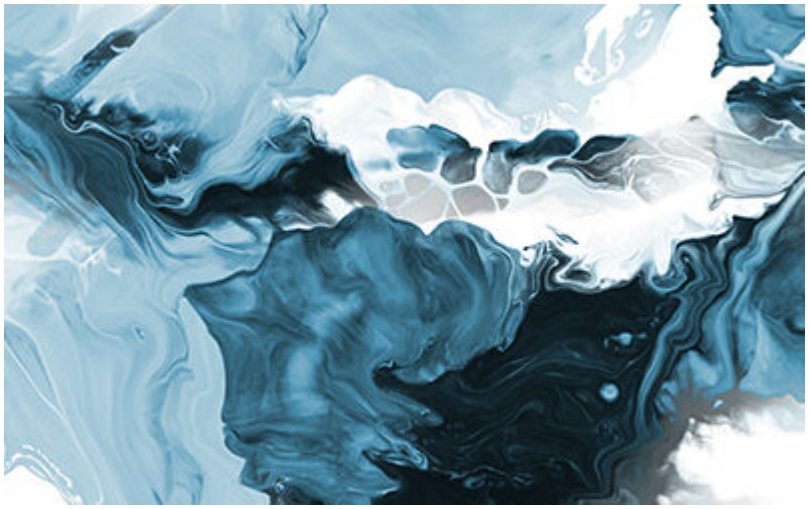
MAYER | BROWN



Cybersecurity

The novel COVID-19 virus has exposed businesses to dynamic cyber threats and data privacy challenges—and accompanying legal risks.

The rapid expansion of remote work and associated strains on employees have created new opportunities for cyber criminals. Further raising risk, critical company systems and data may be exposed by increased remote access, and it may be harder for companies to respond effectively to cyber incidents. As a result, cyber criminals are seeking to exploit COVID-19 through phishing scams, ransomware, business email compromises, and other attacks. For example, one Russian criminal group has been associated with malware that uses a legitimate COVID-19-related map produced by Johns Hopkins University while seeking to steal user passwords.[1] The U.S. Department of Health and Human Services reportedly recently suffered a distributed denial of service attack.[2] And Brno University Hospital, one of the largest COVID-19 testing centers in the Czech Republic, reportedly suffered a cyberattack that shut down its computers, and led to cancelled operations and patient relocations.[3] (For our prior alert on phishing campaigns in Hong Kong, please see here.)

Businesses also are taking an active role in advancing public health and safety by putting in place precautionary measures to slow the spread of COVID-19 or developing new technological tools to advance that important goal. However, the pursuit of such measures raises privacy considerations for companies and for public authorities even as they seek to protect their employees and populations more broadly.[4] The surge in remote work likewise raises privacy challenges, including because of the handling of private information outside a secure work environment and because of the challenges of meeting ongoing compliance obligations with a remote workforce.

We discuss below key cybersecurity and data privacy challenges raised by the COVID-19 crisis. While precise solutions will vary across companies and will need to factor in jurisdiction-specific frameworks, we also highlight key considerations for in-house counsel as they work to mitigate associated legal risks.

Cybersecurity Threats and Challenges

1. Cyber Attackers Seeking to Exploit the COVID-19 Crisis

Cyber criminals and other attackers have sought to take advantage of COVID-19 through a wide range of attacks. For example, cybercriminals impersonating medical experts such as virologists or officials from the World Health Organization have been sending phishing emails containing malicious links or attachments which purport to provide information on how to protect against the coronavirus. The sheer volume of these attacks has been enormous.[5] For example, the security firm Proofpoint recently reported: "To date, the cumulative volume of coronavirus-related email lures now represents the greatest collection of attack types united by a single theme that our team has seen in years, if not ever."[6] Unsuspecting users who click on the links or access the attachments open their systems to a malware attack which may result in further attacks on the company's network, theft of personal information or trade secrets, or company systems being rendered inoperative. (Such ransomware attacks may be particularly devastating, particularly to the extent that they compromise hospitals struggling with the epidemic or other critical infrastructure providers that are already under strain.) Likewise, the Federal Bureau of Investigation recently warned that as part of COVID-19 themed attacks, "[c]riminals are using malicious websites to infect and lock devices until payment is received."[7]

