COVID-19: Regulator Guidance on Privacy and Cybersecurity Issues Raised as Companies Respond to the Pandemic [UPDATE 4: EU/UK Guidance on Contact Tracing Apps]

April 23, 2020

AUTHORS

Daniel K. Alvarez | Elizabeth Bower | Elizabeth P. Gray | Henrietta de Salis
Dominique Mondoloni

The Coronavirus (COVID-19) pandemic has given rise to unprecedented challenges for organizations of all shapes and sizes, from world governments and health care systems to local restaurants and retailers. As companies seek to navigate a path forward, privacy and data security concerns have become a central issue. For example, many companies are facing difficult questions about how to ensure they are complying with applicable privacy laws while also being transparent with employees, customers, and the public. Concurrently, hackers and other bad actors are taking advantage of the crisis to spread their own kinds of viruses and malware to infect and disrupt company systems and gain access to sensitive information.

In response to the issues faced and the questions being asked by organizations, regulators in the United States, United Kingdom (UK), and European Union (EU) have issued guidance on the privacy and data security implications of COVID-19 and how organizations respond. While some regulators seem to be taking a very rigid approach to the laws that they enforce, a number of regulators seem to recognize the gravity and pressures of the situation and have issued guidance reflecting the importance of balancing sometimes competing interests. And at last one regulator has issued a waiver of

certain rules to facilitate easier online access to telehealth-based healthcare services.[1] In this updated client alert, we want to highlight guidance, opinion, and developments that have been released since our last Update Alert on April 15. For a list of releases, blog posts, guidance, and other announcements by privacy regulators in the United States, UK, and EU, please see Appendix A.

- *Don't Forget About Privacy Laws.* A central theme reiterated by almost every regulator is that the unprecedented nature of the situation does not mean we can ignore or otherwise discount the importance of privacy laws. In Europe, for example, the Belgian regulator emphasized that privacy rights established under the General Data Protection Regulation (GDPR) are not incompatible with public health and disease prevention goals. The Italian data protection authority stated that while companies are allowed to collect information related to COVID-19 symptoms, it must be done in a way consistent with the GDPR's privacy principles. In the United States, the Department of Health and Human Services (HHS) issued guidance, among other reasons, "to serve as a reminder that the protections of the [HIPAA] Privacy Rule are not set aside during an emergency."

- *Know What Law Applies.* The rapid pace at which decisions must be made in the face of a crisis like this pandemic makes it easy to forget the maze of privacy laws that may apply to a company's data-handling activities. This is especially true in the United States, where different laws may apply depending on the context in which the data at issue was collected. For example, as part of its guidance, HHS sought to remind readers that the HIPAA Privacy Rule applies only to covered entities (health plans, health care clearinghouses, and health care providers) and business associates. HIPAA does not apply generally to health-related information in the hands of companies that are not covered entities or business associates, though other laws may. Likewise in the EU, member states may interpret and therefore apply GDPR differently. Being clear as to which jurisdiction's laws apply, or which laws apply within a jurisdiction, is critical.

- *Be Mindful About the Information You Collect and How You Collect It.* Companies should not assume that because they think collecting certain information will be important to their COVID-19 response, they are allowed to collect the information – or require it of their employees or customers. For example, the CNIL in France has said that companies should refrain from collecting information related to possible COVID-19 symptoms presented by employees, visitors, or customers, and that the collection and assessment of information related to COVID-19 symptoms is the responsibility of public health authorities, not individual companies. In contrast the UK's Information Commissioner's Office (ICO) has recognized that it may be proportionate to collect data regarding where employees and visitors to offices have travelled or whether they have symptoms. The Irish data protection authority stated that while "[d]ata protection law does not stand in the way of the provision of healthcare and the

[1] *See* Press Release, Dep't of Health and Human Services, OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, March 17, 2020, here.

management of public health issues," companies still have an obligation to ensure that the measures they take in response with respect to personal data "should be necessary and proportionate."

