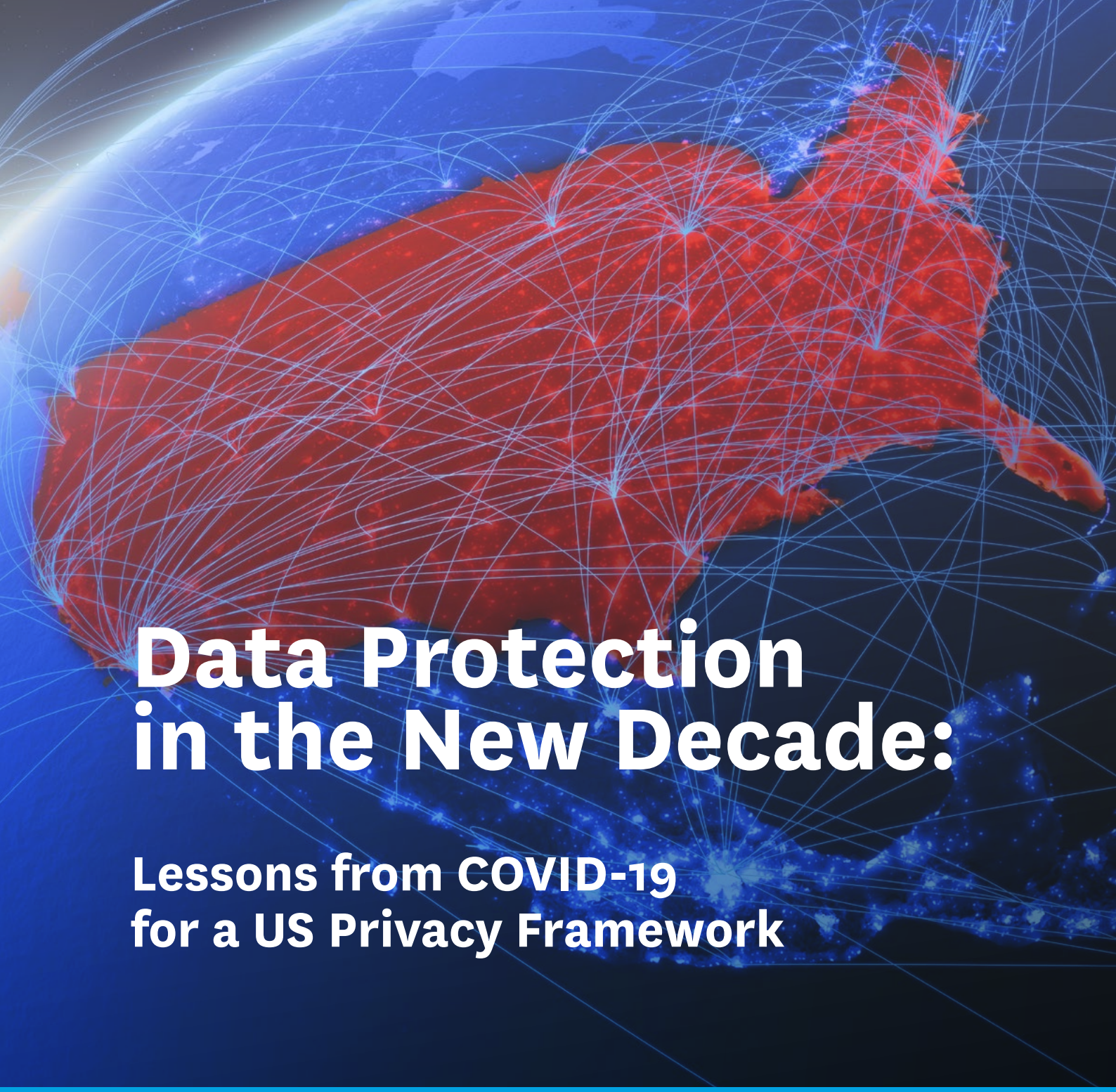

Data Protection in the New Decade:

Lessons from COVID-19 for a US Privacy Framework

August 2020

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Data protection is constantly evolving, and the global experience with COVID-19 in 2020 has offered valuable lessons to help guide that evolution in the future. Digital data and technologies have assumed an even greater importance in economic activity, social connectivity, and public health. Assuring the effective and responsible use of those data and technologies to respond to and recover from COVID-19 will require agile privacy regulations and accountable business practices as companies and governments operate in a rapidly changing environment. In the longer term, the growing role for digital data and technologies has demonstrated once again the need to replace the US patchwork of fragmented state privacy laws with a comprehensive federal privacy framework, and to make sure that framework is aligned with federal sectoral privacy laws.

This discussion paper highlights some of the key data protection lessons from COVID-19. It focuses on providing guidance to inform development of a comprehensive US federal privacy framework, while also drawing on the broader context of other nations and regions.

1. Personal data is essential infrastructure.

When the economy otherwise would have come to a grinding halt as governments issued stay-at home orders, Internet-based tools have kept universities, schools, businesses, governments, and other key parts of our economies and societies operating.

One of the most striking takeaways from the pandemic has been the unmistakable power of personal data and the technologies that facilitate its collection and use. When the economy otherwise would have come to a grinding halt as governments issued stay-at home orders, Internet-based tools have kept universities, schools, businesses, governments, and other key parts of our economies and societies operating. Retail, industrial supply, shareholder meetings, education, entertainment, and most of our social lives have moved online. For younger people, this was no surprise and only continued a familiar trend, but for many the now-sweeping prevalence of Zoom, Skype, FaceTime, Microsoft Teams, Google Meet, TikTok, and numerous other platforms continues to astonish. This digital transformation has led to new business models, processes, and practices, many of which are likely to remain post-COVID-19.

Similarly, the use of data has been essential for responding to the pandemic. Data has been at the center of research on vaccines and treatments, COVID-19 and antibody testing, deploying contact tracing, enforcing quarantines, limiting public gatherings, enforcing other public health measures, engaging in research, and ensuring a safe working environment. Equally, data and technology will be critical to enabling lock-down exit strategies, safe return to work and school protocols, and reopening and re-igniting our economy.

Some of these purposes can be achieved with aggregated or anonymized data, but for many purposes, granular personal data is required. These and other important uses for personal data have not only highlighted the importance of these data, but have also placed greater emphasis on responsible data sharing between and among businesses and government organizations.

Data protection regulations that may have appeared rational and effective in the drafting room have posed issues when confronted with escalating demands for data and connectivity.

The importance of personal data, data sharing, and these applications has illuminated key data protection issues. Comparatively small companies, such as Zoom, have overnight assumed giant proportions in our COVID-19 economy and have needed to scale quickly, posing new challenges for privacy and security.[1] This highlights the importance of ensuring that data protection measures are scalable and efficient. Data protection regulations that may have appeared rational and effective in the drafting room have posed issues when confronted with escalating demands for data and connectivity. In the US, the Department of Health and Human Services (HHS) granted a waiver of penalties for "good faith use of telehealth during the emergency," and relaxed other restrictions applicable to telemedicine and the protection of health-related data in an effort to ensure that Americans had reliable access to healthcare from their homes.[2] At the same time, the extraordinary reliance on personal data drawn from a wide variety of sources has once again highlighted the need for greater, more efficient, and equitable access to data by both private- and public-sector entities.

The need for data protection laws that are both effective and efficient has been amply demonstrated as smaller companies have experienced growing pains, while giant companies are navigating questions about how to use and share vital personal data and addressing the consequences of inadequate data access or sharing. Never before has the need for data protection laws that both protect privacy and facilitate the responsible use of data and technologies been so clear.