Government authorities and agencies have issued guidance to companies and consumers on how to manage these risks. For example, the Department of Homeland Security has highlighted that threat actors "may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes."[8] To mitigate these risks it counselled people to rely only on trusted new sources and to "avoid clicking on links in unsolicited emails." Similarly, the Federal Trade Commission has issued guidance to consumers with tips to avoid "Coronavirus Scams." These range from ignoring online ads for purported vaccinations to vetting online sellers of in-demand items like cleaning products and protective gear.[9] Likewise, the New York Department of Financial Services ("NYDFS") has warned consumers about coronavirus scams on social media, emails, texts and websites.[10] The European Union Agency for Cybersecurity ("ENISA") similarly has released practical tips for cybersecurity when working remotely (a topic we cover in more detail below).[11] Tips range from ensuring awareness of existing threats by monitoring the CERT-EU News Monitor, as well as recommendations on how to recognize malicious emails that attempt to scare the recipient with a threat of severe consequences if they fail to follow a given link.[12]

Numerous experts expect not only cyber criminals, but also nation states, to take advantage of the disruption caused by COVID-19 and the resulting expansion of remote work. Espionage groups are expected to attempt to take advantage of less-secure remote connections, for example, and attacks on government agencies or critical infrastructure are more likely as relevant government agencies focus their resources on COVID-19 response rather than on their cyber mission.[13]

Responsibility for addressing these threats is likely to fall to companies' information security teams. In-house counsel will benefit from awareness of heightened cyber threats during the COVID-19 epidemic, however, and may consider such steps as engaging with the security team to understand the company's current posture in response to these threats (e.g. anti-phishing tools) and evaluating updated cyber risk assessments (and related public disclosures) in light of those threats. Likewise, in-

house counsel may wish to consider whether the company is exposed to heightened legal risk because of increased threats to vendors, and what steps the company might take to mitigate that risk. For example, counsel may wish to review rights and obligations provided for by key vendor contracts in light of changing risks posed in this dynamic environment. Based on this review, counsel may advise business units on how to calibrate their engagement with vendors, such as through the exercise of audit rights to understand the vendor's use of anti-phishing tools or through limitations on vendor access to company systems in the event that risks cannot be otherwise mitigated.

2. Security Risks from the Rapid Move to Remote Working

A wide range of companies have undertaken—or are undertaking—rapid transfers to remote working. Misconfigurations associated with a rapid rollout or a lack of employee training on these new devices and systems can create vulnerabilities for cyber criminals to exploit. For some organizations, the increased use of personal devices by employees poses its own set of risks, including because of the potentially reduced ability to secure those devices. Likewise, companies may struggle to maintain visibility into company-issued devices at home or suffer data loss due to employees forwarding sensitive business or client information to personal accounts. Finally, increased connectivity may create new risks to the extent that critical systems are increasingly accessed from outside the company's network.

In-house counsel will likely be able to reduce legal risk by working with the information technology and information security teams to ensure that reasonable security practices are in place for remote working – and documenting the prioritization of steps taken based upon a risk-based approach. Various technologies, such as encryption, endpoint security tools, virtual private network connections, multi-factor authentication, and data loss protection tools can help reduce cyber risk.[14] Practically speaking, however, it may be difficult for a company to instantaneously achieve an ideal security state for a new fleet of remote devices and users. As a result, in-house counsel will likely benefit from advising internal information security and information technology teams on opportunities to enhance security in a manner that is prioritized based on a company's particular risk profile. For example, this may include advising internal clients to focus on the encryption of certain data, to prioritize the rollout of heightened security tools to teams that handle market-sensitive information, or to ensure the addition of compensating controls to account for increased external connectivity to critical systems.