- *Understand How You Will Use and Share the Information You Collect Before Collecting It.* If you are collecting information for purposes related to your company's response to the pandemic, consider appropriate controls and safeguards to ensure that such information is used only for that purpose. The guidance from the ICO in the UK explained that it is acceptable to inform staff that a co-worker has contracted the virus but this can be done without disclosing the name of the individual unless necessary. And German data protection authorities explained that information collected for the purpose of COVID-19 containment may be used only for that purpose and must be deleted once the pandemic is contained. In the United States, HHS guidance emphasized that disclosure should be limited "to that which is the 'minimum necessary' to accomplish the purpose."

- *Stay Alert for Fraudsters and Other Bad Actors.* Data security and good cyber hygiene remain critical components of any company's response plans, particularly in light of the extensive remote working and online activity that will be asked of many employees. In its guidance, the Irish data protection authority affirmed that "[a]ny data processing in the context of preventing the spread of COVID-19 must be carried out in a manner that ensures security of the data, in particular where health data is concerned." These concerns are heightened by the fact that many bad actors are seeking to leverage the crisis to their own advantage – see, for example, the COVID-19 tracking app for Android that has been identified as ransomware.[2] In the United States, the Federal Trade Commission and the Food and Drug Administration issued warning letters to seven companies selling scam COVID-19 treatments, the FTC is warning consumers to be particularly cautious about clicking on links from sources they do not know, and the Cybersecurity and Infrastructure Security Agency in the Department of Homeland Security has issued a Cyber Alert "reminding individuals to remain vigilant for scams related" to COVID-19. Even state agencies have been active, warning consumers and companies alike to stay vigilant.

March 24, 2020 Alert

Since our March 19, 2020 Client Alert, additional guidance has been issued by U.S., UK, and EU regulators that underscores the main points above, including specific recommendations for remote work and cybersecurity. For example, the National Institute of Standards and Technology (NIST) recently released a bulletin highlighting its Special Publication Series on enterprise risks related to remote work environments, which focuses on best practices for managing risk. Likewise, the EU and several member states have issued similar cybersecurity considerations: the Irish Data Protection Commission notes that organizations should clearly document telework policies, and the EU Agency for Cybersecurity (ENISA) notes, among other cybersecurity tips, that such policies should include clear escalation processes should vulnerabilities be identified or exploited.

[2] *See, e.g., Coronavirus tracking app is actually malware*, AndroidCommunity.com, March 17, 2020, here.

Moreover, regulators continue to express that reasonable data collection and usage practices likely do not violate applicable privacy laws. For example, the Equal Employment Opportunity Commission (EEOC) published a Frequently Asked Questions platform for high-level issues that may arise during this time, it has updated its Pandemic Preparedness guidelines to account for COVID-19, and issued guidance regarding the application of anti-discrimination laws in the workplace. The Federal Communications Commission (FCC) adopted a declaratory ruling confirming that the COVID-19 "constitutes an 'emergency' under the Telephone Consumer Protection Act (TCPA)" and therefore healthcare providers and government officials may communicate about the virus, its causes, and mitigating factors, without violating TCPA.

March 31, 2020 Alert

On March 24, 2020, three U.S. Senators sent a letter to the Chairman and Commissioners of the FTC and to the Secretary of Education noting that "[s]tudent privacy must not fall by the wayside as the current pandemic moves learning from the classroom to online offerings at home." Specifically, they sought clarification on how FERPA and COPPA applies to education technology services and providers and urged the agencies to release joint guidance on this issue. The letter does not address the memo or FAQs recently published by the Student Privacy Policy Office of the Department of Education. However, it does serve as a reminder to providers of remote-learning technologies and platforms, as well as other platforms that serve children and families, to be mindful of their obligations under these laws.

In California, reports suggest that a coalition of businesses have sought to delay enforcement of the California Consumer Protection Act (CCPA), based in part on the impact of COVID-19. These reports indicate that the Office of the California Attorney General (CA AG), however, has rejected the request.[3] CCPA has been in force since January 1, 2020, and the CA AG can begin taking enforcement actions on July 1, 2020.