2. Artificial intelligence applications are especially essential.

The importance of personal data has been especially clear in the use of artificial intelligence (AI). AI, which usually relies on large amounts of data, has played a critical role in most of the data uses mentioned above. AI is at the heart of the development of the COVID-19 vaccines currently being tested, and is also essential for various apps developed to diagnose, track, and trace the disease, as well as enable the safe return to work, public transportation, and public spaces. Other important uses of AI in the response to the pandemic include AI applications for:

- Developing and assessing new medicines;
- Performing automated tracing of people in contact with COVID-19 carriers;
- Assisting with automated quarantine measures so individuals can quarantine at home rather than in a government facility;
- Powering models for predicting the spread of coronavirus and the effectiveness of various government and private-sector protective measures; and
- Protecting the security of the networks and applications on which we all depend, and which are more under attack than ever before.

Governments, businesses, and researchers have recognized the enormous potential of AI to transform society, including everything from improving healthcare, to creating efficiencies in the workplace, to streamlining research efforts, to revolutionizing the economy. While understanding the importance of AI to the future of society, some regulators have also approached AI with a heavy dose of caution, as if the potential risks of AI tools could be managed by trying to restrict development of the technology itself.

In the face of these and other critical functions that AI is serving, it seems increasingly clear that we need to develop tools for protecting privacy in the AI context that do not seek to impede development of the technology itself. To be sure, we need proper guardrails to guide the responsible development and deployment of AI and associated tools, but the response to COVID-19 has highlighted the importance of fostering these new technologies and applications.[3]

3. Privacy is one of many fundamental rights.

The right to privacy is fundamental, and its importance has been once again demonstrated by the responses to COVID-19. But the right to privacy is not absolute and must be balanced with other important fundamental rights and values, such as healthcare and freedom of movement. We have long known that in times of crisis, governments and individuals have an understandable tendency to prioritize security, whether national security or public health. If data protection laws are too burdensome or too inflexible, they risk being compromised in such trying times. Fortunately, fundamental rights are not an either/or question. It is possible to protect privacy while responding effectively to a public emergency, but doing so requires well-tailored laws, flexible administration and implementation grounded in organizational accountability, and rigorous enforcement in the absence of good faith efforts to comply.

In the US, privacy outside of government intrusions is not explicitly recognized as a fundamental human right, and current privacy laws often depend on the industry being regulated and the state where an individual resides. For example, in the healthcare industry—one of the few sectors with federal privacy regulation—personal health information, as defined under the Health Insurance Portability and Accountability Act (HIPAA), may or may not be protected depending on who possesses the data.[4] COVID-19, and the reliance of our most effective responses on personal data, have accentuated the need to recognize privacy as a fundamental right and afford it more consistent federal protection. Large swaths of the private sector are not subject to any privacy legislation other than to the FTC Act's prohibition against unfair and deceptive business practices, which also applies to data practices. The gaps in regulation can result in varied and inconsistent approaches to privacy for US citizens, even though data itself ignores sectoral or geographic divides.

In the EU, privacy has perhaps been treated in the data protection community too singularly above other human rights. Although the General Data Protection Regulation (GDPR) set a new standard for comprehensive data protection laws

around the globe, it did not provide enough clarity around how to balance privacy among other fundamental rights. At least 29 different pieces of guidance have been issued by European data protection authorities (DPAs) on how to balance privacy and data protection while responding to the pandemic.[5] The Global Privacy Assembly has assembled a COVID-19 Taskforce to address pandemic-specific concerns and best practices with hopes of providing consistency across geographies "while finding the right balance between supporting innovation to combat the pandemic and ensuring people's personal data and information rights are respected."[6] A greater, more explicit recognition that privacy is one of a number of fundamental rights might lead to a more balanced, flexible, and efficient application of data protection.

