek testing for COVID-19 infection.

Developers are considering contact-tracing apps that use GPS, cell phone location data, and/or Bluetooth.[3] Most privacy-intrusive are the GPS-based apps and tracing systems that rely on cell phone location data, such as those in use in South Korea and Israel. These apps and systems track and communicate individuals' locations and movements to a centralized source, such as the government.[4] They can pinpoint the potential location of exposure, as well as the phones of the users who appear to have been in close contact with one another. The apps in use in Singapore[5] and Australia,[6] communicate

ATTORNEY ADVERTISING

between phones using Bluetooth technology to alert users if they have come in contact with someone who has reported himself or herself as COVID-19 positive. These decentralized apps, however, will not tell a user where or to whom they were exposed. As such, privacy advocates favor this technology.[7]

The United States is distinct from many of the countries where these apps have been adopted, such as Singapore, South Korea, and Taiwan, as the United States has a patchwork of state and federal privacy laws, and, for employers, various federal and state employment laws that can apply to the implementation and use of this technology. Countries where the apps have been rolled out with some success have utilized a coordinated, national strategy and have relied on the authority of the central government. In the United States, the interplay between state and federal authority makes it unlikely that the United States will—or even could—have a single, federally mandated, technology-based contact-tracing strategy. Moreover, the United States faces demographic and socioeconomic differences that may challenge the effectiveness of mobile-enabled, technology-based contact tracing, such as subpopulations that do not uniformly have smart phones, and persons who do not keep their smart phones on their person at all times. Nevertheless, for employers considering technology-based contact-assessment and tracing strategies, the following sections of this alert summarize salient legal and logistical considerations.

Legal Framework for Employer-Based Contact Tracing

Employer-based contact tracing implicates a variety of laws, including workplace laws like the Americans with Disabilities Act ("ADA"), other federal and state employment and civil rights laws, privacy and consumer protections, and—particularly with respect to public employers—federal and state constitutional issues. Although most state governments already collect COVID-19 data pursuant to their public health reporting role, federal and state constitutional and statutory prohibitions render state-mandated apps challenging to implement in the United States. As such, voluntary, employer-adopted contact-tracing programs that mandate (or, alternatively, strongly encourage) employee participation are more promising from an implementation perspective. Employers looking to introduce these apps may point to their duty under the Occupational Safety and Health Act ("OSHA") to furnish to workers "employment and a place of employment, which are free from recognized hazards that are causing or are likely to cause death or serious physical harm."[8] Notably, many employers already require health screening for various conditions, and some jobs mandate ongoing health checks, consistent with OSHA standards and subject to ADA restrictions and safeguards.

Americans with Disabilities Act

The ADA is relevant to an employer considering adoption of a contact-tracing program. The Equal Employment Opportunity Commission ("EEOC")—the cognizant federal enforcement agency—has not directly opined on contact-tracing apps, but has issued guidance on other employer responses to the pandemic. Specifically, employers may restrict access to facilities by employees who pose a "direct threat" to the health or safety of others if there is a "business necessity" for such restriction, like the need to provide a safe working environment. The EEOC, based on the latest guidance from the U.S. Centers for Disease Control and Prevention ("CDC"), has categorized COVID-19 as a "direct threat."[9] However, the criteria assessment used by the employer in implementing such restriction (e.g., medical examinations or medical inquiries) must genuinely serve the asserted business necessity and not be more intrusive than necessary.[10]

With respect to COVID-19, the EEOC has advised that employers may require medical examinations—including COVID-19 testing or body temperature checks—of their employees, provided that such examinations are job-related and consistent with business necessity (including where employees have a medical condition that would pose a "direct threat" to the health or safety of others, which includes COVID-19 as noted above). Further, and particularly relevant to the contact-tracing app,

employers may make inquiries that are not disability-related (i.e., not likely to elicit information about a disability), such as inquiring about travel-related exposure to pandemic viruses such as COVID-19, regardless of whether COVID-19 constitutes a "direct threat."[11] As with all medical information, the data must be stored confidentially and separately from the employee's personnel file.[12]

By analogy, use of a contact-tracing app for purposes of assessing individuals' COVID-19 exposure risk would not be prohibited under the ADA (and analogous state disability rights laws), provided the above standards and guidelines are followed. The ability of an employer to meet these standards may vary based on specific employment settings, applicable privacy laws, and whether the app is in fact not more intrusive than necessary to meet the business necessity.

Many states and certain localities have their own disability rights laws. Although such laws generally tend to follow the ADA and are interpreted consistent with the federal EEOC guidelines and approach, employers should consult applicable state and local law for any variations before designing and implementing a program.

