Digital Contact Tracing and Data Protection Law

September 24, 2020

Congressional Research Service
https://crsreports.congress.gov
R46542

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46542

September 24, 2020

Jonathan M. Gaffney
Legislative Attorney

Eric N. Holmes
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Digital Contact Tracing and Data Protection Law

Coronavirus Disease 2019 (COVID-19) has infected millions of Americans since the ongoing pandemic began, and the disease has caused many thousands of deaths across the country. Government officials attempting to slow the spread of COVID-19 have implemented a number of responses, including widespread stay-at-home orders, travel advisories, and an increase in testing. State and local public health authorities are also making use of public health investigation techniques to ascertain how the disease has spread. One such technique is contact tracing, a process by which public health investigators identify individuals who have come into contact with infected persons.

Officials and technology companies have suggested that contact tracing may be accomplished more quickly and easily with the assistance of digital tools. For example, digital technology might assist with tracking individual movements and encounters using information collected from mobile devices. However, public health authorities' use of digital tools capable of collecting individual information also raises concerns about how to preserve the privacy and security of that data.

This report will discuss how data privacy and security (together, data protection) law applies to a public health authority's use of digital contact tracing tools. The report begins with a discussion of contact tracing, the role of technology in assisting with contact tracing, and potential privacy concerns. The second section of the report details key federal privacy laws—the Health Insurance Portability and Accountability Act, the Communications Act, the Family Educational Rights and Privacy Act, the Children's Online Privacy Protection Act, the Privacy Act, the Electronic Communications Privacy Act, and the Federal Trade Commission Act—and discusses what rights and obligations these laws may create for users and providers of digital contact tracing tools. Next, the report reviews selected state and foreign data protection laws and their application to digital contact tracing. The report concludes by providing an overview of data protection bills introduced in the 116th Congress in response to the COVID-19 pandemic and discussing some considerations for Congress as it weighs such legislation.

Contents

Tables

Appendixes

Contacts

Coronavirus Disease 2019 (COVID-19) has infected millions of Americans since the ongoing pandemic began, and the disease has caused many thousands of deaths across the country. Government officials attempting to slow the spread of COVID-19 have implemented a number of responses, including widespread stay-at-home orders,[1] travel advisories,[2] and an increase in testing.[3] State and local public health authorities are also making use of public health investigation techniques to ascertain how the disease has spread. One such technique is *contact tracing*, a process by which public health investigators identify individuals who have come into contact with infected persons.

Officials and technology companies have suggested that contact tracing may be accomplished more quickly and easily with the assistance of digital tools. For example, digital technology might assist with tracking individual movements and encounters using information collected from mobile devices. However, public health authorities' use of digital tools capable of collecting individual information also raises concerns about how to preserve the privacy and security of that data.

This report discusses how data privacy and security laws (together, data protection laws[4]) apply to digital contact tracing tools used by a public health authority or its agents. In the first section, the report discusses contact tracing and how technology has evolved to assist in this activity.[5] It includes, in particular, a description of the main types of mobile contact tracing applications (apps) that have been developed thus far—namely, "location tracking" apps and "proximity tracking" apps.[6] It then lays out some privacy concerns raised by privacy advocates and describes the ways in which these app developers have responded to the concerns.[7]

In the second section, the report describes existing federal data protection laws and their application to digital contact tracing. Rather than a single overarching federal data protection law, the United States has a "patchwork" of various federal laws governing privacy and security practices.[8] These include, for example, the Health Insurance Portability and Accountability Act, which limits healthcare entities' use of health information; the Communications Act, which limits phone carriers' use of customer data; and the Federal Trade Commission Act, which prohibits companies from engaging in deceptive or unfair data protection practices.[9] This section focuses in particular on whether these laws apply to digital contact tracing activities at all, and, to the extent they do, the limitations they impose on the ability of public health authorities to collect and use digital contact tracing data.

---

[1] Jasmine C. Lee, Sarah Mervosh, Yuriria Avila, Barbara Harvey, & Alex Leeds Matthews, *See How All 50 States Are Reopening (And Closing Again)*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/us/states-reopen-map-coronavirus.html (last visited Aug. 17, 2020).

[2] *E.g.*, *COVID-19 Travel Advisory*, OHIO DEP'T OF HEALTH, https://coronavirus.ohio.gov/wps/portal/gov/covid-19/families-and-individuals/COVID-19-Travel-Advisory/ (last visited Aug. 17, 2020); *COVID-19 Travel Advisory*, N.Y. DEP'T OF HEALTH, https://coronavirus.health.ny.gov/covid-19-travel-advisory (last visited Aug. 17, 2020); *NJ Travel Advisory Form*, NJ.GOV, https://covid19.nj.gov/forms/njtravel (last visited Aug. 17, 2020).

[3] *See* COVID TRACKING PROJECT, https://covidtracking.com/ (last visited Aug. 17, 2020).

[4] For a further discussion of the concept of data protection, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[5] *See infra* "Background."

[6] *See infra* "Digital Tools."

[7] *See infra* "Concerns and Issues."

[8] *See infra* "Federal Data Protection Laws and Digital Contact Tracing."

[9] *Id.*

The third section of the report discusses some state and foreign data protection laws and their application to digital contact tracing, specifically, the California Consumer Privacy Act (CCPA), Canada's federal privacy laws, and the European Union's General Data Protection Regulation (GDPR).[10] These laws are noteworthy because they apply to many American companies and also provide a point of comparison with the patchwork of laws at the federal level. Finally, this report concludes with an overview of the data protection bills that have been introduced in the 116th Congress in response to the COVID-19 pandemic and discusses some considerations for Congress as it considers proposed legislation.[11]

Background

Introduction to Contact Tracing

The term *contact tracing* generally refers to procedures used to identify and monitor people who have been in contact with someone diagnosed with an infectious disease, and thus facilitate implementing targeted control measures (such as quarantines) to prevent the broader spread of the illness. Contact tracing is standard procedure in public health investigations, and historically involves officials interviewing and contacting infected and potentially-exposed persons. State and local health departments ("health departments" or "public health authorities") traditionally conduct contact tracing, rather than federal authorities.[12] However, the Centers for Disease Control and Prevention (CDC) has published guidance for health departments conducting contact tracing.[13] For more detail on contact tracing in response to COVID-19, see CRS In Focus IF11609, *Contact Tracing for COVID-19: Domestic Policy Issues*, by Kavya Sekar and Laurie A. Harris.

Digital Tools

Manual contact tracing—which entails several iterations of interviews, exposure notification to potentially affected individuals, and contact follow-up—may be too slow to keep pace with COVID-19's spread.[14] Consequently, technologists have been working to develop digital contact-tracing tools to supplement traditional contact tracing activities.[15]

Digital contact tracing or *digital exposure notification* refers to the use of technology to identify and notify individuals who may have come into contact with a person who has tested positive for COVID-19—functions which, in traditional contact tracing, would be performed by a public

[10] *See infra* "Selected State, Foreign, and International Data Protection Laws."

[11] *See infra* "Legislation" and "Considerations for Congress."

[12] *See* CRS Report R43809, *Preventing the Introduction and Spread of Ebola in the United States: Frequently Asked Questions*, coordinated by Sarah A. Lister (detailing state and local roles in monitoring disease outbreaks in the context of the Ebola virus).

[13] *Contact Tracing for COVID-19*, CTRS. FOR DISEASE CONTROL & PREVENTION (Sept. 10, 2020), https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/contact-tracing.html.

[14] ASS'N OF STATE & TERRITORIAL HEALTH OFFS., ISSUE GUIDE: COVID-19 CASE INVESTIGATION AND CONTACT TRACING: CONSIDERATIONS FOR USING DIGITAL TECHNOLOGIES 4 (2020) [hereinafter ASTHO], https://www.astho.org/ASTHOReports/COVID-19-Case-Investigation-and-Contact-Tracing-Considerations-for-Using-Digital-Technologies/07-16-20/; *see also* Jennifer Steinhauer & Abby Goodnough, *Contact Tracing Is Failing in Many States. Here's Why*, N.Y. TIMES (July 31, 2020), https://www.nytimes.com/2020/07/31/health/covid-contact-tracing-tests.html.

[15] CRS In Focus IF11609, *Contact Tracing for COVID-19: Domestic Policy Issues*, by Kavya Sekar and Laurie A. Harris.

health investigator during and after interviews with infected or presumptively infected individuals.[16] Public health authorities have turned to both private and public entities to support development of these technologies. Certain emergent digital contact tracing and exposure notification technologies can support these functions by gathering data from mobile devices running mobile applications (apps).

- Digital contact tracing or "location tracking" apps trace a mobile device's movement using location information, such as global positioning system (GPS) or cell site location information.[17]
- Digital exposure notification or "proximity tracking" apps receive and transmit device identifiers using Bluetooth technology when two devices with the app remain in close proximity to each other for a specific amount of time.[18]

Both of these app types use the data they collect to determine whether app users have come into contact with other app users, though proximity tracking apps do so without using any location information.[19] Examples of location tracking apps include Rhode Island's CRUSH COVID RI app and apps based on MIT's Safe Paths app.[20] Proximity tracking apps include those built on Google and Apple's exposure notification system, such as Virginia's COVIDWISE app.[21] **Appendix A** includes a current list of state apps. For more information on the technical development and implementation of digital contact-tracing tools, see CRS In Focus IF11559, *Digital Contact Tracing Technology: Overview and Considerations for Implementation*, by Patricia Moloney Figliola.