Many in-house counsel also are likely to be called upon to advise companies on the secure handling of sensitive data at home. Many companies, for example, have rules for handling certain data only in controlled environments—or have a flat bar on taking certain data home. Such rules may no longer be feasible for a remote work force. Still, handling confidential business and employee information outside the controlled environment of an office can be risky. Cyber attackers or other thieves may attempt to capitalize on opportunities created by remote work to steal or corrupt this type of information. For example, various security measures utilized in a typical call center environment (e.g., no electronic devices, paper or printers) coupled with close oversight, physical security and secure disposal would limit the opportunity for misuse, retention or misdirection of customer information. Employees working remotely may operate free of these restrictions, potentially leading to the loss of sensitive customer information (and potentially raising issues under governing contracts, which may impose such restrictions). Companies may also face legal hurdles with respect to the collection of certain sensitive information in home environments, such as credit card numbers, social security numbers, bank account

information, and health information collected by call center employees, banking personnel, or healthcare professionals engaging in telemedicine.

In-house counsel will likely benefit from focusing on a few key points as they advise their internal clients on these matters. First, it likely will be important to maintain a flexible and common-sense approach to advice in this area, including by developing solutions that allow business to continue while appropriately securing information. (Working closely with relevant internal teams to understand available options – asking whether an employee really needs access to certain data, for example, or whether technical tools can reduce risk – may particularly serve this goal.) Second, in-house counsel will likely want to ensure that training is updated to be consistent with the agreed-upon approach, that policies are likewise amended, and that those policies are enforced. Third, companies should also be aware of regulatory obligations with respect to the handling of sensitive data. Keeping abreast of rule changes will be key; for example, HHS's Office of Civil Rights is waiving all potential HIPAA penalties for good faith use of telehealth remote communications during the COVID-19 emergency.[15] At the same time, multiple EU agencies have stated that the current pandemic does not justify failure to follow fundamental data protection principles, including the need to maintain (and document) adequate security measures for personal data.[16] Finally, companies should consider whether a proposed approach is consistent with their contractual obligations—e.g., with respect to the performance of customer service functions (call centers, payment processing, or loan servicing).

3. Challenges of maintaining standard cybersecurity operations

Businesses also may face challenges maintaining their standard cybersecurity operations when resources are stretched thin addressing remote working issues or members of the security team are themselves working remotely. Staffing a business' security operations center or operating it remotely may be challenging, for example. Likewise, a company may struggle to deliver an effective incident response capability with numerous stakeholders out of the office or to perform tasks that require physical presence, such as a penetration test on a new product prototype.

Counsel may wish to review existing incident response materials and other key cybersecurity policies and procedures in order to identify potential stumbling blocks for relevant business units (and associated legal risk). For example, to understand and address incident response capabilities, counsel may wish to review and amend relevant incident response plans and playbooks in light of likely scenarios and the practical realities of remote working or medical unavailability of key stakeholders.

Counsel also may wish to consider that compliance and audit teams may face new difficulties when completing their assessments remotely. Collection and storing of audit evidence could prove challenging, and travel to client sites may not be possible. Preparation of financial statements may be hindered by the inability to collect certain disclosures. Some regulators are providing guidance for companies on these issues. For example, the UK's Financial Reporting Council (FRC) published guidance last week and is holding weekly calls with large UK audit firms.[17] The SEC has also issued guidance on how it will continue market monitoring and engagement with market participants, including the publication of a temporary no-action letter regarding the Self-Regulatory Organization's enforcement of Consolidated Audit Trail compliance rules.[18] Companies will benefit from staying abreast of these regulatory developments, as well as taking practical steps to reduce compliance risk. For example, companies may wish to consider making critical files, such as process documents and

compliance manuals, available to key compliance and audit personnel with appropriate access settings. Likewise, companies should understand any relevant deadlines. For example, the NY DFS extended the data for filing the Certification of Compliance with its Cybersecurity Regulation for calendar year 2019 from April 15, 2020 to June 1, 2020 (although it still expects licensed entities to file timely notifications if a cybersecurity event occurs).[19]

Beyond internal processes, businesses should expect that vendors and contractual counterparties will face their own challenges—both in terms of their availability and capabilities once retained. This may include vendors assisting with daily cybersecurity operations, penetration testing firms, or vendors for incident response. Considering the unprecedented circumstances, in-house counsel may consider reviewing vendor contracts along with the CISO to ensure that security vendors will be able to deliver contracted security services upon which the company relies—and plan accordingly if that is in question, whether because the vendor has moved to remote working or faces other practical challenges (or even bankruptcy). In the context of incident response, these circumstances make it all the more important to have key vendors retained in advance of incident. Companies also should anticipate possible challenges delivering an efficient response even once a vendor is in place. For example, incident investigations may face delays if a forensic firm cannot remotely image compromised machines. (As discussed above, companies also likely should generally evaluate the cyber risk presented by engagement with vendors across their business.)