4. Traditional interpretations of principles of data protection have proven insufficient to provide adequate protection.

The global response to combatting COVID-19 has challenged traditional interpretations of privacy principles. This is not the first time that innovative uses of data have challenged long-standing notions of privacy. Artificial intelligence, and big data and blockchain before that, have highlighted the inadequacies of many of the privacy principles that emerged from the OECD in 1980.[7] Technologies and needs have changed over the past 40 years; data protection tools must keep up. As CIPL noted earlier this year, "[o]ur digital world and society need new and different approaches to regulating data privacy, while still empowering individuals."[8]

Nowhere is the inadequacy of some data protection tools clearer than in the case of individual consent. Conventional approaches to privacy protection have long relied on consent as the most important method to protect individual privacy. In the US, notice and consent are heavily entrenched keystones of privacy. Critics have argued for years that this framework is insufficient to protect individual privacy or afford meaningful individual choice. If consent is defined broadly, or if it is possible to require consent to use a service, then consent is not serving its intended purpose. Rather, the notion of consent may present an illusory choice to individuals, particularly when a product or service cannot be provided without the use of personal data. It instead often serves to protect organizations from liability. Furthermore, the burden of notice and consent on individuals can result in consent fatigue, rendering many of their choices meaningless.[9] FTC Commissioner Rebecca Slaughter summarized the limitations of notice and consent in an FTC hearing in April 2019:

> [F]or a notice and consent regime to be effective, both elements must be meaningful—notice must give consumers information they need and can understand, and consumers must have a choice about whether to consent. I am concerned that today, when it comes to our digital lives, neither notice nor consent is meaningful.[10]

The EU recognized the limits of consent when drafting the GDPR, and regulators have noted that consent without choice is not truly consent. Recital 42 states: "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."[11] Nevertheless, in the GDPR, consent is the first listed basis for processing to be lawful (art. 6), the first exception to the general prohibition for processing special categories of personal data (art. 9), and the first basis for permitting transfers of personal data to third countries lacking adequate data protection (art. 49). While this ranking is not intended to confer a privileged status on consent, it nevertheless has contributed to a culture that still promotes consent as the primary means of ensuring data protection.

[O]ur overreliance on consent for decades has reduced the effectiveness of data protection law and led to broad exceptions or meaninglessly broad consent requests.

COVID-19 has demonstrated one of the key inadequacies of consent: there are many uses of data for which consent is not desirable or possible, such as developing a vaccine for the greatest pandemic of the past century, enforcing quarantine, or contact tracing for people who have been exposed to the coronavirus, not to mention protecting national security, enforcing criminal laws, and conducting life-saving research. Consent can indeed play an important role in data protection when there are meaningful choices to be made, but our overreliance on consent for decades has reduced the effectiveness of data protection law and led to broad exceptions or meaninglessly broad consent requests.

5. The focus on collection of data is less important than the use of data after collection.

Many data protection requirements, particularly in the US, revolve around the initial collection of data. For example, the strongest privacy protection in the US—the Fourth Amendment right against unreasonable searches and seizures—explicitly has been limited to data collection only; once the government has the data, it may generally do with the data as it wishes.[12] Furthermore, the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA), the two US federal laws designed to provide "Fourth Amendment like protections" to electronic records, primarily govern the procedures for accessing electronic communications, but do not set use or storage limitations after the initial collection parameters are met.[13] Focusing on collection as the primary means of protecting individuals is problematic because there are always legitimate reasons for collecting data—protecting borders, prosecuting crime, preventing terrorist attacks, enforcing tax laws, etc.

The COVID-19 pandemic has demonstrated other compelling reasons for collecting and using sweeping personal data—testing, tracing, enforcing quarantines and other public health measures, conducting research—but almost all involve data that most people would not want used for other purposes without a separate, similarly compelling reason.[14] For example, tracking location data is inappropriate in many cases, but it is critical when tracking, tracing, and stopping the spread of a global pandemic. Similarly, disclosing health data to employers or the government would be

unacceptable in most circumstances, but COVID-19 has demonstrated a legitimate need for this information to help ensure the safety of the public. These examples highlight the importance of considering not only initial data collection, but also data use.