Concerns and Issues

Digital contact-tracing tools have the potential to collect information capable of identifying individuals. Indeed, for proximity or location tracking apps to function, the apps must be able to associate an individual's positive COVID-19 diagnosis with that individual's unique identifiers or location history. Privacy advocates have therefore expressed concern about the privacy and security of any information collected by digital contact-tracing tools.[22] The implementation of these tools raises two types of privacy risks: unwanted access to information by government

[16] ASTHO, *supra* note 14, at 6; *see* JOSEPH ALI ET AL., DIGITAL CONTACT TRACING FOR PANDEMIC RESPONSE 3-4 (Jeffrey P. Kahn ed., 2020), https://muse.jhu.edu/book/75831/pdf.

[17] *See* Patrick Howell O'Neill et al., *COVID Tracing Tracker*, MIT TECH. REV. (May 7, 2020), https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

[18] *Id.*

[19] *Id.* For readability, this report will refer to both app types as "digital contact tracing" throughout.

[20] *CRUSH COVID RI*, R.I. DEP'T OF HEALTH, https://health.ri.gov/covid/crush/ (last visited Sept. 22, 2020); *Private Kit: Safe Paths; Privacy-By-Design*, MIT.EDU, https://safepaths.mit.edu (last visited Sept. 22, 2020); *see also The PathCheck GPS+ Solution*, PATHCHECK FOUND., https://pathcheck.org/en/technology/gps-digital-contact-tracing-solution (last visited Sept. 22, 2020).

[21] *Privacy-Preserving Contact Tracing*, APPLE, https://www.apple.com/covid19/contacttracing (last visited Sept. 22, 2020); *see* Sarah McCammon, *Virginia Unveils App to Aid Contact Tracing*, NPR (Aug 5, 2020), https://www.npr.org/sections/coronavirus-live-updates/2020/08/05/899414953/virginia-unveils-app-to-aid-contact-tracing.

[22] *See, e.g.*, DANIEL KAHN GILLMOR, ACLU, PRINCIPLES FOR TECHNOLOGY-ASSISTED CONTACT TRACING (2020), https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_contact_tracing_principles.pdf (asserting that digital contact tracing tools may cause "significant risks to privacy, civil rights, and civil liberties"); Mark Zastrow, *South Korea Is Reporting Intimate Details of COVID-19 Cases: Has It Helped?* NATURE (Mar. 18, 2020), https://www.nature.com/articles/d41586-020-00740-y (noting that South Korea's extensive data collection "has raised privacy concerns" by allowing infected people to be identified).

actors, such as law enforcement,[23] and unwanted access to information by private actors, such as third-party advertisers.[24] Even if public health authorities do not voluntarily share identifiable information with third parties, digital contact-tracing tools may be susceptible to security breaches or misuse, with the risks of these harms increasing as apps collect more information.[25]

Technologists have responded to these risks by attempting to build privacy protections into digital contact-tracing tools.[26] Many of these built-in protections implement recommendations made by privacy advocates, such as storing data locally and using identifiers that change at regular intervals.[27] Privacy advocates have responded more positively to proximity tracking apps, which are generally seen as less intrusive than location tracking apps because they record only that two devices have been in proximity to each other at some point, rather than the geographical location of a specific device at a particular time.[28]

Federal Data Protection Laws and Digital Contact Tracing

In contrast to the European Union—which, as discussed later, has a comprehensive privacy law—the United States has a patchwork of federal laws that govern data protection practices.[29] Many of these laws are discussed in detail in CRS Report R45631, *Data Protection Law: An Overview*. Consequently, rather than providing a complete overview of federal data protection law, this section surveys those federal laws most relevant to digital contact tracing. This section begins with a discussion of the Health Insurance Portability and Accountability Act's (HIPAA) data protection requirements, which are the main federal rules governing the privacy and security of

[23] *E.g.*, Matthew Guariglia, *The Dangers of COVID-19 Surveillance Proposals to the Future of Protest*, ELEC. FRONTIER FOUND. (Apr. 29, 2020), https://www.eff.org/deeplinks/2020/04/some-covid-19-surveillance-proposals-could-harm-free-speech-after-covid-19 (warning of the danger of "surveillance creep"); Mike Giglio, *Would You Sacrifice Your Privacy to Get out of Quarantine?* ATLANTIC (Apr. 22, 2020), https://www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172/ (same). This risk is largely outside the scope of this report, and some risk of unwanted law enforcement access may be mitigated by the protections of the Fourth Amendment. For more information on the potential application of Fourth Amendment protections to digital contact tracing, see CRS Legal Sidebar LSB10449, *COVID-19, Digital Surveillance, and Privacy: Fourth Amendment Considerations*, by Michael A. Foster.

[24] *E.g.*, Stephen Groves, *Tech Privacy Firm Warns Contact Tracing App Violates Policy*, ASSOCIATED PRESS (May 22, 2020), https://apnews.com/03f2756664184cf1789c9b970beb7111 (reporting that an app used by North Dakota and South Dakota shared user information with third parties).

[25] *E.g.*, Natasha Singer, *Virus-Tracing Apps Are Rife with Problems. Governments Are Rushing to Fix Them*, N.Y. TIMES (July 8, 2020), https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html (detailing security flaws in contact tracing apps); *Joint Statement on Contact Tracing for Norway*, MEDIUM (May 19, 2020), https://medium.com/@jointstatementnorway/joint-statement-on-contact-tracing-for-norway-331ee49fc6f6 (averring that the amount of information collected by Norway's contact tracing app could allow "bad actor[s]" to spy on Norwegian citizens).

[26] *See Privacy-Preserving Contact Tracing*, APPLE, https://www.apple.com/covid19/contacttracing (last visited Sept. 22, 2020) (detailing the properties of the Apple-Google framework that protect individuals' privacy).

[27] *Compare id. with* KAHN GILLMOR, *supra* note 22, at 6 (setting forth recommendations for contact tracing tools).

[28] *E.g.*, Geoffrey A. Fowler, *I Downloaded America's First Coronavirus Exposure App. You Should Too*, WASH. POST (Aug 18, 2020), https://www.washingtonpost.com/technology/2020/08/17/coronavirus-exposure-notification-app/; *ACLU Comment on Apple/Google COVID-19 Contact Tracing Effort*, ACLU (Apr. 10, 2020), https://www.aclu.org/press-releases/aclu-comment-applegoogle-covid-19-contact-tracing-effort.

[29] For further discussion of the concept of data protection, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

health information stored or collected by healthcare entities.[30] It then surveys other federal laws that may apply to contact tracing, starting with those more targeted in scope and concluding with more broadly applicable laws.

The Health Insurance Portability and Accountability Act (HIPAA)

Pursuant to its authority under the Health Insurance Portability and Accountability Act (HIPAA),[31] the Department of Health and Human Services (HHS) has enacted data protection regulations known as the Privacy, Security, and Breach Notification Rules, which this report will collectively call the HIPAA Data Protection Rules.[32] The HIPAA Data Protection Rules are the primary federal data protection provisions regulating personal health information.[33] This section first provides an overview of the HIPAA Data Protection Rules' requirements and then analyzes how these requirements apply to digital contact tracing.

Overview of the HIPAA Data Protection Rules

Covered Entities and Business Associates

The HIPAA Data Protection Rules regulate the use, disclosure, and security of protected health information (PHI) by *covered entities* and their *business associates*.[34] Covered entities include *health plans*, *health care clearinghouses*, and *health care providers* who transmit electronic health information in connection with a HIPAA-covered transaction (such as billing).[35] A health plan is an "individual or group plan that provides, or pays the cost of, medical care."[36] This includes health insurance companies, health maintenance organizations, and government programs—such as Medicaid and Medicare—that pay for health care.[37] Health care clearinghouses are entities that process health information from a nonstandard format into a standard format, or vice versa.[38] Lastly, health care providers include providers of services covered by Sections 1861(u) or 1861(s) of the Social Security Act (which includes, among other things, physicians' services, hospital services, physical therapy services, and skilled nursing facility services) or any person who otherwise "furnishes, bills, or is paid for health care in the normal course of business."[39] Health care is "care, services, or supplies related to the health of an

[30] 42 U.S.C. § 1320d-2; 45 C.F.R. pt. 164.

[31] 42 U.S.C. § 1320d-2.

[32] 45 C.F.R. pt. 164; *see also* CTRS. FOR MEDICARE & MEDICAID SERVS., HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES (Sept. 2018), https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecuritytextonly.pdf.

[33] In re Mitchell, No. 18-40736, 2019 WL 1054715, at *5 (Bankr. D. Idaho Mar. 5, 2019) ("HIPAA is the primary federal law passed to ensure an individual's right to privacy over his or her medical records . . . .").

[34] 45 C.F.R. § 164.104.

[35] *Id.* § 160.103. HIPAA-covered transactions include transactions related to payments and remittance advice, claims status, eligibility, coordination of benefits, claims and encounter information, enrollment and disenrollment, referrals and authorizations, and premium payment. *Transactions Overview*, CTRS. FOR MEDICARE & MEDICAID SERVS., https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview (last visited Sept. 22, 2020).

[36] 45 C.F.R. § 160.103.

[37] *Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Sept. 22, 2020).

[38] 45 C.F.R. § 160.103.