Privacy Challenges

1. Asking individuals about their diagnoses or symptoms

The Centers for Disease Control and Prevention (CDC) recently issued guidance recommending that employers actively encourage sick employees to stay home. Interpreting this guidance, the Equal Employment Opportunity Commission (EEOC) confirmed that while the rules of the Americans with Disabilities Act (ADA) and the Rehabilitation Act continue to apply, those rules do not interfere with or prevent employers from following guidelines and recommendations from the CDC and state/local public health authorities about how employers should handle COVID-19. Specifically, under the EEOC's guidance, employers may:

- ask employees who report feeling ill at work, or who call in sick, questions about their symptoms to determine if they have or may have COVID-19;
- require employees to stay home if they have symptoms of the COVID-19;
- screen applicants for symptoms of COVID-19 in the hiring process;
- delay the start date of an applicant who has COVID-19 symptoms; and
- withdraw the job offer of an applicant with COVID-19 symptoms since this individual cannot safely enter the workplace.

As such, employers may find it necessary to ask employees about their symptoms, require notification of higher than normal body temperatures, and require self-declarations regarding employees recent proximity to individuals who have tested positive for COVID-19. While employers may ask employees to provide limited health-related information specific to COVID-19, employers must be mindful to pose such questions and/or requests on a consistent basis and avoid discriminatory use of the results. To avoid collecting unnecessary information, employers may simply ask employees to stay home if they

show certain symptoms, rather than asking them about the specific symptoms they have.

Multinational companies deploying global responses to those questions and trying to set-up harmonized policies across their organizations will need to remain cognizant of regional or domestic frameworks and guidelines. In the European Union, data privacy in the employment context is one of those areas where the General Data Protection Regulation (GDPR) authorized national laws to impose specific requirements. The European Data Protection Board (EDPB) emphasized that the principles of proportionality and data minimization (i.e., collection of minimum necessary personal data) are amongst the most relevant to consider in relation to the collection of specific health information in the context of COVID-19. In line with the EDPB, the UK's Information Commissioner's Office (ICO) indicated that it is reasonable for businesses to ask individuals with whom they come into contact, such as members of staff or visitors, whether they are experiencing COVID-19 symptoms, but organizations may not need to collect more specific information about individuals' health conditions and should not collect more personal data than they need.[20] The view of the French data protection supervisory authority (CNIL) is somewhat more restrictive. In its guidelines, the CNIL mentioned that employers should refrain from collecting in a systematic and generalized manner, or through surveys and individual requests, information relating to potential symptoms of an employee and their relatives.[21] Similar principles can be found in guidelines issued by the Belgian and Italian data protection authorities.[22] The German Datenschutzkonferenz, a collective body comprising independent federal and state data protection supervisory authorities, added other aspects in recent guidelines by reminding that health data must be kept confidential, used solely for the intended purpose and deleted once the purpose is achieved (as a general rule, after the end of the pandemic).[23]

2. Conducting or requiring examinations of employees

COVID-19 presents certain unique data privacy challenges for employers, particularly as companies contemplate how and whether to collect medical data for the purposes of responding to this pandemic. As the companies try to do their part to "flatten the curve," a key question to consider is whether the information gathered from employees regarding their health status is a proportionate and reasonable response to the pandemic.

In the United States, the ADA generally regulates employer disability-related inquiries and medical examinations and imposes a wide range of restrictions on companies, including limiting when employers may conduct "medical examinations" of employees and protecting employees' confidential medical information.