Finally, responses to the COVID-19 pandemic highlight the importance of applying a risk- or harm-based approach to data use. "Data used in one context for one purpose or subject to one set of protections may be both beneficial and desirable, where the same data used in a different context or for another purpose or without appropriate protections may be both dangerous and undesirable."[15] Focusing future privacy legislation on data use will create more desirable outcomes for individuals and society because it permits or excludes data uses based on their actual risk and the available mitigations and helps to ensure that data is used responsibly.

6. With less reliance on consent, we must develop and use a wider variety of tools to move to an accountability-based model of data protection.

COVID-19 has provided ample evidence of the need for more focused and flexible tools that help ensure organizational accountability without impeding innovations that may literally be lifesaving. Many of these tools already exist to not only ensure legal compliance, but also to help organizations—without waiting for regulators or laws—engage in responsible and accountable data use. This is particularly important when moving beyond consent to focus instead on legitimate interests or public benefits, and balancing the benefits of intended data uses against harms that might result. A few of examples of relevant accountability tools include:

- **The CIPL Accountability Framework:** This organizational accountability tool provides a helpful framework to all organizations for building, implementing, and demonstrating accountable data practices and outcomes.[16] The Accountability Framework helps conceptualize a comprehensive and risk-based privacy management program that consists of seven components: leadership and oversight, risk assessments, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement.[17] Two important hallmarks of this approach are the necessity of leadership buy-in as well as the need for review and oversight throughout the lifecycle of data use.[18]

- **Privacy Impact Assessments:** Privacy Impact Assessments (PIAs) can help organizations consider societal and company values while analyzing the risks and benefits of data uses. This internal accountability tool can help ensure consistent assessment of risks across organizational silos. It can also help to analyze reticence risks—or the risks of not acting on a particular use of data—in certain situations.[19] PIAs can be a trigger for a larger review or consideration of data use, in the form of a data review board (DRB).

- **Data Review Boards:** Data Review Boards (DRBs), or data ethics boards, are another tool to provide additional oversight and help foster responsible innovation around new and innovative uses of data. DRBs call on a diverse panel of reviewers to consider the risks and benefits of a particular data use and suggest mitigation strategies to help ensure the proper protection and security of data.[20] DRBs can create a variety of use cases to guide future decisions, and can help demonstrate accountability and thoughtfulness to regulators.

- **Privacy certifications and codes of conduct:** Certifications and codes of conduct implementing applicable privacy requirements could assist businesses of all sizes in establishing effective and compliant data practices, including on the issues of data use and sharing for social good. Certifications such as ISO27701:2019, which outlines establishing and maintaining a Privacy Information Management System, may be helpful to build a culture that fosters privacy and security.[21] The NIST Privacy Framework can similarly provide guidance that helps an organization develop and implement privacy protective data policies.[22]

These tools are only a survey of many tools available to strengthen accountable data practices. CIPL's recent blog post "Covid-19 Meets Privacy: A Case Study for Accountability" provides an overview of 12 accountability steps organizations, government bodies, education and research institutions can implement to enable responsible data use and sharing and protect privacy in the context of COVID-19.[23] In the post-COVID-19 world, there will be louder calls for corporate leaders and their boards, as well as government bodies, to foster and demonstrate accountability—to individuals, the public, regulators, and markets. These tools are the future of ensuring responsible innovation with robust protections for individual privacy. They should also be specifically enabled in future US privacy law.

7. The most helpful approach to ensuring privacy in the US will be comprehensive privacy legislation at the national level.