[39] *Id.*; 42 U.S.C. § 1395x(u), (s).

individual."[40] A business associate is one who, among other actions, "creates, receives, maintains, or transmits protected health information" on behalf of a covered entity for an activity regulated under HIPAA generally (not simply the Data Protection Rules), such as claims processing, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing.[41]

The HIPAA Data Protection Rules recognize that entities may engage in conduct that makes them covered entities (covered functions), while, at the same time, performing other functions that do not render them covered entities. For instance, institutions of higher learning may, in addition to providing education, run a health clinic that provides healthcare for students.[42] Such an entity may become a "hybrid entity" by complying with organizational requirements that include designating a specific component of its organization as the "health care component."[43] In such situations, only the designated health care component of a hybrid entity is required to comply with the HIPAA Data Protection Rules.[44]

Substantive Requirements

The HIPAA Data Protection Rules' substantive requirements govern covered entities' treatment of PHI. PHI includes information that (1) "identifies," or can reasonably "be used to identify," an individual; (2) is "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (3) relates to an individual's past, present, or future physical or mental health, health care provision, or payment for the provision of health care; and (4) is transmitted by or maintained in electronic or any other form or medium.[45]

The HIPAA Data Protection Rules address, among other things, covered entities': (1) use or sharing of PHI, (2) safeguards for securing PHI, and (3) notification of consumers following a breach of PHI records. On the first issue, HIPAA's Data Protection Rules prohibit covered entities from using PHI or sharing it with third parties without valid patient authorization, unless the use is for purposes of treatment, payment, or "health care operations," or falls within a specific statutory exception.[46] One such exception, which is particularly relevant to contact tracing allows covered entities to use or disclose PHI—without individual patient authorization or the opportunity for the patient to agree or object—to "a public health authority" that is legally authorized to collect the information "for the purpose of preventing or controlling disease, injury, or disability," including "the conduct of public health surveillance."[47] A "public health authority"

[40] 45 C.F.R. § 160.103.

[41] *Id.*

[42] *Can A Postsecondary Institution Be A "hybrid entity" under the HIPAA Privacy Rule?* U.S. DEP'T OF HEALTH & HUMAN SERVS. (Nov. 25, 2008), https://www.hhs.gov/hipaa/for-professionals/faq/522/can-a-postsecondary-institution-be-a-hybrid-entity-under-hipaa/index.html.

[43] *Id.*; 45 C.F.R. §§ 164.103, 164.105.

[44] 45 C.F.R. § 164.105(a)(1).

[45] *Id.* § 160.103.

[46] *Id.* §§ 164.506–512. "Health care operations" are defined as including a number of activities, such as: (1) "[c]onducting quality assessment and improvement activities"; (2) evaluating healthcare professionals and health plan performance; (3) underwriting and "other activities related to the creation, renewal, or replacement" of health insurance or health benefits contracts; (4) "conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs"; (5) business planning and development, such as "conducting cost-management and planning-related analyses related to managing and operating the entity"; and (6) "business management and general administrative activities of the entity." *Id.* § 164.501.

[47] *Id.* § 164.512(b).

includes any agency or authority of the "United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe," that is "responsible for public health matters as part of its official mandate," as well as "a person or entity acting under a grant of authority from or contract with" such an agency.[48] This definition encompasses the CDC as well as state and local public health departments, among others.[49] With respect to data security, covered entities must maintain various administrative, physical, and technical safeguards to protect against threats or hazards to the security of PHI.[50] Lastly, under the data breach notification requirements, covered entities must, among other things, notify affected individuals within 60 calendar days after discovering a breach of "unsecured" PHI.[51]

Enforcement

Violations of the HIPAA Data Protection Rules can lead to civil or criminal enforcement. The HHS Office of Civil Rights is responsible for investigating and enforcing civil violations of HIPAA's requirements and may impose monetary penalties, which vary depending on the violator's culpability.[52] The U.S. Department of Justice has criminal enforcement authority under HIPAA and may seek fines or imprisonment against a person who "knowingly" obtains or discloses "individually identifiable health information" (as defined below) or "uses or causes to be used a unique health identifier" in violation of HIPAA's requirements.[53]

The HIPAA Data Protection Rules and Digital Contact Tracing

As noted, the HIPAA Data Protection Rules do not apply to all health-related data. Only PHI held by covered entities and their business associates is subject to the Rules' requirements. Thus, the extent to which the Rules apply to digital-contact tracing applications depends on whether the parties developing the apps and processing app information fall within the definitions of covered entities or business associates and whether the app uses PHI.

---

[48] *Id.* § 164.501.

[49] *Disclosures for Public Health Activities*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html (last visited Sept. 22, 2020).

[50] 45 C.F.R. §§ 164.302–318.

[51] *Id.* §§ 164.400–414. Unsecured PHI is defined as PHI that is "not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary . . . ." *Id.* § 164.402. HIPAA regulations define a "breach" as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under [HIPAA's privacy regulations] which compromises the security or privacy of the protected health information." *Id.* This definition contains several exclusions, including where the covered entity has a "good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information." *Id.*

[52] 42 U.S.C. § 1320d-5; 45 C.F.R. § 160.404. The amounts range from $100 per violation (with a total maximum of $25,000 per year for identical violations) up to $50,000 per violation (with a total maximum of $1,500,000 per year for identical violations). 45 C.F.R. § 160.404(b). The low-end of the penalty spectrum applies when the offender "did not know and, by exercising reasonable diligence, would not have known" of the violation, and the high-end of the penalty spectrum applies when "it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or by exercising reasonable diligence, would have known that the violation occurred." *Id.*

[53] 42 U.S.C. § 1320d-6. *See also Enforcement Process*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html ("OCR also works in conjunction with the Department of Justice (DOJ) to refer possible violations of HIPAA.").

Are public health authorities or app developers Covered Entities or Business Associates?

Because state and local public health authorities are the primary users of data collected through contact tracing, a critical threshold issue is whether they are *covered entities* subject to the HIPAA Data Protection Rules. This issue is complicated by the fact that a public health authority may perform various functions within one agency. For example, a public health authority may provide clinical care (e.g., diagnostic testing), and thus qualify as a health care provider subject to HIPAA's requirements. The same agency might also engage in community-wide or state-wide disease control activities, such as contact tracing, that do not appear to be among the functions by which HIPAA defines covered entities.

A health department that engages in both health care activities and disease control functions may choose to operate as a hybrid entity. In so doing, state and local health departments may limit their obligations under the HIPAA Data Protection Rules solely to their performance of discrete covered healthcare functions. Any information the hybrid entity obtains for use in disease control activities such as contact tracing would not be subject to the Rules' protections.[54] Moreover, under the public health authority exception, PHI received by the public health authority from a covered entity, such as a healthcare provider, would not be subject to the HIPAA Data Protection Rules.[55]

Third-party software developers are not generally covered entities subject to the HIPAA Data Protection Rules. Moreover, a third-party software developer that creates, maintains, or administers an app used in a public health authority's contact tracing operations would not qualify as a business associate subject to the HIPAA Data Protection Rules if the public health authority is not a covered entity when performing its disease control functions. This is because, as explained above, HIPAA defines a business associate as one who "creates, receives, maintains, or transmits protected health information" on behalf of a covered entity.[56]

Do contact-tracing apps use PHI?

Even if an entity is a covered entity or a business associate under HIPAA, the HIPAA Data Protection Rules only apply to PHI. To be sure, contact-tracing apps rely on health-related information (e.g., information that shows whether individuals have been diagnosed with, or exposed to, COVID-19). Thus, whether HIPAA Data Protection Rules apply to entities involved in developing and operating a contact-tracing app would largely depend on whether the information used for digital contact tracing is *individually identifiable*.

HIPAA deems health information not identifiable if the covered entity takes either of two steps.[57] One option is that the covered entity can de-identify the information by ensuring that eighteen specific types of identifiers have been removed (including, for example, "[a]ll geographic subdivisions smaller than a State," "[t]elephone numbers," and "[d]evice identifiers").[58] Alternatively, the covered entity may obtain documentation showing that an expert has

[54] 45 C.F.R. § 164.105(a)(1).

[55] *Id.* § 164.512(b).

[56] *Id.* § 160.103.

[57] *Id.* § 164.514(b).

[58] *Id.* § 164.514(b)(2).

determined that there is a "very small" risk of identification from the information.[59] If the covered entity chooses this approach, the HHS Office of Civil Rights may assess the expert's qualifications in the course of an audit or investigation.[60]

Many find it difficult to conceive how covered entities could make contact-tracing app information unidentifiable. Contact-tracing apps necessarily depend on information that accurately tracks individual movements and contacts. Both location tracking and proximity tracking apps function by associating a person who has tested positive for a disease with a device identifier generated by the app. In the case of location tracking apps, this includes GPS or cell site location information, which provides geographic information much smaller than a state. Apps could also request additional identifying information: Singapore's app, for example, requires app users to provide phone numbers.[61] Accordingly, the most likely option by which a covered entity could establish that the health information used for digital contact tracing is not identifiable may be to obtain an expert determination that the risk of identification from the information is "very small."[62]

Any such determination would likely assess the steps taken by the app to make identification difficult. Google and Apple's exposure notification system provides for apps that use randomly generated identifiers, which cycle every 10–20 minutes to reduce the risk of linking any group of identifiers to an individual.[63] Location tracking apps may take similar measures to mitigate tracking risk. For example, North Dakota's location tracking app associates location information with a random ID number and only stores location information when a device remains at a location for more than ten minutes.[64] However, even apps that associate information with randomly generated identifiers may be susceptible to "linkage attacks" in which an entity might be able to identify a particular device, and apps that collect more detailed information may potentially pose a greater risk.[65]

Other Federal Data Protection Laws

While the HIPAA Data Protection Rules are the federal privacy standards most directly targeted at health data, they are only one component of the "patchwork" of federal laws governing entities' data protection obligations. This section surveys other relevant federal laws and discusses how they might apply to digital contact tracing. It begins with the more targeted laws—namely, the Communications Act, the Family Educational Rights and Privacy Act, the Children's Online

[59] *Id.* § 164.514(b)(1).