Federal and State Constitutional Limitations

Public employers' use of a contact-tracing app is subject to additional requirements—in particular, the federal Constitution's Equal Protection Clause and Due Process Clause protections. The Equal Protection Clause requires that a law that discriminates on the basis of disability pass the rational basis test to be upheld.[13] The rational basis test is the least stringent level of review courts apply and requires that the government's action be rationally related to achieving a legitimate government interest. Courts generally are deferential to legislative decisions when reviewing government actions under the rational basis test, and typically uphold such action. Here, COVID-19 does not generally qualify as a disability, which makes the applicability of the protections of the Equal Protection Clause questionable. To the extent COVID-19 could qualify as a disability under certain circumstances—where, for example, an individual's symptoms are severe enough to be debilitating, become chronic, or exacerbate an existing disability—the public employer's interest is in maintaining a healthy work environment and preventing the spread of COVID-19 to other employees and the public at large. Using a contact-tracing app may be rationally related to this goal, as it will enable an employer to identify a potentially infected employee, limit such employee's interactions in the workplace—including barring that employee's immediate workplace presence—and institute testing or self-quarantine measures for potentially exposed employees or other individuals who may have interacted with the infected employee (e.g., customers). However, any analysis of such programs will be fact-specific and, as is the case under the ADA and other federal, state and local anti-discrimination laws (which also apply in the public employer context), an employer is not allowed to implement such programs in an unequal or discriminatory manner.

The Due Process Clause requires that a government employee who has a right to continued employment receive notice and the opportunity to respond prior to termination.[14] In practice, this requires providing the employee notice of the reason for the charges against him or her and an opportunity to respond to the charges in a fair hearing, prior to terminating employment. In the context of a contact-tracing app, this means that not only must the use of the app and its metrics be consistent across all employees, but also, if a government employer chooses to terminate employment based on an employee's refusal to use a required contact-tracing app, the affected employee must have a post-action right to appeal the termination.

This approach is also advisable for a suspension without pay, although in limited cases, an employer may still be considered to have afforded due process to an employee even without a pre-suspension hearing. There must be an opportunity for a post-action appeal, and the government must show there was a need to act quickly or that it would have been "impractical to provide [a] predeprivation process."[15] In making this determination, a court will weigh (1) the private interest that will be

ATTORNEY ADVERTISING

affected by the government's action; (2) the risk of an erroneous deprivation of the employee's rights, and the probable value of additional or alternative procedural safeguards, such as a pre-suspension hearing; and (3) the government's interest.[16]

Employers should note that many state constitutions include parallel equal protection and due process requirements. Thus, employers would also need to consider any nuances under applicable state constitutional protections.

Other Legal Considerations

In addition to the above, employers should be cognizant of these additional laws that contact tracing implicates.

- Federal, State, and Local Anti-Discrimination Laws. In addition to the ADA, several federal laws, including Title VII of the Civil Rights Act, the Age Discrimination in Employment Act, the Pregnancy Discrimination Act, and the Genetic Information Nondiscrimination Act, as well as many corresponding state and local laws, variously prohibit discrimination in the workplace on the basis of race, color, religion, sex, national origin, age, pregnancy, and genetic information. Consequently, use of contact-tracing apps must not be conducted in a discriminatory manner based on an individual's protected characteristics (e.g., requiring the app to be installed by employees who are over 65 years old or pregnant solely because they may be at higher risk from COVID-19).[17]

- Other Employment Laws and Contract Rights. Some states may have employment rights laws more protective than the anti-discrimination and disability rights laws referenced above. For instance, to the extent the app provides employers with access to information about an individual user's off-duty whereabouts or activities, it may implicate state "off-duty conduct" laws, such as those in California and New York, which prohibit employers from taking adverse action against employees for their lawful after-work activities. However, many of these laws contain exceptions for conduct that materially conflicts with an employer's business interest, which could arguably include protecting its employees from COVID-19 exposure, even outside the workplace.[18] Of further consideration is that many of the app designs, such as those that are Bluetooth-dependent, do not track or provide this information, and, even if they do, employers may not have access to the centralized repository of information. Employers must also comply with wage and hour laws in implementing the contact-tracing app's requirements. Among other things, such wage laws impose limitations on passing along the costs of these programs to employees (e.g., requiring employees to purchase a smart phone or utilizing an employee's data bandwidth for purposes of the app). Finally, employees may have contractual rights—under either an individual employment agreement or collective bargaining agreement—that limit use of these apps for employment purposes.