The ease with which individuals and data cross borders heightens the importance of ensuring that the legal protections afforded to personal data operate at the highest level possible and interconnect as seamlessly as feasible. Despite this awareness, as mentioned above, the US continues to subject much of its personal data to a fragmentary sectoral approach at the federal level and through piecemeal state regulation, while the EU, although achieving supranational regulation on the surface, continues to permit national requirements, local interpretations, and limits on the flow of data outside of the EU. Patchwork approaches create obstacles for creating a single digital market, promoting data sharing, and generally fostering innovation. Indeed, the EU's highest court recently placed significant limitations on EU-US data flows, ruling that the US lacks adequate privacy protections for European citizens' personal data.[24] While the specific deficiencies at the heart of the decision might not have been different under a comprehensive US privacy law, the absence of such a law substantially contributed to the underlying challenge against data transfers from

the EU to the US. Thus, a single comprehensive approach to privacy not only has the potential to usher in economic growth and equal data protection for all US citizens, it would also improve the US's ability to attract necessary cross-border data flows from other countries.

The COVID-19 pandemic has brought home the importance of broad data protection laws that connect seamlessly because the coronavirus has amply demonstrated its disregard for political borders, and because the volume of data needed to develop and test vaccines and treatments necessarily requires sharing across jurisdictions.[25] The same has always been true for non-COVID-related data uses as well, and it will continue to be true after the pandemic.

While a US federal privacy law may not appear to be the immediate priority in the midst of a public health crisis, it should be considered a top priority to help foster economic growth as the nation looks to rebuild the post-COVID economy.

While a US federal privacy law may not appear to be the immediate priority in the midst of a public health crisis, it should be considered a top priority to help foster economic growth as the nation looks to rebuild the post-COVID economy. Given that COVID-19 has demonstrated the value of such a comprehensive law for protecting privacy while also facilitating innovative uses of data, and considering that the effective use of personal data is at the center of much of our economic activities, a comprehensive federal privacy law will be an important prerequisite for economic recovery post-COVID-19. As noted, a number of accountability tools and frameworks exist to help facilitate responsible data practices in the absence of a law. However, there is an important role for "Congress to sketch out the rights that consumers have and the obligations that the businesses should be subject to."[26] National privacy legislation can also foster consumer trust, potentially increasing the willingness of consumers to share information and adopt new technologies that could help address COVID-19 from both a public health and economic perspective.

Perhaps the most important takeaway is that privacy legislation should keep an eye toward the future. Any new privacy law should carefully consider the implications of future unknown circumstances and technologies and accommodate the implications of those circumstances by remaining principles-based, impact-focused, and technology-neutral. Regulating too rigidly results in blanket waivers, while regulating too broadly can fail to provide any substantive protections at all. Poorly targeted regulation can result in compromises to privacy when security or health are of highest concern, or it can limit technological breakthroughs due to a lack of proper guidance to facilitate its responsible development. Protections must be firm enough to protect individual interests and rights while flexible enough to balance modern data uses, technologies, and public interest concerns.

COVID-specific privacy debates respond to today's health crisis and can help organizations address the pandemic. But those debates also provide us with an opportunity to learn from current experience, better prepare for the data uses of the future, and foster socially responsible and accountable practices while also protecting the emerging issues of today highlight the overall preexisting need for a comprehensive US privacy framework. The lessons outlined above will serve as helpful guidance for any modern, functional approach to privacy.

[1] For an analysis of corporations experiencing growth amidst the COVID-19 outbreak, see "Prospering in the Pandemic: The Top 100 Companies," Financial Times (19 June 2020), available at: https://www.ft.com/content/844ed28c-8074-4856-bde0-20f3bf4cd8f0.

[2] "Secretary Azar Announces Historic Expansion of Telehealth Access to Combat COVID-19," HHS (17 March 2020), available at https://www.hhs.gov/about/news/2020/03/17/secretary-azar-announces-historic-expansion-of-telehealth-access-to-combat-covid-19.html.

[3] For more information on building accountability in AI, see "Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, Second Report: Hard Issues and Practical Solutions," CIPL (February 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf.