[60] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Nov. 6, 2015), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#expert.

[61] *What Data Is Collected? Are You Able to See My Personal Data?* TRACETOGETHER, https://support.tracetogether.gov.sg/hc/en-sg/articles/360043735693-What-data-is-collected-Are-you-able-to-see-my-personal-data- (last visited Sept. 22, 2020).

[62] 45 C.F.R. § 164.514(b)(1).

[63] APPLE INC. & GOOGLE LLC, EXPOSURE NOTIFICATION: BLUETOOTH SPECIFICATION (Apr. 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf.

[64] *Care19*, NDRESPONSE.GOV, https://ndresponse.gov/covid-19-resources/care19 (last visited Sept. 22, 2019).

[65] Simson L. Garfinkel, *De-Identification of Personal Information*, NAT'L INST. OF STANDARDS & TECH. 17 (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf#page=25; Natasha Singer, *Virus-Tracing Apps Are Rife With Problems. Governments are Rushing to Fix Them*, N.Y. TIMES (July 8, 2020), https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html.

Privacy Protection Act, and the Privacy Act. It then turns to the Electronic Communications Privacy Act and the Federal Trade Commission Act, which are both broad in scope.

The Communications Act

The Communications Act restricts what "telecommunications carriers"—namely, landline and mobile telephone operators[66]—may do with "customer proprietary network information" (CPNI).[67] CPNI includes information relating to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[68] Carriers may not "disclose" customers' CPNI to third parties or give third parties "access to" CPNI without customer approval or unless an exception in the Act applies.[69] Exceptions include, among other things, disclosures to "providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency."[70] Carriers must also implement various data security safeguards, such as "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI," and must notify law enforcement and affected customers after a "breach" of CPNI.[71]

Most relevant for contact tracing, the Act's CPNI protections may prohibit cell phone carriers from disclosing users' geolocation data to contact-tracing apps. While courts have not considered whether the CPNI definition includes cellphone geolocation data, the Federal Communications Commission (FCC) has recently taken the position in an enforcement action that it is covered.[72] Even if geolocation data is CPNI, disclosing such data for contact tracing may qualify for the exception based on contact-tracing being an "emergency service" and contact tracing apps

[66] 47 U.S.C. § 153(51), (52); *see also* United States v. Radio Corp. of Am., 358 U.S. 334, 349 (1959) ("In contradistinction to communication by telephone and telegraph, which the Communications Act recognizes as a common carrier activity . . . the Act recognizes that broadcasters are not common carriers and are not to be dealt with as such.")

[67] 47 U.S.C. § 222.

[68] *Id.* § 222(h)(1). The Act further states that CPNI includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier," but does not include "subscriber list information." *Id.*

[69] *Id.* § 222(c)–(d); 47 C.F.R. § 64.2007. The regulations provide that, generally, customer approval must be "opt-in" approval. 47 C.F.R. § 64.2007(b). "Opt-in approval" requires that "the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access[.]" *Id.* § 64.2003(k). However, carriers only need to obtain "opt-out approval" to use or disclose individually identifiable CPNI to its agents and affiliates for marketing communications-related service. *Id.* § 64.2007(b). Under "opt-out approval," a customer is deemed to have consented if he has "failed to object" within a specified waiting period after being provided the "appropriate notification of the carrier's request for consent." *Id.* § 64.2003(l). Exceptions include, among other things, using or disclosing individually identifiable CPNI to disclose "aggregate customer information," provide or market service offerings for services to which the customer already subscribes, or provide "inside wiring installation, maintenance, and repair services." 47 U.S.C. § 222(c)–(d); 47 C.F.R. § 64.2005.

[70] 47 U.S.C. § 222(d); 47 C.F.R. § 64.2004(a).

[71] 47 C.F.R. § 64.5110; *id.* §§ 64.2009–.2011.

[72] On February 28, 2020, the FCC issued notices of apparent liability (NAL) to AT&T, Verizon, Sprint, and T-Mobile, alleging that they violated the Communications Act's CPNI requirements by disclosing wireless customers' location information to third parties without the customers' consent. *See* FED. COMMC'NS COMM., FCC PROPOSES OVER $200 MILLION IN FINES AGAINST FOUR LARGEST WIRELESS CARRIERS FOR APPARENTLY FAILING TO ADEQUATELY PROTECT CONSUMER LOCATION DATA (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf.

serving as "providers of information or database management services []."[73] However, the scope of this exception is unclear; neither the FCC nor courts appear to have defined the key terms—*information or database management services* and *emergency services*—or to have otherwise opined on the nature of this exception.

Uncertainty over how courts would treat carriers who disclose CPNI for contact tracing purposes creates risks for carriers. Under the Communications Act, the FCC may impose a *forfeiture penalty* against those who "willfully or repeatedly" violate the Act's requirements.[74] Along with the FCC's civil authority, the Communications Act further imposes criminal penalties on those who "willfully and knowingly" violate the Act or the FCC's implementing regulations.[75] Lastly, the Communications Act also provides a private right of action for those aggrieved by violations of the Act's common carrier requirements, which include the CPNI provisions.[76] In such actions, plaintiffs may seek actual damages and reasonable attorneys' fees.[77]

Family Educational Rights and Privacy Act (FERPA)

As the new school year commences this fall, schools and universities may seek to work with private sector developers or public health authorities engaging in contact tracing.[78] In doing so, any "educational agency or institution" receiving federal funds (covered entities) must comply with the Family Educational Rights and Privacy Act of 1974 (FERPA).[79] FERPA creates privacy protections for student education records, which are defined broadly to include any "materials which . . . contain information directly related to a student" and are "maintained by an educational agency or institution."[80] Among other things, FERPA prohibits covered entities from having a "policy or practice" of permitting the release of education records or "personally identifiable information contained therein" without the parent's consent (or student's consent if the student is over 18 or attends a postsecondary institution).[81] This consent requirement is

[73] 47 U.S.C. § 222(d)(4)(C).

[74] *Id.* § 503(b)(1). For common carriers, forfeiture penalties may be up to $160,000 for each violation or each day of a continuing violation but may not exceed $1,575,000 for any "single act or failure to act." *Id.* § 503(b)(2)(B); 47 C.F.R. § 1.80(b)(2).

[75] Any person who "willfully and knowingly" violates the Act's requirements may be fined up to $10,000 and imprisoned up to one year, and anyone who "willfully and knowingly" violates any FCC "rule, regulation, restriction or condition" made under the authority of the Act shall be fined up to $500 for "each and every day during which such offense occurs." 47 U.S.C. §§ 501–502.

[76] *Id.* § 206.

[77] *Id.*

[78] *See, e.g.*, Mohana Ravindranath & Amanda Eisenberg, *Contact Tracing Apps Have Been A Bust. States Bet College Kids Can Change That*, POLITICO (Aug. 19, 2020), https://www.politico.com/news/2020/08/19/contact-tracing-apps-have-been-a-bust-states-bet-college-kids-can-change-that-398701.

[79] 20 U.S.C. § 1232g(a)(3).

[80] *Id.* § 1232g(a)(4)(A). However, FERPA excludes certain things from the "education records" definition, specifically: (1) records made by "instructional, supervisory, and administrative personnel" that are kept "in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute"; (2) "records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement"; and (3) records made or maintained by a "physician, psychiatrist, psychologist, or other recognized professional or paraprofessional" on a student who is "eighteen years of age or older, or is attending an institution of postsecondary education," that are only used "in connection with the provision of treatment" and are "not available to anyone other than persons providing such treatment," except for a "physician or other appropriate professional of the student's choice." *Id.* § 1232g(a)(4)(B).

[81] *Id.* § 1232g(b). The right to consent transfers from the parent to the student once the student turns 18 years old or attends a postsecondary institution. *Id.* § 1232g(d).

subject to certain exceptions.[82] Most relevant, under the "health or safety emergency" exception, if a covered entity determines that "there is an articulable and significant threat to the health or safety of a student or other individuals," then it may disclose "information from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals."[83]

In March 2020, the Department of Education (ED) released its responses to "Frequently Asked Questions" (FAQs) on FERPA's application to the COVID-19 pandemic, which suggests that covered entities may, in some situations, disclose students' COVID-19 diagnoses to public health authorities under the health and safety exception.[84] In that guidance document, ED stated that "immunization and other health records" that are "directly related to a student and maintained" by a covered entity are "education records" under FERPA.[85] However, it further explained that the COVID-19 pandemic could, depending on local conditions, be a sufficient "threat" under the health and safety exception.[86] According to ED, if "local public health authorities determine that a public health emergency, such as COVID-19, is a significant threat to students or other individuals in the community, an educational agency or institution in that community may determine that an emergency exists as well."[87] It further noted that, when such "threats" exist, "[p]ublic health department officials may be considered 'appropriate parties'" under the health and safety exception, even "in the absence of a formally declared health emergency."[88] The guidance emphasized, however, that the health and safety exception is a "flexible standard under which [ED] will not substitute its judgement" for that of the covered entity.[89]

Although the health and safety exception gives covered entities considerable discretion, parents or adult students who believe that their rights under FERPA have been violated through a covered entity's disclosure of student medical records may file a complaint with ED.[90] FERPA authorizes the Secretary of Education to "take appropriate actions," which may include withholding federal education funds, issuing a "cease and desist order," or terminating eligibility to receive any federal education funding.[91] FERPA does not, however, contain any criminal provisions or a private right of action.[92]

---

[82] Exceptions include, among other things, allowing covered entities to disclose educational records to (i) certain "authorized representatives," (ii) school officials with a "legitimate educational interest," or (iii) "organizations conducting studies" for covered entities "for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instructions." *Id.* § 1232g(b); 34 C.F.R. § 99.31.