April 15, 2020 Alert

Several regulators have developed and issued additional guidance, reiterating the continued applicability of governing regulations, but recognizing some of the unique issues highlighted by the COVID-19 pandemic. The FTC blogged about remote learning and children's privacy, noting that COPPA continues in force, as do the general requirements of parental consent, but it reiterated that "schools may consent on behalf of parents to the collection of student personal information by educational technology services." This collection must be limited to education – and not commercial – purposes. The EEOC supplemented its earlier COVID-19 guidance, reiterating that, as anti-discrimination laws continue, so too do filing deadlines, though it has temporarily suspended certain actions and decisions. The Securities and Exchange Commission stressed the importance of required disclosures, but also noting its longstanding acceptance of "well-reasoned judgments that entities have made."

[3] *See e.g., COVID-19 Will Apparently Not Delay CCPA*, The National Law Review (Mar. 26, 2020), here.

COVID-19: Regulator Guidance on Privacy and Cybersecurity Issues Raised as Companies Respond to the Pandemic [UPDATE 4: EU/UK Guidance on Contact Tracing Apps]

The use of personal data for tracking and pandemic response efforts is center stage for many regulators. The European Data Protection Board, for instance, has mandated its expert subgroups to develop and issue guidance on geolocation tracking and data anonymization, as well as the processing of health data for research purposes. The European Commission has likewise issued a recommendation proposing a common approach to the use of technology and data to combat the pandemic.

UPDATE: April 23, 2020

The European e-Health Network published a guide to a common EU "toolbox" that explains the essential requirements for national contact tracing and warning apps. The apps should be voluntary; approved by the national health authority; privacy-preserving – personal data must be securely encrypted; and dismantled as soon as no longer needed. The guide was published as part of the European Commission's recommendation adopted on April 8, 2020, and the European Commission published a guidance that also requires these apps to be in compliance with the EU privacy and data protection laws. Among other things, the guidance provides that the apps should be designed in a manner that the national health authorities (or entities carrying out tasks in the public interest in the field of health) are data controllers.

The UK ICO published an opinion with respect to the joint initiative by Apple and Google on a Contact Tracing Framework (CTF). ICO assessed that CTF appears to be aligned with the principles of data protection by design and default, including compliance with the data minimization principle. ICO noted that the CTF is designed to generate a limited amount of data from the user's device, including "tokens" that are not associated with other data that may identify or locate the device user. ICO emphasized that the procedures for collecting specific consent from app users must be addressed before the apps are rolled out.

On April 21, 2020, the European Data Protection Board (EDPB) adopted two guidelines that address COVID-19. The guideline concerning the processing of health data for research purposes recognizes that the scientific and medical research conducted by both public authorities and private entities serves important public interest. With respect to international data transfers for scientific purposes, the guideline provides that private entities may rely upon Article 29 derogations – transfer necessary for important reasons of public interest and explicit consent from data subjects – in the absence of an adequacy decision or appropriate safeguards. The guideline on geolocation and other tracing tools emphasizes that in the context of a contact tracing app, proximity data should be used as these apps do not require tracking the location of individual users.

Willkie is continuing to monitor the regulators' responses and will provide regular updates. Meanwhile, if you have any questions about whether your plans potentially trigger any privacy or data security concerns, please do not hesitate to reach out to Willkie's team of experts.

Appendix A: Regulator Guidance, Releases, and Blog Posts

Jurisdiction	**Links to Guidance**
U.S.	• Department of Education, COVID-19 ("Coronavirus") Information and Resources for Schools and School Personnel • Department of Education, Student Privacy Policy Office, FERPA & Coronavirus Disease 2019 (COVID-19) Frequently Asked Questions (FAQs) • Department of Education, Student Privacy Policy Office, FERPA and Virtual Learning Related Resources • Department of Health and Human Services, Office for Civil Rights, Bulletin: HIPAA Privacy and Novel Coronavirus • Department of Health and Human Services, COVID-19 and HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties during a Nationwide Public Health Emergency • Department of Education, Student Privacy Policy Office, COVID-19 and HIPAA: Disclosures to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities • Equal Employment Opportunity Commission, Pandemic Preparedness in the Workplace and the Americans with Disabilities Act • Equal Employment Opportunity Commission, EEOC Continues to Serve the Public During COVID-19 Crisis • Federal Communications Commission, Consumer and Governmental Affairs Bureau Assures Public Health Officials that Pandemic-Related Emergency Robocalls are Lawful under the TCPA • Federal Trade Commission, Coronavirus Scams: What the FTC is Doing • Federal Trade Commission, Remote Learning and Children's Privacy • Federal Trade Commission, COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus • Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Defending Against COVID-19 Cyber Scams