[4] "Covered Entities and Business Associates," US Dept. of Health & Human Services, available at https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[5] "DPA Guidance on COVID-19," IAPP (May 2020), available at https://iapp.org/resources/article/dpa-guidance-on-covid-19/. Notably, the rest of the world has not fared much better. The Global Privacy Assembly has compiled 40+ guidance documents from DPAs around the world as well as six international organizations. "GPA COVID-19 Response Repository," Global Privacy Alliance, available at: https://globalprivacyassembly.org/covid19/. These documents are designed to help companies navigate the crisis while accounting for data protection and other rights, but there is a risk of conflicting guidance.

[6] "Global Privacy Assembly Establishes COVID-19 Taskforce," Hunton Privacy Blog (1 June 2020), available at https://www.huntonprivacyblog.com/2020/06/01/global-privacy-assembly-establishes-covid-19-taskforce/#more-19070.

[7] "First Report: Artificial Intelligence and Data Protection in Tension," CIPL (10 October 2018), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf. See "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" European Parliamentary Research Service (July 2019), available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (C 58 final) (Oct. 1, 1980), available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[8] "Eight Privacy Priorities for 2020 and Beyond," CIPL (9 March 2020), available at https://www.informationpolicycentre.com/cipl-blog/eight-privacy-priorities-for-2020-and-beyond.

[9] "Are Our Privacy Laws Asking Too Much of Consumers and Too Little of Businesses?" CIPL (13 Dec. 2019), available at: https://www.informationpolicycentre.com/cipl-blog/are-our-privacy-laws-asking-too-much-of-consumers-and-too-little-of-businesses.

[10] Remarks of Commissioner Rebecca Kelly Slaughter, FTC Hearing #12, US Federal Trade Commission (10 April 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1513009/slaughter_remarks_at_ftc_approach_to_consumer_privacy_hearing_4-10-19.pdf. FTC Commissioner Christine Wilson also recently noted that an "over-reliance on notice and consent should be avoided given what we know about the effectiveness (or lack thereof) of privacy disclosures in the technology space." US FTC Commissioner Christine Wilson, "Privacy and Public/Private Partnerships in a Pandemic," Remarks at Privacy + Security Academy, available at: https://www.ftc.gov/system/files/documents/public_statements/1574938/wilson_-_remarks_at_privacy_security_academy_5-7-20.pdf.

[11] GDPR, Recital 42; see also Ben Wolford, "What Are the GDPR Consent Requirements," GDPR EU, available at https://gdpr.eu/gdpr-consent-requirements/.

[12] See Fred H. Cate & Beth E. Cate, "The Supreme Court and Information Privacy," in Fred H. Cate & James X. Dempsey, Bulk Collection: Systematic Government Access to Private-Sector Data 195, 207 (2017) ("Moreover, the Supreme Court interprets the Fourth Amendment to apply only to the collection of information, not its use. Even if information is obtained in violation of the Fourth Amendment, the Supreme Court has consistently found that the Fourth Amendment imposes no independent duty on the government to refrain from using it. 'The Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands, and an examination of its origin and purposes makes clear that the use of fruits of a past unlawful search or seizure "[works] no new Fourth Amendment wrong."'" (quoting United States v. Leon, 468 U.S. 897, 906 (1984)).

[13] Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 George Washington Law Review 1208, 1212 (2004). Some observers have noted that "ECPA 'was designed to regulate wiretapping and electronic snooping rather than commercial data gathering,' and litigants attempting to apply ECPA to online data collection have generally been unsuccessful." See "Data Protection Law: An Overview," Congressional Research Service (25 March 2019), available at https://fas.org/sgp/crs/misc/R45631.pdf.

[14] CIPL has advocated for storage and use limitations as one solution to this issue: "Data processing undertaken in the Covid-19 context to predict virus peak levels or to understand people's interaction and likelihood of contamination, must be conducted under clearly limited time frames. Once the purpose of processing is fulfilled, data should not be stored and used any more for another new objective that is unrelated to the original purpose." "Covid-19 Meets Privacy: A Case Study for Accountability," CIPL (4 April 2020), available at https://www.informationpolicycentre.com/cipl-blog/covid-19-meets-privacy-a-case-study-for-accountability.