[83] 34 C.F.R. § 99.36(c). Covered entities that disclose "personally identifiable information from education records" under this exception must record in the student's education record the "articulable and significant threat" that formed the basis of the disclosure and the parties who requested or received the information. *Id.* § 99.32(a)(5).

[84] U.S DEP'T OF EDUC., FERPA & CORONAVIRUS DISEASE 2019 (COVID-19): FREQUENTLY ASKED QUESTIONS (FAQS), (Mar. 2020), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions_0.pdf.

[85] *Id.* at 2.

[86] *Id.* at 3.

[87] *Id.*

[88] *Id.* at 4.

[89] *Id.*

[90] 34 C.F.R. § 99.63.

[91] 20 U.S.C. § 1232g(f); 34 C.F.R. § 99.67.

[92] *See* Gonzaga Univ. v. Doe, 536 U.S. 273, 290 (2002) ("In sum, if Congress wishes to create new rights enforceable under § 1983, it must do so in clear and unambiguous terms—no less and no more than what is required for Congress to create new rights enforceable under an implied private right of action. FERPA's nondisclosure provisions contain no rights-creating language, they have an aggregate, not individual, focus, and they serve primarily to direct the Secretary

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) and its implementing regulations[93] protect the privacy of children under the age of 13 by imposing certain obligations on *operators* of online services (including apps)[94] collecting children's information. Specifically, to be subject to COPPA's requirements, an entity must: (1) collect or maintain personal information from users of the service (or have the information collected or maintained on its behalf); (2) operate the service "for commercial purposes"; and (3) either direct its service towards children or have "actual knowledge that it is collecting personal information from a child."[95]

If COPPA applies to a contact-tracing app, the app's operator must undertake a number of privacy-protecting steps. First, an operator must provide notice as to what type of information is collected and how it is used.[96] Second, the operator may not collect, use, or disclose personal information without receiving verifiable parental consent before the information is collected.[97] Lastly, operators must comply with certain data retention and deletion requirements, and they must also establish and maintain "reasonable procedures" designed to "protect the "confidentiality, security, and integrity" of the information.[98]

COPPA's consent requirement does not apply if information is collected, used, or disclosed "for an investigation on a matter related to public safety."[99] This provision could arguably permit public health authorities to access data for use in contact tracing without parental consent, even if the data would normally be protected by COPPA. However, the Federal Trade Commission (FTC) has not issued any guidance on the applicability of this exception to digital contact tracing. Lastly, operators must comply with certain data retention and deletion requirements, and they must also establish and maintain "reasonable procedures" designed to "protect the confidentiality, security, and integrity" of the information.[100]

The FTC is responsible for enforcing COPPA, and enforces violations of COPPA as violations of "a rule defining an unfair or deceptive act or practice" under the Federal Trade Commission Act (FTC Act).[101] The FTC has recovered considerable civil penalties against technology companies for violations of COPPA.[102] For further discussion of FTC enforcement, see the later section, "The Federal Trade Commission Act."

---

of Education's distribution of public funds to educational institutions.").

[93] 15 U.S.C. §§ 6501–06; 16 C.F.R. pt. 312.

[94] *See Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (last visited Aug. 14, 2020). Under COPPA, an *operator* is any person who operates a website or online service for commercial purposes in interstate and foreign commerce, and who "collects or maintains personal information" from or about the website's or online service's users. 15 U.S.C. § 6501(2).

[95] 15 U.S.C. § 6501(2), 6502(a); 6 C.F.R. § 312.2–312.3.

[96] 16 C.F.R. § 312.4.

[97] *Id.* § 312.5. COPPA also requires that the operator provide a method by which a parent can review the information shared by a child, prevent its further use, and take steps to ensure that personal information of children is properly secured. *Id.* §§ 312.6, 312.8.

[98] *Id.* §§ 312.8, 312.10.

[99] 15 U.S.C. § 6502(b)(2)(E)(iv).

[100] 16 C.F.R. §§ 312.8, 312.10.

[101] 15 U.S.C. § 6502(c).

[102] *E.g.*, Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sep. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-

Are Contact-Tracing Apps Covered?

Should COPPA apply to contact-tracing apps, it imposes significant limitations on how app administrators treat children's information. However, whether contact-tracing app administrators are subject to COPPA depends on (1) whether the app's administrator, which might be either a public health authority or a third-party contractor, collects personal information, (2) whether the app is operated for "commercial purposes," and (3) whether the apps are either directed to children or app administrators knowingly collect the personal information of children. While this analysis will ultimately turn on the factual particulars of any given contact-tracing app, it appears unlikely that most app administrators will be subject to COPPA, as discussed further below.

Collection of Personal Information

For purposes of COPPA, "collecting" personal information is defined broadly to include "the gathering of any personal information from a child by any means," including requesting the submission of personal information and passively tracking a child online.[103] "Personal information" means "individually identifiable information about an individual collected online."[104] The definition lists several specific examples, including a name, address, screen name, "[g]eolocation information sufficient to identify street name and name of a city or town," and a "persistent identifier" such as a "unique device identifier."[105]

Location tracking apps are likely to use geolocation information specific enough to qualify as "personal information" under COPPA, such as GPS information that is precise enough to identify street names and town names.[106] Whether proximity tracking identifiers qualify as "individually identifiable" is less clear. A cycling identifier like those used by the Apple-Google framework is not "persistent," even if it is a "unique device identifier."[107] For more discussion on this point, see "Do contact-tracing apps use PHI?," above.

If apps gather or use personal information, COPPA applies only if the app's *operator* collects the information. Plausible operators of contact tracing apps include either a public health authority or a third party contracted by a public health authority to manage app data, such as the app's developer.[108] If the operator does not receive any personal information from app users, COPPA

youtube-will-pay-record-170-million-alleged-violations; Press Release, Fed. Trade Comm'n, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That It Violated Children's Privacy Law (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

[103] 16 CFR § 312.2.

[104] *Id.*

[105] *Id.*

[106] *See* JAY STANLEY & JENNIFER STISA GRANICK, ACLU, THE LIMITS OF LOCATION TRACKING IN AN EPIDEMIC 3 (2020), https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf (noting that GPS typically has an accuracy of "5 to 20 meters under an open sky").

[107] APPLE, EXPOSURE NOTIFICATION 3 (2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf?1 (describing a "rolling proximity identifier" that "changes about every 15 minutes").

[108] *See* ASS'N OF STATE & TERRITORIAL HEALTH OFFS., ISSUE GUIDE: COVID-19 CASE INVESTIGATION AND CONTACT TRACING: CONSIDERATIONS FOR USING DIGITAL TECHNOLOGIES 7 (2020), https://www.astho.org/ASTHOReports/COVID-19-Case-Investigation-and-Contact-Tracing-Considerations-for-Using-Digital-Technologies/07-16-20/ (noting that "most states are contracting with members of the private sector to outsource data storage, data management, and workforce functions"); *see also Healthy Together App*, UTAH.GOV, https://coronavirus.utah.gov/healthy-together-app/ (indicating in an FAQ that "public health officials and a limited number of development employees" with a third-party contractor may access location data of app users). Utah's app no longer collects location information. Bethany Rodgers, *Utah's Expensive Coronavirus App Won't Track People's Movements Anymore, Its Key Feature*, SALT LAKE TRIBUNE

would not apply. However, even decentralized app configurations rely on collection of some data—namely, the location information or proximity identifiers associated with a positive diagnosis—by a centralized authority.[109] Such an authority would qualify as "collecting" information under COPPA.

Commercial Purposes

Online service administrators are not *operators* under COPPA unless they are operating online services for "commercial purposes."[110] Public health investigations undertaken by state and local governments are arguably noncommercial. Thus, contact-tracing apps may not be for "commercial purposes" if the information is obtained solely by public health officials for contact-tracing purposes. However, sharing app data with a for-profit third party, as North Dakota's contact-tracing app did for a time,[111] might constitute a "commercial purpose" under COPPA.[112]

Personal Information of Children

COPPA applies only when an operator operates an online service "directed to children" or when the operator has "actual knowledge" that it is collecting personal information from a child.[113] A child is an individual under the age of 13.[114] In determining whether an online service is directed to children, the FTC considers a range of indicia, including the online service's "subject matter, visual content, [and] use of animated characters or child-oriented activities."[115] The FTC may also consider "competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience."[116]

Public health authorities that have released contact-tracing apps describe the apps in staid terms and with limited imagery, often emphasizing the role the apps will play in responding to the public health crisis.[117] Officials in Virginia have taken the additional step of explicitly stating that their app is not intended for use by anyone under 13.[118] Contact-tracing apps are thus unlikely to

(July 11, 2020), https://www.sltrib.com/news/politics/2020/07/11/states-m-healthy-together/.

[109] *See* APPLE, EXPOSURE NOTIFICATION FREQUENTLY ASKED QUESTIONS 5 (2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf (detailing the situations in which a public health authority will have access to proximity tracking data).

[110] 15 U.S.C. § 6501(2).

[111] Stephen Groves, *Tech Privacy Firm Warns Contact Tracing App Violates Policy*, ASSOCIATED PRESS (May 22, 2020), https://apnews.com/03f2756664184cf1789c9b970beb7111.