- Health Care and Other Laws. Contact-tracing apps could, with some legal calculation and proactive compliance measures, incorporate health data received from the employees' health care providers (e.g., a COVID-19 positive test, a presumptive COVID-19 diagnosis). Receiving information from provider or laboratory sources could theoretically be routinized and would be much more accurate and efficient than relying on employees' self-reports of COVID-19 diagnoses through their voluntary entry of their diagnosis into the app. But such a practice of the provider or lab reporting identifiable health information to an app will implicate health information privacy laws. Under HIPAA—the principal federal health care privacy law—employers do not have a general right to receive health information from their employees' health care providers. Rather, health care providers are permitted to disclose protected health information only for payment, treatment, or health care operations; otherwise, patient authorization is required for use or disclosure of identifiable health information.[19] As a general matter, app developers will need independent authority under HIPAA to

ATTORNEY ADVERTISING

receive health information directly from providers, and, depending on the rationale for disclosure, may have downstream limitations on the ability to re-disclose that information. Diagnosis information coming directly from a laboratory to an employer, including through an app, would require patient consent under CLIA.[20] In addition, collecting information without specific consent or updating app software without consent can violate other federal and state electronic technology and privacy laws.[21] Therefore, employers who wish to implement this technology would need to obtain from each employee an authorization to allow the provider or lab to send the health information to the app and even to the employer, depending on the design of the app; a clear consent that authorizes the employer's obtaining, using and disclosing employee health and geolocation data; and consent for installation of the software for contract assessment and tracing purposes.

- Other Information Privacy Laws. Requiring employees to use the contact-tracing app also implicates state privacy laws, which generally protect an employee's right or expectation against unreasonable, substantial, or serious interference with privacy unless such right or expectation is outweighed by a legitimate business interest (here, protecting the health and safety of its employees), and provided that the interest is met using the least intrusive means (e.g., collecting only the minimal information necessary to accomplish the employer's goal and anonymizing such information to the maximum extent possible). Notably, in nearly all cases, an employee will not have a reasonable expectation of privacy if the employer has notified the employee of the data collection, and has obtained the consent of the employee. Some states—like California under the California Consumer Privacy Act—require advance notice to the employees of the data collection,[22] and information held by an employer is likely subject to state data privacy and security laws. Likewise, other consumer protection laws (such as the federal Fair Credit Reporting Act and similar state laws) might be deemed to apply if a third party aggregating the data is viewed as a consumer reporting agency; in such case, the employer would be required to provide notice to, and obtain the consent of, an employee before collecting or relying on the data to take adverse action against the employee.

Because of contact-tracing apps' intrusive nature and the laws discussed above, employer-required or employer-implemented electronic contact tracing could be viewed as overreaching. These concerns would be heightened for an employer seeking to implement a blanket requirement that all employees must install and use the app, or seeking to gather and use COVID-19 data of employees when they are off duty. As such, any employer-implemented program should be carefully designed, reviewed, and vetted. In general, consent-based approaches will be easier to implement, particularly if the consent, even if opt-out, is prominent and comprehensive notice of how the information will be used is provided.

Practical Considerations for Contact Tracing in the United States

Assuming adherence to the legal standards outlined above, an employer would still need to overcome cultural, workplace, demographic, and socioeconomic differences that may limit mobile-enabled, technology-based contact tracing's effectiveness. Importantly, effectiveness likely requires widespread adoption at a regional level. A recent study modeled that, for a city of one million people, approximately 56% percent of the population (or 80% of smart phone users) would need to participate to halt an outbreak.[23]

As a threshold matter, many individuals may not carry their phones with them at all times as a matter of personal habit or employment restrictions. For instance, employees in industrial occupations like manufacturing, construction, resource extraction, and agriculture often store their phones, along with other personal items, in a locker during their shifts. Likewise, national security employees and similar government personnel are often prohibited from carrying personal devices while performing their duties, due to confidentiality concerns.

ATTORNEY ADVERTISING

In addition, smart phones are a luxury good. Many Americans—particularly lower-income Americans—lack smart phones or use temporary, disposable phones, and some people have elected not to acquire smart phones for personal or philosophical reasons. Absence of these devices, therefore, reduces the reach of technology-enabled contact tracing.

Finally, public fear of government and corporate mass surveillance is well established. As such, employers may encounter considerable resistance if they require (or even strongly encourage) installation of these apps on employees' personal smart phones, which have large amounts of personal data and are already subject to heightened legal protections.[24]

Employer-Based Contact Tracing Frequently Asked Questions

Can I require my employees to download a contact-tracing app as a condition of continued employment?