	• National Institute of Standards and Technology, Security for Enterprise Telework, Remote Access, and Bring Your Own Devices (BYOD) Solutions • Securities and Exchange Commission, Statement on the Importance of High-Quality Financial Reporting in Light of the Significant Impacts of COVID-19 • U.S. Senate, Letter to the FTC and Department of Education regarding Student Privacy (March 24, 2020) • Washington, State Office of Cybersecurity, Phishing attacks use coronavirus outbreak to trick victims
Australia	• Office of the Australian Information Commissioner, COVID-19
Austria	• Data Protection Authority, Datensicherheit und Home-Office (in German)
Belgium	• Data Protection Authority, COVID-19 et traitement de données à caractère personnel sur le lieu de travail
Canada	• Office of the Privacy Commissioner of Canada, Privacy and the COVID-19 Outbreak
Denmark	• Data Protection Authority, Gode råd om hjemmearbejde (in Danish)
European Union	• European Union Agency for Cybersecurity, Top Tips for Cybersecurity When Working Remotely • UPDATE: European Commission, Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data • ***UPDATE: European Commission, Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection*** • European Data Protection Board, Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak • European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak (adopted March 19, 2020)

	• European Data Protection Board, Request for Mandate regarding geolocation and other tracing tools in the context of the COVID-19 outbreak – Technology ESG • European Data Protection Board, Request for mandate regarding the processing of health data for research purposes in the context of the COVID-19 outbreak – CEH ESG • ***UPDATE: European Data Protection Board, Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*** • ***UPDATE: European Data Protection Board, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*** • European Data Protection Supervisor, Letter re Monitoring the Spread of COVID-19 • ***UPDATE: eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States***
France	• CNIL, Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles (in French)
Germany	• Federal Commissioner for Data Protection and Freedom of Information, Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie (in German)
Iceland	• Data Protection Authority, COVID-19 og persónuvernd (in Icelandic)
Ireland	• Data Protection Commission, Data Protection and COVID-19 • Data Protection Commission, Five Steps to Secure Cloud-based Environments
Italy	• Garante Privacy, Coronavirus: No do-it-yourself (DIY) data collection, says the Italian DPA (in Italian and in English)
Liechtenstein	• Data Protection Authority, Datenschutz im Home-Office (in German)
Netherlands	• Data Protection Authority, Veilig thuiswerken tijdens de coronacrisis (in Dutch)

New Zealand	• Office of the Privacy Commissioner, Civil Defense National Emergencies (Information Sharing) Code 2013 • Office of the Privacy Commissioner, COVID-19 and Privacy FAQs • Office of the Privacy Commissioner, Employee Health Privacy for GPs in a Covid-19 World
Spain	• Data Protection Authority, Campañas de phishing sobre el COVID-19 (in Spanish) • Data Protection Authority, Report from the State Legal Service on Processing Activities Relating to the Obligation for Controllers for Private Companies and Public Administrations to Report on Workers Suffering from COVID-19
U.K.	• Information Commissioner's Office, Data protection and coronavirus: what you need to know • ***UPDATE: Information Commissioner's Office, Opinion: Apple and Google joint initiative on COVID-19 contact tracing technology***

Willkie has multidisciplinary teams working with clients to address coronavirus-related matters, including, for example, contractual analysis, litigation, restructuring, financing, employee benefits, SEC and other corporate-related matters, and CFTC and bank regulation. Please click here to access our publications addressing issues raised by the coronavirus. For advice regarding the coronavirus, please do not hesitate to reach out to your primary Willkie contacts.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Henrietta de Salis
+44 20 3580 4710
hdesalis@willkie.com

Dominique Mondoloni
+33 1 53 43 45 68
dmondoloni@willkie.com