[112] *Cf. Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (noting in section N.2. that a school contractor collecting student personal information that intends to use personal information "for its own commercial purposes in addition to the provision of services to the school" must obtain additional consent for this use). Additionally, COPPA does not explicitly apply to government bodies, such as state and local public health authorities, and it is unclear whether the FTC can bring enforcement actions against state governments for unfair and deceptive acts and practices. For further discussion of this issue, see the section "The Federal Trade Commission Act."

[113] 15 U.S.C. § 6502.

[114] *Id.* § 6501.

[115] 16 C.F.R. § 312.2.

[116] *Id.*

[117] *E.g.*, *CRUSH COVID RI*, R.I. DEP'T OF HEALTH, https://health.ri.gov/covid/crush/ (last visited Sept. 22, 2020); *Care19*, NDRESPONSE.GOV, https://ndresponse.gov/covid-19-resources/care19 (last visited Sept. 22, 2020); *PathCheck SafePlaces Mobile App*, TETON CTY., WYO. HEALTH DEP'T, https://www.tetoncountywy.gov/2156/PathCheck-SafePlaces-Mobile-App (last visited Sept. 22, 2020).

[118] *Virginia Department of Health COVIDWISE - Privacy Policy*, VA. DEP'T OF HEALTH (July 10, 2020),

be "directed at children," though operators may still face obligations under COPPA if they knowingly collect personal information from a child.

Given the above considerations—that contact-tracing apps are arguably not operated for commercial purposes and the apps are not typically directed at children—COPPA appears unlikely to place obligations on most public health authorities or third party contractors managing contact-tracing apps. However, this issue must ultimately be decided on a case-by-case basis, in light of the facts surrounding the particular app at issue.

The Privacy Act

As discussed, contact tracing is typically conducted by state and local health authorities rather than the federal government. However, it is conceivable that federal agencies like the CDC might help coordinate contact tracing activities among the states and might exchange contact tracing information with them as part of this process. To the extent that federal agencies receive contact-tracing information pertaining to individuals, they must comply with the Privacy Act of 1974.[119] Under the Privacy Act, federal agencies[120] must comply with privacy protections for any "record" they maintain in a "system of records."[121] The Privacy Act defines a *record* as encompassing "any item, collection, or grouping of information about an individual that is maintained by an agency" and that contains the individual's "name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[122] It further defines *system of records* as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[123] The Act also requires agencies to publish a notice in the federal register whenever they establish or revise a system of records, describing the nature of the system.[124] When the Privacy Act's protections apply, agencies must obtain the "prior written consent of the individual to whom the record pertains" before disclosing it to "any person, or to another agency."[125] However, the Privacy Act contains a number of exceptions to this consent requirement, such as the "routine use" exception, which allows agencies to use a record "for a purpose which is compatible with the purpose for which it was collected."[126] There is also a "health and safety" exception, which requires a showing that "compelling circumstances" affect the health and safety of an individual.[127]

Particularly relevant to COVID-19 and digital contact tracing, on July 20, 2020, the Department of Health and Human Services (HHS) published a system of records notice (SORN) explaining

https://www.vdh.virginia.gov/covidwise/privacy-policy/ (stating that the app "is not intended for children under the age of 13" and that the public health authority does "not knowingly allow a child under 13 to use the App").

[119] 5 U.S.C. § 552a.

[120] For purposes of the Privacy Act, an *agency* is an "authority of the Government of the United States, whether or not it is within or subject to review by another agency," including any "establishment in the executive branch" and "any independent regulatory agency" but not Congress, the courts, or the governments of the U.S. territories and District of Columbia. *Id.* §§ 551(1), 552(f)(1), 552a(a)(1).

[121] *Id.* § 552a(b)–(e).

[122] *Id.* § 552a(a)(4).

[123] *Id.* § 552a(a)(5).

[124] *Id.* § 552a(e)(4).

[125] *Id.* § 552a(b).

[126] *Id.* § 552a(a)(7).

[127] *Id.* § 552a(b)(8).

that it had established a new department-wide system of records covering "records used for surveillance and investigation of epidemics, preventable diseases and health problems."[128] This replaced an earlier system of records, which covered the same type of materials but was limited to the CDC, rather than all of HHS.[129] The SORN issued by HHS explains that the records covered by this system include "medical records and related documents," such as "case reports, lab requisition forms, patient consent forms, assurance statements, analytical testing data, questionnaires, and contact tracing reports."[130] It further explains that uses falling under the "routine use" exception include, among other things, disclosures to "HHS contractors and agents" and "state, local, and Tribal health departments and authorities."[131] This SORN is noteworthy because it indicates that, if HHS or the CDC does obtain medical records, contact tracing reports, or similar documents that show an individual's COVID-19 diagnosis or exposure (including information collected from digital contact tracing apps), then this information would be maintained in the system of records identified in the SORN and would likely be subject to the Privacy Act's requirements. However, the SORN also indicates that HHS has determined such records could be disclosed to its contractors or to state and local health departments under the routine use exception. Thus, even if the Privacy Act applies to this information, HHS likely has some flexibility in disclosing these records for contact-tracing purposes.

To the extent an individual believes that the CDC or any other federal agency has used contact-tracing information in a way that violates their rights under the Privacy Act, they may bring a civil action against the government in federal court.[132] The Act expressly allows any individual who has been "adverse[ly] affect[ed]" by an agency's violation to bring such actions.[133] If the individual prevails in the suit, the court may order the agency to "amend the individual's record in accordance with his request or in such other way as the court may direct" and to pay the reasonable attorney fees and litigation costs incurred by the individual.[134] Furthermore, if the court determines the agency acted "intentional[ly] or willful[ly]" then "the United States shall be liable to the individual" for an amount equal to their "actual damages" resulting from the violation, along with reasonable attorney fees and litigation costs.[135]

Electronic Communications Privacy Act (ECPA)

Congress passed the Electronic Communications Privacy Act (ECPA)[136] to, among other things, address the use of wiretapping or electronic eavesdropping equipment. The first part of ECPA, sometimes referred to as the Wiretap Act, criminalizes the unauthorized interception or disclosure of electronic communications in transmission.[137] Another section of ECPA, known as the Stored Communications Act (SCA), prohibits the unauthorized access of electronic communications at

[128] Notice of a New Statement of Records, and Rescindment of a System of Records, 85 Fed. Reg. 43859-01 (July 20, 2020), https://www.govinfo.gov/content/pkg/FR-2020-07-20/pdf/2020-15564.pdf.

[129] *Id*.

[130] *Id*. at 43,859–60.

[131] *Id*. at 43,860.

[132] 5 U.S.C. § 552a(g).

[133] *Id*. § 552a(g)(1).

[134] *Id*. § 552a(g)(2).

[135] *Id*. § 552a(g)(4).

[136] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[137] 18 U.S.C. §§ 2510–2522. Congress originally enacted these restrictions as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as the Wiretap Act), which ECPA amends. Pub. L. No. 90-351, 82 Stat. 197, 211.

rest (i.e., an e-mail stored on a server).[138] ECPA also includes language describing the processes government entities must undertake prior to gaining access to any electronic communications protected by the statute. Violations of ECPA may result in both civil and criminal penalties.[139] For a more detailed overview of ECPA and its provisions, see CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

Legal Background

ECPA protects only the *contents* of *electronic communications*. "Electronic communication" is broadly defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[140] The contents of an electronic communication are "any information concerning the substance, purport, or meaning of [a] communication."[141]

The different portions of ECPA contain different prohibitions and exceptions. The Wiretap Act prohibits "intercept[ing]" an electronic communication or disclosing an intercepted electronic communication.[142] "Intercept" means "the aural or other acquisition" of the contents of an electronic communication "through the use of any electronic, mechanical, or other device."[143] The Wiretap Act does not apply when the person intercepting the electronic communication is a party to the communication or a party to the communication has given consent,[144] nor does it apply when the electronic communication is available to the general public.[145]

While the Wiretap Act protects electronic communications in transit, the SCA prohibits unauthorized access to "a facility through which an electronic communication service is provided" that results in access to a communication "in electronic storage,"[146] as well as the voluntary disclosure of an electronic communication maintained on a "remote computing service" or held in electronic storage by "a person or entity providing an electronic communication service."[147] Electronic storage is either the "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" or "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[148] The SCA does not define "a facility through which an electronic communication service is provided"; however, the SCA's legislative history indicates that Congress intended to protect communications stored by third parties on a user's behalf, such as

[138] 18 U.S.C. §§ 2701–2711.

[139] *Id.* §§ 2520, 2707 (civil penalties for Wiretap Act and SCA); §§ 2511(4), 2701(b) (criminal penalties).

[140] *Id.* § 2510(12).

[141] *Id.* §§ 2510(8), 2711(a).

[142] *Id.* § 2511(1).

[143] *Id.* § 2510(4).

[144] *Id.* § 2511(2)(c), (d).

[145] *Id.* § 2511(2)(g).

[146] *Id.* § 2701(a).

[147] *Id.* § 2702(a). An "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15). A "remote computing service" is "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(3).

[148] *Id.* § 2510(17).

emails stored on a remote server.[149] Similar to the Wiretap Act, the SCA does not apply when a party to the communication has consented to its access or disclosure.[150] The SCA also permits disclosure of electronic communications to a government entity in the event of "an emergency involving danger of death or serious physical injury to any person."[151]

How Do ECPA's Exceptions Apply?