In general, private employers likely could lawfully mandate that employees utilize a contact-tracing app, provided that the mandatory program is administered in a manner that is no more intrusive than necessary to meet the legitimate business concern. The permissibility of a contact-tracing app may vary based on differing employment settings, the employer's business necessity for employee proximity, and whether the employer can implement less intrusive measures to provide a safe environment. For instance, a professional services firm, where the vast majority of employees can (or do) work remotely and thus present no immediate danger to anyone else in the workplace, may have difficulty showing the app is a business necessity and not more intrusive than necessary. On the other hand, an industrial meat-processing plant that requires in-person presence and where the nature of the work prevents social distancing within the plant may readily make the required showing, but note that the app may not be effective if these employees do not keep their smart phones on their person during the work day and, instead, store them in a locker off the factory floor.

Further, employers must ensure that the app is used in a non-discriminatory manner and that any medical or other personal information the employer obtains is stored confidentially and separate from employees' personnel files. Employers would likely be required to cover the costs associated with the apps or the acquisition of smart phones to run the apps for employees who do not already own smart phones. Employers should seek to obtain consent from employees that authorizes the employer to obtain, use, and disclose to public health officials employee health information and geolocation data, as well as installation of the software for contact assessment and tracing.

Public employers may also mandate use of a contact-tracing app. However, in addition to satisfying the requirements noted above, they must consider the equal protection and due process implications. In particular, with respect to due process, public employers likely must ensure that there is a post-determination appeal process for anyone who has been denied access to the workplace as a result of being identified as COVID-19 positive or at risk based on his/her geolocation contacts. Voluntary employee participation programs may be more defensible from a privacy law perspective, but will require widespread adoption for public health effectiveness.

As an employer, can I have access to the centralized information of the contact-tracing app to be aware of the identity of employees with a COVID-19 positive indication?

Employers will need consent from their employees to receive from an app controller any medical information about their employees. Yet this access will depend on app design, and many of the model apps are being built in a decentralized way, such that this centralized, identifying information will not be available to the employer or to other third parties. Limiting any third-party access to this electronically-generated infection exposure information has become, in fact, a design feature to alleviate privacy concerns.

The best that might be done in such apps would be that they would alert the employee him/herself to that employee's COVID-19 risk, and the employer would need to adopt a policy by which employees are required to report the fact that they have been in close contact with someone who is infected, as indicated by the app. Likewise, as noted above, if an employer has access to an employee's off-duty whereabouts or activities, or other personal information, it may implicate state GPS tracking, off-duty conduct, and privacy laws. Ideally, the contact-tracing app would either restrict an employer's access to information about an individual user's off-duty whereabouts, activities, or personal information, or be designed not to collect or store such information in the first instance. Any information the employer does receive and store, however, would be subject to applicable state information privacy and security rules.

As an employer, how may I enforce my requirement that employees install, monitor, and update a contact-tracing app?

Employers may pre-install apps on employer-issued devices, and, once the apps are installed, the devices may have an ability to monitor adherence to the employer's policy. However, employers will face practical difficulties actually forcing their employees to install apps on their personal devices, and, on all devices, they will have little ability to force employees to actively review—much less use—any information the apps provide. Moreover, for an app that is driven by the device holder's own self-reported COVID-19 diagnosis (as opposed to an app driven by direct reports from laboratories of COVID-19-infected persons and their mobile phone number), the app algorithm functions only as well as the integrity of the input—meaning that a noncompliant employee who reports a COVID-19 diagnosis late or not at all would obviate the successful functioning of the app.

Rather, as with most workplace policies, adoption and adherence will likely depend on cooperation and employee "buy-in." The necessity of a cooperative approach also has precedent in the employee social media context—as several states prohibit employers from requiring employees to provide social media account usernames and passwords.

As an employer, may I require an employee to self-quarantine or get tested based on an app reading of COVID-19 exposure?

Yes, but this assumes that (a) the app is configured to report the employee's diagnosis to the employer, and (b) the diagnosis itself has been promptly and accurately reported to the app, either by the employee (as in most apps under development) or by a provider or laboratory (although this depends on the provider's/lab's willingness to cooperate in a voluntary app reporting system). Note that employers may be required to permit an employee to work from home, provide sick time, and/or cover the costs of COVID-19 testing for at-risk employees.

Are there contact-tracing apps available in the U.S. market today that may be used?