The ADA generally prohibits covered employers from requiring medical examinations of employees unless such examinations are job-related and consistent with business necessity.[24] To meet that standard, an employer must have a reasonable belief, based on objective evidence, that (i) an employee's ability to perform essential job functions will be impaired by the medical condition, or (ii) an employee will pose a "direct threat" to himself/herself or to others due to the medical condition.[25] Given the current push for companies and individuals to "flatten the curve," employers may choose to recommend that employees check their own temperature before coming to work or once arriving at work, as part of an effort to stop the spread of the virus, particularly in the workplace.

However, the EEOC recently updated its prior technical assistance document from the H1N1

pandemic, entitled "Pandemic Preparedness in the Workplace and the Americans with Disabilities Act" to address COVID-19.[26] "Because the CDC and state/local health authorities have acknowledged community spread of COVID-19 and issued attendant precautions as of March [11] 2020," the guidance reads, "employers may measure employees' body temperature. As with all medical information, the fact that an employee had a fever or other symptoms would be subject to ADA confidentiality requirements."

In the European Union, the EDBP reminded employers that they should only access and process health data if their own legal obligations allow it. Although the Belgian data protection authorities have indicated that temperature testing might not be a processing activity under the GDPR to the extent that no actual storage or recording is made of the data, other data protection authorities in the European Union such as German or French ones have rejected the permissibility of such testing.[27] Employers planning to examine their employees should discuss any contemplated mandatory medical tests or examinations, including temperature-taking, with their legal counsel before adopting or implementing such measures.

3. Sharing health information

Employers should be mindful that the ADA establishes the basic rule that, with limited exceptions, employers must keep confidential any medical information they learn about an applicant or employee.[28] The CDC's guidance reminds employers to maintain the confidentiality of employees with confirmed COVID-19. Therefore, with respect to any notices to the workplace regarding potential or confirmed COVID-19 cases, employers should avoid including the employee's name and avoid including any identifying factors about the employee (e.g., job title).

With respect to a health care provider sharing information about an employee with an employer, HHS's March 2020 COVID-19 & Health Insurance Portability and Accountability Act (HIPAA) Bulletin emphasized that in the event of a nationwide public health emergency, such as the COVID-19 pandemic, health care providers may share patient information with "anyone necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public. . . ."[29] This presumably includes disclosure of the patient's information to their employer, so long as the employer is in a position to "prevent or lesson the serious and imminent threat…" HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety.[30] HHS issued guidance stating that federal health privacy law authorizes employers to request protected health information from health care providers without employees' consent, if necessary to "prevent a serious and imminent threat." The guidance makes clear, however, that health care providers are not required to provide the information, and should use their own professional judgment in deciding whether to do so.

In the European Union, the EDBP has observed that even if employers should inform staff about COVID-19 cases and take protective measures, no more information than necessary should be communicated (especially not the name of the affected individuals) unless so required by national laws. In line with the EDPB statement, in the UK, the ICO observed that it is probably not necessary to name the affected individual(s), unless it is strictly required to protect other individuals. In cases where it is necessary to reveal the name of the person concerned, the individual concerned should be informed in advance and their dignity and integrity protected.[31] Similar principles have been stated by other

European data protection authorities.[32]

4. Disclosure of travel plans

The World Health Organization (WHO) declared COVID-19 a pandemic on March 11, 2020. In order to prevent the further spread of the virus, American citizens who have traveled to "high risk" countries must self-quarantine for a period of 14 days. While travel outside of the United States is not strictly prohibited, on March 19, 2020, the U.S. Department of State issued a Level 4 "Do Not Travel" advisory, warning U.S. citizens to avoid all international travel due to the global impact of COVID-19. Given the quarantine requirement and travel advisory, employers may ask employees questions about exposure to COVID-19 during recent travel, and may ask employees to disclose the locations they have traveled to, even if the travel was not work-related. (In the European Union, data privacy principles requires companies to document the actions undertaken to this end and the information collected.)

The CDC guidance warns, however, that in order to "prevent stigma and discrimination in the workplace, [employers should] use" the CDC's guidance and recommendations to determine an employee's risk of COVID-19. Determinations about an employee's status should not be made based on race or country of origin.