Both the Wiretap Act and the SCA include exceptions to their prohibitions when a party to the communication has given consent.[152] A public health official would not violate ECPA in receiving or disclosing contact-tracing information, even to a third party, because the public health official would likely be a party to the original communication.[153] Further, even if an entity collecting contact-tracing information is not a party to the communication, the majority of guidance on the adoption of digital contact-tracing tools, including guidance from the CDC, suggests that use of such tools should be voluntary.[154] Assuming that contact-tracing apps provide sufficient information on how information they collect will be used and shared, app providers likely could be able to rely on app users' consent.[155]

In addition to involving a transfer of data from a diagnosed app user to a public health authority, proximity tracking apps can involve countless transfers of data between users. These apps broadcast identifiers to any device within range of the app user's device, and any Bluetooth-capable devices that use a Google or Apple operating system—i.e., nearly all smartphones[156]—can send and receive these identifiers.[157] Some potential harms identified by privacy advocates,

---

[149] Hately v. Watts, 917 F.3d 770, 782 (4th Cir. 2019) (citing H.R. Rep. No. 99-647, at 18 (1986)); Garcia v. City of Laredo, 702 F.3d 788, 791 (5th Cir. 2012) (noting that, prior to passage of the SCA, "the United States Code provided no protection for stored communications in remote computing operations and large data banks that stored e-mails").

[150] 18 U.S.C. §§ 2701(c)(2), 2702(b)(3).

[151] *Id.* § 2702(b)(8).

[152] 18 U.S.C. §§ 2511(c),(d),(g), 2701(c)(2), 2702(b)(3).

[153] *See* In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 142–43 (3d Cir. 2015) (applying the "party to the communication" exception when Google placed a cookie on plaintiffs' web browsers that transmitted browsing activity to Google).

[154] CTRS. FOR DISEASE CONTROL & PREVENTION, GUIDELINES FOR THE IMPLEMENTATION AND USE OF DIGITAL TOOLS TO AUGMENT TRADITIONAL CONTACT TRACING 2 (2020), https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/guidelines-digital-tools-contact-tracing.pdf; *see also* JOSEPH ALI ET AL., DIGITAL CONTACT TRACING FOR PANDEMIC RESPONSE 20 (Jeffrey P. Kahn ed., 2020), https://muse.jhu.edu/book/75831/pdf (recommending "basic disclosure and voluntary agreement or authorization" for use of digital contact tracing tools); DANIEL KAHN GILLMOR, ACLU, PRINCIPLES FOR TECHNOLOGY-ASSISTED CONTACT-TRACING 4 (2020), https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_contact_tracing_principles.pdf (recommending voluntary participation for digital contact tracing tools).

[155] *See* Williams v. Affinion Grp., LLC, 889 F.3d 116, 121–22 (2d Cir. 2018) (holding that the consent exception to the ECPA applies when the customer is presented a webpage informing the customer that by clicking the "YES" button their information will be transferred to a third party). *But see* Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993) (informing employee that employee telephone calls would be "monitored" did not inform the employee of the manner in which monitoring would be conducted or that the employee individually would be monitored, and therefore did not constitute consent for the employer to record the employee's telephone calls).

[156] *See Mobile Operating System Market Share United States of America: Aug 2019 – Aug 2020*, STATCOUNTER GLOBAL STATS, https://gs.statcounter.com/os-market-share/mobile/united-states-of-america (last visited Sept. 22, 2020) (noting that more than 99% of U.S. smartphones run a Google or Apple operating system).

[157] *See* APPLE, EXPOSURE NOTIFICATION FREQUENTLY ASKED QUESTIONS 3 (2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf (noting that once enabled, a user's device will broadcast signals for other devices to receive).

such as the use of Bluetooth beacons to collect identifiers,[158] would therefore likely not violate ECPA, because the broadcast of a user's identifier is readily accessible by the public.[159]

The SCA contains an exception for disclosures made to government entities in the event of "an emergency involving danger of death or serious physical injury to any person."[160] Whether the COVID-19 outbreak constitutes such an emergency is unclear. The exception's historical application is largely to criminal investigations, particularly those involving kidnapping.[161]

The Federal Trade Commission Act

The Federal Trade Commission Act (FTC Act) is an integral part of the federal data protection law landscape. The key provision of the FTC Act, Section 5, declares unlawful "unfair or deceptive acts or practices" (UDAP) "in or affecting commerce."[162] The Act provides that an act or practice is only "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[163] While the Act does not define "deceptive," the Federal Trade Commission (FTC), which enforces the UDAP prohibition, has clarified in guidance that an act or practice is to be considered deceptive if it involves a material "representation, omission, or practice that is likely to mislead [a] consumer" who is "acting reasonably in the circumstances."[164] This prohibition broadly applies to most individuals and entities, although certain entities—such as common carriers, non-profits, and banks—are exempt.[165]

In contrast to many of the other federal data protection laws, the FTC Act does not impose any specific data protection obligations, such as a requirement to obtain consumer consent before sharing their data. Nevertheless, the FTC has used its case-by-case enforcement of the FTC Act's UDAP prohibition to signal the type of privacy practices it views as "unfair" or "deceptive," thus

---

[158] *See* Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. TIMES (June 14, 2019) (discussing the use of Bluetooth beacons in retail stores); Andrew Crocker et al., *The Challenge of Proximity Apps for COVID-19 Contact Tracing*, ELEC. FRONTIER FOUND. (Apr. 10, 2020), https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing (speculating that a "widespread network of Bluetooth readers" could be used to track individual app users).

[159] *See* 18 U.S.C. § 2511(2)(g).

[160] *Id.* § 2702(b)(8).

[161] *E.g.*, In re Application of U.S. for a Nunc Pro Tunc Order for Disclosure of Telecomms. Records, 352 F. Supp. 2d 45 (D. Mass 2005); United States v. Gilliam, No. 11 Crim. 1083, 2012 WL 4044632 (S.D.N.Y. Sep. 12, 2012)); Jayne v. Sprint PCS, No. CIV S-07-2522, 2009 WL 426117 (E.D. Cal. Feb. 20, 2009).

[162] 15 U.S.C. § 45(a)(1); *see also* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE 1 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (noting that the FTC's "primary legal authority comes from Section 5 of the Federal Trade Commission Act").

[163] 15 U.S.C. § 45(n).

[164] FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION 1–2, (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (capitalization altered); *see also*, In re Int'l Harvester Co., No. 9147, 1984 WL 565290, at *85 (FTC Dec. 21, 1984) ("Our approach to deception cases was described in a policy statement that the Commission issued in 1983. . . . In brief, a deception case requires a showing of three elements: (1) there must be a representation, practice, or omission likely to mislead consumers; (2) the consumers must be interpreting the message reasonably under the circumstances; and (3) the misleading effects must be 'material,' that is, likely to affect consumers' conduct or decision with regard to a product.").

[165] 15 U.S.C. § 45(a)(2) (providing the FTC with jurisdiction over all "persons, partnerships, or corporations" except certain exempted entities); Nat'l Fed'n of the Blind v. FTC, 420 F.3d 331, 354 (4th Cir. 2005) ("The FTC Act gives the agency jurisdiction over 'persons, partnerships and corporations,' but no authority over nonprofit organizations.").

creating what some scholars have called a "common law of privacy."[166] For instance, the FTC has frequently alleged that companies act deceptively when they violate their own privacy policies, such as collecting data they say they will not collect or failing to protect personal information from unauthorized access despite promises that that they would do so.[167] The FTC has also maintained that a company's failure to adopt reasonable data security standards may be "unfair" in and of itself.[168]

It is unclear whether the FTC could bring a UDAP action against state health departments or app developers acting on their behalf if the FTC believes these developers' data privacy and data security practices run afoul of the UDAP standard. For example, courts have invoked the state action doctrine—which provides immunity for certain state actions that might otherwise violate federal antitrust laws—in suits brought by the FTC against states or third parties acting under state authority alleging violations of the FTC Act's prohibition of "unfair methods of competition."[169] This doctrine may also apply to the FTC's UDAP authority, although the case law on this issue is relatively sparse. At least one district court has applied the state action doctrine to bar the FTC from using its UDAP enforcement power against a state entity, but that decision was later vacated on other grounds.[170] If the doctrine does apply to UDAP actions, it may apply not only to actions taken by the State itself but also to actions "carried out by others pursuant to state authorization," such as private parties or sub-state entities like municipal governments.[171] However, for immunity to apply to non-state actors, the conduct at issue must meet a two part test: the challenged action must be (1) "clearly articulated and affirmatively expressed as state policy" and (2) "actively supervised by the State."[172]

If the FTC decides to bring an enforcement action for a UDAP violation, it may commence either administrative enforcement proceedings or civil litigation against alleged violators.[173] In an administrative enforcement proceeding, an Administrative Law Judge (ALJ) hears the FTC's complaint and may issue a cease and desist order prohibiting the respondent from engaging in

---

[166] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619 (2014). For a further discussion of the FTC's "common law of privacy," see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[167] *See, e.g.*, Compl., In re Myspace LLC, No. C-4369 (F.T.C. Aug. 30, 2012) (alleging Myspace provided advertisers with users' personally identifiable information, despite promises in its privacy policy that it would not share such information); Compl., FTC v. Ruby Corp., No. 1:16-CV-02438 (D.D.C. Dec. 14, 2016) (alleging that operators of dating site AshleyMadison.com deceived consumers by assuring them that personal information would be protected but failing to implement the necessary security to prevent a data breach).

[168] *See, e.g.*, Compl. At 8, United States v. Rental Research Servs., Inc., No. 0:09-cv-00524-PJS-JJK (D. Minn. Mar. 5, 2009), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf (alleging that defendant's failure to employ reasonable and appropriate security measures to protect consumers' personal information was an unfair act or practice).

[169] *See, e.g.*, FTC v. Phoebe Putney Health Sys., Inc., 568 U.S. 216, 224–228 (2013) (applying the state action doctrine to an FTC enforcement action alleging unfair competition in violation of the FTC Act, but ultimately holding that the defendant was not entitled to immunity because there was no evidence the State affirmatively contemplated that the defendant would engage in the conduct at issue).