[15] Fred H. Cate & Rachel D. Dockery, "Artificial Intelligence and Data Protection: Observations on a Growing Conflict," Seoul National University Journal of Law & Economic Regulation, Vol. 11. No. 2 (2018), at page 123.

[16] FTC Commissioner Christine Wilson recently referred to the CIPL Accountability Wheel as "an excellent visual framework for businesses to design privacy programs for emerging technologies assisting with combatting Covid-19.... I recommend that companies evaluate their privacy programs in light of these elements, considering carefully each of these areas." US FTC Commissioner Christine Wilson, "Privacy and Public/Private Partnerships in a Pandemic," Remarks at Privacy + Security Academy, available at: https://www.ftc.gov/system/files/documents/public_statements/1574938/wilson_-_remarks_at_privacy_security_academy_5-7-20.pdf.

[17] "The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society," CIPL (23 July 2018), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

[18] For more information on CIPL's efforts to define and promote effective organizational accountability, see "Organizational Accountability," CIPL, available at https://www.informationpolicycentre.com/organizational-accountability.html. As part of this project on Organizational Accountability, CIPL has recently published three important resources. See "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework," CIPL (May 2020); "Organizational Accountability in Light of FTC Consent Orders," CIPL (13 November 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf; "CIPL Accountability Q&A," CIPL (3 July 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf.

[19] See "Eight Privacy Priorities for 2020 and Beyond," CIPL (9 March 2020).

[20] Rachel Dockery, Fred Cate, & Stanley Crosley, "Why Data Review Boards Are a Promising Tool for Improving Institutional Decision-Making," IAPP (28 February 2020), available at https://iapp.org/news/a/why-data-review-boards-are-a-promising-tool-for-improving-institutional-decision-making/.

[21] "ISO/IEC 27701:2019: Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," ISO, https://www.iso.org/standard/71670.html.

[22] National Institute of Standards and Technology, NIST Privacy Framework, https://www.nist.gov/privacy-framework.

[23] "Covid-19 Meets Privacy: A Case Study for Accountability," CIPL (4 April 2020), available at https://www.informationpolicycentre.com/cipl-blog/covid-19-meets-privacy-a-case-study-for-accountability.

[24] C-311/18, Data Protection Comm'r v. Facebook Ireland Ltd., Maximillian Schrems, ECLI:EU:C:2020:559, Judgement of 16 July 2020, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12540818.

[25] CIPL recently advocated for global interoperability and collaboration in its response to the EU Commission's Consultation on a European Strategy for Data: "A European data space must be developed with an eye on global interoperability and collaboration if Europe wants to create a truly attractive policy environment for its data economy. Long-standing EU rules on international data transfers have ensured that European protections follow the data regardless of where it travels globally. The European strategy for data should be based on a similar model. Any type of data residency requirement or obligation to store data in Europe would raise several challenges and hinder the ability of European organisations to innovate. Equally, the EU should continue to be vocal in opposing data localisation trends in other countries." "Centre for Information Policy Leadership's Response to the EU Commission's Consultation on a European Strategy for Data," CIPL (29 May 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_the_eu_commissions_consultation_on_a_european_strategy_for_data__29_may_2020_.pdf.

[26] "The Role of The Federal Trade Commission in Privacy and Beyond: A Fireside Chat with Commissioners Rebecca Kelly Slaughter and Christine S. Wilson," The Brookings Institution (28 October 2019), available at: https://www.brookings.edu/wp-content/uploads/2019/10/gs_20191028_ftc_privacy_transcript.pdf.

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at **http://www.informationpolicycentre.com/.**

If you would like to discuss this report or require additional information, please contact Markus Heyder, mheyder@HuntonAK.com; Matt Starr, mstarr@HuntonAK.com or Sam Grogan, sgrogan@HuntonAK.com.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

DC
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels
Park Atrium
Rue des Colonies 11
1000 Brussels
+32 2 643 58 00

20274-082020