5. Compliance with the CCPA's disclosure requirements

Amid companies' efforts to "flatten the curve" and prevent the spread of the virus, companies have likewise continued to work to maintain compliance with the California Consumer Privacy Act (CCPA), which took effect on January 1, 2020. One of the new requirements that the CCPA imposes on employers is the obligation to provide employees, at or before the point of collection of their personal information, with a notice that details what personal information the employer will be collecting about them and what the employer will be doing with that information. An employer may not "collect categories of personal information other than those disclosed in the notice of collection" and if an employer intends to collect new categories of personal information, then it must first provide a new notice at collection.[33] Similarly, an employer may not use personal information for a materially different purpose than those disclosed in the notice at collection unless it notifies the employee and obtains explicit consent from them.

Accordingly, companies will need to make sure that, prior to collecting any of the information described above (such as travel information), the company has first provided a notice to its employees detailing what information will be provided and how that information will be used. If a company has already provided such a notice to its employees, it will need to make sure that the notice adequately covers this new information and the COVID-19-related purposes for which it will be used; otherwise, the notice will be need to be updated and consent may need to be obtained from the employee.

6. Collection of Geolocation Data

Recent reports indicate that various groups are developing tools that will alert people to self-isolate if they are identified as having recently been in contact with someone diagnosed with COVID-19. These tools will rely on collecting and monitoring large amounts of geolocation and health information about individuals on an ongoing basis in order to be effective. They could be either used by companies or pursued more broadly by public authorities as part of their measures to fight the spread of the virus.

The deployment of these types of technologies could have numerous benefits in terms of protecting public health and helping public and private sector organizations manage and minimize disruption within their workforce. However, such tools will raise questions of how to deploy them consistently with data privacy laws (and other relevant legal principles) in the jurisdictions in which they may be implemented. Privacy questions also will arise from efforts to use anonymous location data to predict areas where a serious outbreak might occur or to analyze the effectiveness of social distancing measures.

In the European Union, the General Data Protection Regulation (GDPR) and the ePrivacy directive and its local implementation across Member States will have to be considered. The EDPB has cautioned that while the GDPR should not hinder measures taken in the fight against the pandemic, controllers are still responsible for ensuring the protection of personal data and ensuring that they process it in accordance with the existing legal requirements. In that context, the EDPB has explained that collection of aggregated/anonymized data is preferable where possible.[34] (While anonymized data is not subject to privacy regimes, businesses should consider whether any such data is anonymized in such a manner that it cannot be traced back to individuals.)

Authors

- Marcus A. Christian
- Raj De
- Régine Goury
- Charles Helleputte
- Stephen Lilley
- Mark Prinsley
- Andrew Rosenman
- Lei Shen
- David Simon
- Jeff Taft
- Ulrich Worm
- Oliver Yaros
- Vanessa Klesy
- Björn Vollmuth
- Ana Bruder
- Diletta De Cicco
- Veronica Glick
- Niketa Patel
- Gabriel Perlman
- Joshua Silverstein
- Amber Thomson

[1] Krebs on Security, "Live Coronavirus Map Used to Spread Malware, Krebs on Security" (Mar. 20, 2020), available at https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/.

[2] *See* The Hill, "Top US Health Agency Suffer Cyberattack" (Mar. 16, 2020), available at

https://thehill.com/policy/cybersecurity/487756-top-us-health-agency-suffers-cyberattack-report.

[3] *See* Healthcare IT News, "Cyberattack on Czech Hospital Forces Tech Shutdown During Coronavirus Outbreak" (Mar. 19, 2020), available at https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak.

[4] As discussed below, the large-scale collection of location data is one of the most significant data privacy challenges facing governments in the European Union.

[5] *See* ARS Technica, "The Internet is Drowning in COVID-19-Related Malware and Phishing Scams" (Mar. 16, 2020), available at https://arstechnica.com/information-technology/2020/03/the-internet-is-drowning-in-covid-19-related-malware-and-phishing-scams/.

[6] *See* Sherrod DeGrippo, TA505 and Others Launch New Coronavirus Campaigns; Now the Largest Collection of Attack Types in Years (Mar. 16, 2020), *available at* https://www.proofpoint.com/us/corporate-blog/post/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack.

[7] Federal Bureau of Investigation, *FBI Sees Rise In Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic*, Alert No. I-032020-PSA (Mar. 20, 2020), *available at* https://www.ic3.gov/media/2020/200320.aspx.