In general, not yet, although the governors of North and South Dakota have introduced an app as part of a statewide effort in their jurisdictions.[25] There has been limited adoption of this app, which, initially, was only available for the iPhone and is generally imprecise in how it uses GPS and cell tower location data to track people's locations.[26] Some design specifications have been released for other apps, but those apps appear not yet available for use. The Safe Paths app under development by researchers at the Massachusetts Institute of Technology is currently undergoing beta testing.[27] Apps being used in other countries are available in those markets alone, and other developers are in the process of developing apps for use in the U.S. market.

ATTORNEY ADVERTISING

1. Adam Rogers, The Asian Countries that Beat COVID-19 Have to Do It Again, WIRED, (Apr. 6, 2020) https://www.wired.com/story/the-asian-countries-that-beat-covid-19-have-to-do-it-again/.
2. Kelly Servick, Cellphone Tracking Could Help Stem the Spread of Coronavirus. Is Privacy the Price?, Science, (Mar. 22, 2020) https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price; Sarah Perez, This Week in Apps: COVID-19 Contact Tracking Apps, Virtual Dating on the Rise, Quibi Makes a Debut, TechCrunch, (Apr. 11, 2020), https://techcrunch.com/2020/04/11/this-week-in-apps-covid-19-contact-tracing-apps-virtual-dating-on-the-rise-quibi-makes-a-debut/.
3. Derek Thompson, The Technology that Could Free America from Quarantine, Atlantic, (Apr. 7, 2020), https://www.theatlantic.com/ideas/archive/2020/04/contact-tracing-could-free-america-from-its-quarantine-nightmare/609577/.
4. Isobel Asher Hamilton, Compulsory Selfies and Contact-Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, and It's Part of a Massive Increase in Global Surveillance, Business Insider, (Apr. 14, 2020), https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3.
5. I. A. Hamilton, Business Insider (Apr. 14, 2020).
6. Kim Lyons, Australia's COVIDSafe Contact Tracing App Already Has More Than a Million Downloads, The Verge, (Apr. 26, 2020), https://www.theverge.com/2020/4/26/21237598/australia-coronavirus-contact-tracing-privacy.
7. Daniel Kahn Gillmor, Principles for Technology-Assisted Contact-Tracing, ACLU White Paper, (Apr. 16, 2020), https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing.
8. Section 5(a)(1) of the Occupational Safety and Health Act of 1970.
9. EEOC, EEOC-NVTA-2009-3, Pandemic Preparedness in the Workplace and the Americans with Disabilities Act (Mar. 21, 2020), https://www.eeoc.gov/facts/pandemic_flu.html.
10. 42 U.S.C. § 12112; *see also* United States v. Bethlehem Steel Corp., 446 F.2d 652 (2d Cir. 1971).
11. *Id.*
12. 29 C.F.R. § 1630.14.
13. *City of Cleburne v. Cleburne Living Center, Inc.*, 473 U.S. 432 (1985).
14. *Cleveland Bd. of Educ. v. Loudermill*, 470 U.S. 532, 541 (1985).
15. *Gilbert v. Homar*, 520 U.S. 924 (1997).
16. *Gilbert*, 520 U.S. at 931–32 (citing *Mathews v. Eldridge*), 424 U.S. 319, 335.
17. 42 U.S.C. § 2000e *et seq*.; 29 U. S.C. 621 *et seq.;* 42 U.S.C. § 2000ff *et seq*.
18. N.Y. Labor Law § 201-d; Cal. Labor Code § 96.
19. 45 C.F.R. § 164.502(iv).
20. 42 C.F.R. § 493.1291(l).
21. *E.g.*, Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030; 18 U.S.C. §§ 2510-2522.
22. Cal. Civ. Code § 1798.100. (Note, however, that most of California Consumer Privacy Act's provisions, including the major consumer rights, do not apply to employee data until January 1, 2021 under current law.)
23. Leon Kelion, Coronavirus: NHS Contact Tracing App to Target 80% of Smartphone Users, BBC News, (Apr. 16, 2020), https://www.bbc.com/news/technology-52294896.
24. *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014).
25. Jennifer Valentino-DeVries, Natasha Singer, and Aaron Krolik, A Scramble for Virus Apps that Do No Harm, NYTimes, (Apr. 29, 2020).
26. *Id.*
27. Massachusetts Institute of Technology, Project Safe Paths, https://www.media.mit.edu/projects/safepaths/overview/ (last visited Apr. 27, 2020).

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have. © 2020 Ropes & Gray LLP

ATTORNEY ADVERTISING