[8] Cybersecurity and Infrastructure Security Agency, "Defending Against COVID-19 Cyber Scams" (Mar. 6, 2020), available at https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.

[9] *See* Federal Trade Commission, "Coronavirus Scams: What the FTC is Doing" (last accessed Mar. 22, 2020), available at https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing.

[10] *See* New York State Department of Financial Services Alert (last accessed Mar. 22, 2020) available at https://www.dfs.ny.gov/consumers/alerts/coronavirus.

[11] *See* "Top Tips for Cybersecurity when Working Remotely" (Mar. 15, 2020), available at https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely.

[12] Available here: https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html.

[13] *See* Lily Hay Newman, *Corona Virus Sets the Stage for Hacking Mayhem*, Wired.com, available at https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/.

[14] Many of those security tools are highlighted by ENISA in its recently issued security recommendations, discussed above.

[15] *See* U.S. Department of Health and Human Services, "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency" (Mar. 19, 2020), available at

https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

[16] *See*, *e.g.*, the statement adopted by the European Data Protection Board on March 19, 2020 (discussed in more details below), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[17] *See* The Financial Reporting Council, "Guidance on Audit Issues Arising from the Covid-19 (Coronavirus) Pandemic" (Mar. 16, 2020), available at https://www.frc.org.uk/news/march-2020-(1)/guidance-on-audit-issues-arising-from-the-covid-19.

[18] *See* the U.S. Securities and Exchange Commission, "SEC Coronavirus (COVID-19) Response" (last modified Mar. 20, 2020), available at https://www.sec.gov/sec-coronavirus-covid-19-response.

[19] *See* New York State Department of Financial Services Order (Mar. 12, 2020), available at https://www.dfs.ny.gov/system/files/documents/2020/03/ea20200312_covid19_relief_order.pdf.

[20] *See* the ICO blogpost available here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/covid-19-general-data-protection-advice-for-data-controllers/.

[21] *See* the CNLI statement issued on March 6, 2020 available here: https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles.

[22] *See* the Belgian data protection guidelines issued on March 13, 2020 available: https://www.autoriteprotectiondonnees.be/covid-19-et-traitement-de-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel-sur-le-lieu-de-travail and the Italian data protection guidelines issued on March 2, available here: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117#1.

[23] *See* BfDI, Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie, available at https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/07_Empfehlungen_Datenschutz_Corona.html.

[24] "The term 'covered entity' means an employer, employment agency, labor organization, or joint labor-management committee. . . . The term 'employer' means a person engaged in an industry affecting commerce who has *15 or more employees* for each working day in each of 20 or more calendar weeks in the current or preceding calendar year" (emphasis added). 42 U.S.C. §12111.

[25] Such restrictions do not apply to visitors or other non-employees.

[26] *See* U.S. Equal Employment Opportunity Commission, "Pandemic Preparedness in the Workplace and the Americans with Disabilities Act" (Mar. 21, 2020), available at https://www.eeoc.gov/facts/pandemic_flu.html.

[27] *See*, as an example, the position of some German data protection authorities available here: https://www.covid19.law/2020/03/compulsory-temperature-testing-and-the-protection-of-employee-data/.

[28] 42 U.S.C. § 12112(d)(3)(B).

[29] U.S. Department of Health and Human Services, "COVID-19 & HIPAA Bulletin – Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency" (Mar. 2020), available at https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf.

[30] 45 C.F.R. § 164.512(j).

[31] *See* the ICO blogpost available here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/covid-19-general-data-protection-advice-for-data-controllers/. For more information about the use of personal data of employees in the UK, *see* https://www.employerperspectives.com/2020/03/right-to-know-covid-19/.

[32] See, for example, the position of the Belgian data protection authorities or a more recent one issued on March 18 by the Greek data protection authorities, available here: https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=163,39,44,101,194,223,3,99.

[33] California Attorney General California Consumer Privacy Act Regulations – Proposed Text of Modified Regulations (March 11, 2020).

[34] See the European Data Protection Board statement adopted on March 19, 2020, available here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.