[170] *See* Cal. *ex rel.* Christensen v. FTC, 549 F.2d 1321, 1322 (9th Cir. 1977) ("The district court held that [the state action doctrine as established by the Supreme Court Case *Parker v. Brown*] immunized the advertising program in substantially the same manner and for substantially the same reasons described by the Supreme Court in holding California raisin marketing practices immune from antitrust liability. We express no opinion on the ultimate question of immunity under Parker v. Brown because we hold that judicial intervention in this case was premature.").

[171] *Phoebe Putney Health Sys.*, 568 U.S. at 225–26 (citation omitted).

[172] *Id.* at 225 (citation omitted).

[173] 15 U.S.C. §§ 45(a)(2), 45(b), 53(b).

wrongful conduct.[174] In civil litigation, the FTC may seek an injunction against a party that "is violating, or is about to violate" the FTC Act.[175] Historically, courts have allowed the FTC to obtain, in addition to injunctions, all forms of equitable relief, such as requiring the defendant to disgorge its ill-gotten gains.[176] However, the Seventh Circuit recently restricted the FTC's ability to seek broad equitable relief in these suits, and the Supreme Court has agreed to review this issue.[177] FTC enforcement actions are often settled, with parties entering into consent decrees.[178] The FTC may later bring a civil action for monetary penalties if parties subsequently violate such consent decrees, or any other final order of the FTC.[179]

Selected State, Foreign, and International Data Protection Laws

In addition to the federal laws discussed above, a number of state, foreign, and international[180] laws could potentially impact the development and implementation of contact-tracing apps.[181] Although these laws do not apply outside their respective jurisdictions, app developers engaged in interstate or international commerce may have to comply with these varying requirements. Likewise, users who have installed contact-tracing apps and travel to other jurisdictions may trigger the laws' application. This section discusses the major data laws of three jurisdictions—California, Canada, and the European Union—and how those laws may impact digital contact tracing.

---

[174] *Id.* § 45(b); *see also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (Oct. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority ("Upon conclusion of the hearing, the ALJ issues an 'initial decision' setting forth his findings of fact and conclusions of law, and recommending either entry of an order to cease and deist or dismissal of the complaint.").

[175] 15 U.S.C. § 53(b). In light of a recent decision by the U.S. Court of Appeals for the Third Circuit, the FTC may be unable to bring civil suits based on past UDAP violations that are no longer ongoing. In *FTC v. Shire ViroPharma, Inc.*, the Third Circuit held that, in civil actions under Section 13(b) of the FTC Act, the FTC must show that the defendant "is violating, or is about to violate" the law and that this standard requires more than simply showing that the conduct is "likely to recur." 917 F.3d 147, 159 (3d Cir. 2019) ("In short, we reject the FTC's contention that Section 13(b)'s 'is violating' or 'is about to violate' language can be satisfied by showing a violation in the distant past and a vague and generalized likelihood of recurrent conduct. Instead, 'is' or 'is about to violate' means what it says—the FTC must make a showing that a defendant is violating or is about to violate the law." (footnote omitted)). For additional background on this issue, see CRS Legal Sidebar LSB10232, *UPDATE: Will the FTC Need to Rethink its Enforcement Playbook? Third Circuit Considers FTC's Ability to Sue Based on Past Conduct*, by Chris D. Linebaugh.

[176] CRS Legal Sidebar LSB10388, *Will the FTC Need to Rethink Its Enforcement Playbook (Part II)? Circuit Split Casts Doubt on the FTC's Ability to Seek Restitution in Section 13(b) Suits*, by Chris D. Linebaugh.

[177] *Id.*

[178] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 610–11 (2014) ("[V]irtually every [privacy-related] complaint has either been dropped or settled.").

[179] 15 U.S.C. § 45(l).

[180] *Foreign law* refers to the domestic laws of other countries, while *international law* refers to laws that apply among nations. *See, e.g.*, *Foreign, Comparative, and International Law: Definitions*, UNIV. OF MICH. L. LIBR. (Aug. 18, 2020, 12:29 pm), https://libguides.law.umich.edu/fcil.

[181] For a comparison of state privacy laws, including bills introduced in state legislatures, see Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PROF'LS (updated July 6, 2020), https://iapp.org/resources/article/state-comparison-table/. For a detailed discussion of foreign and international privacy laws, see *Online Privacy Law*, L. LIBR. OF CONG. (July 24, 2020), https://www.loc.gov/law/help/online-privacy-law/index.php. For a discussion of how different countries and other international jurisdictions are using electronic tools to respond to the COVID-19 pandemic, see GLOB. LEGAL RSCH. DIRECTORATE, L. LIBR. OF CONG., LL FILE NO. 2020-019000, REGULATING ELECTRONIC MEANS TO FIGHT THE SPREAD OF COVID-19 (2020).

California

The California Constitution recognizes privacy as an inalienable right.[182] In furtherance of this right, California has enacted a number of privacy laws,[183] including the California Consumer Privacy Act of 2018 (CCPA).[184] California enacted the CCPA[185] to "giv[e] consumers an effective way to control their personal information."[186] The CCPA took effect on January 1, 2020,[187] and the California Attorney General's regulations implementing the CCPA took effect on August 14, 2020.[188] The CCPA generally regulates how businesses collect and use consumers' personal information. It limits a covered business's activities, affords individuals specific rights over their personal information, and establishes enforcement mechanisms.

Scope of the CCPA

The CCPA protects *consumers*—natural persons who are California residents[189]—and their *personal information*—"information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[190] Examples of personal information under the CCPA include biometric information, internet browsing and search histories, and geolocation data.[191] Personal information does not include publicly available information, de-identified information (that is, information that associated with a particular consumer[192]), or aggregate information.[193] It also does not include information protected by HIPAA.[194]

Under the CCPA, a covered *business* is any for-profit entity, including a sole proprietorship, partnership, or corporation, that (1) operates in California, (2) collects or receives consumers' personal information, and (3) satisfies any of the following thresholds:[195]

- earns more than $25 million in annual gross revenue;
- buys, sells, or receives the personal information of 50,000 or more California residents; or

[182] CAL. CONST. art. I, § 1.

[183] For a list of California privacy laws, see *Privacy Laws*, CAL. DEP'T OF JUSTICE, https://oag.ca.gov/privacy/privacy-laws (last visited Sept. 22, 2020). Of note, California's analogue to the federal Privacy Act is the Information Practices Act of 1977, CAL. CIV. CODE §§ 1798–1798.78. California's analogue to HIPAA is the Confidentiality of Medical Information Act, CAL. CIV. CODE §§ 56–56.37.

[184] CAL. CIV. CODE §§ 1798.100–1798.199.

[185] California Consumer Privacy Act of 2018, Assemb. 375, 2017-18 Sess. (Cal. 2018), 2018 Cal. Stat. ch. 55.

[186] *Id.* § 2(i).

[187] CAL. CIV. CODE § 1798.198(a).

[188] *See CCPA Regulations*, CAL. DEP'T OF JUSTICE, https://oag.ca.gov/privacy/ccpa/regs (last visited Sept. 22, 2020).

[189] CAL. CIV. CODE § 1798.140(g).

[190] *Id.* § 1798.140(o)(1).

[191] *Id.*

[192] *Id*, § 1798.140(h).

[193] *Id.* § 1798.140(o)(2)–(3).

[194] *Id.* § 1798.145(c)(1)(A).

[195] *Id.* § 1798.140(c)(1).

- derives more than 50% of its annual revenue from the sale of California residents' personal information.[196]

Consumer Rights

The CCPA protects three broad categories of consumer rights. First, it grants consumers a right to certain information about how and why businesses collect and use their personal data.[197] Before collecting any personal information from a consumer, a business must disclose the categories of information it will collect and the purpose of the collection.[198] Businesses must also notify consumers of their rights under the CCPA.[199] In addition, a consumer may request several other types of information from a business, including: (1) the specific pieces of personal information a business has collected;[200] (2) where it obtained the information;[201] and (3) the categories of third parties with which it shared the information.[202]

Second, the CCPA guarantees a consumer's right to request that a business delete any information it has collected about the consumer.[203] This right is subject to several limitations.[204] For example, a business is not required to delete information necessary to complete the transaction for which it collected the information or to fulfill the terms of a warranty.[205] Similarly, a business need not delete information necessary to detect security incidents or illegal activity or to identify and repair system errors.[206]

Third, the CCPA gives a consumer the right to opt out of the sale of the consumer's information to third parties.[207] Consumers may exercise this right at any time,[208] and a business that receives a customer's opt-out direction may not sell that customer's information unless the customer later reauthorizes the sale.[209] In addition, businesses may not sell the data of a consumer under sixteen years old without express consent from either the consumer or their guardian.[210]

Business Obligations

Along with the individual rights above, the CCPA imposes several obligations on covered businesses. First, the CCPA prohibits discrimination against a consumer based on that consumer's exercise of any of the above rights.[211] Under this prohibition, a business may not deny goods or

[196] *Id.* § 1798.140(c)(1)(A)–(C).

[197] *Id.* §§ 1798.100, 1798.110, 1798.115.

[198] *Id.* § 1798.100(b).

[199] *See id.* §§ 1798.105(b), 1798.120(b).

[200] *Id.* § 1798.100(a).

[201] *Id.* § 1798.110(a)(2).

[202] *Id.* § 1798.110(a)(4).

[203] *Id.* § 1798.105(a).

[204] *See id.* § 1798.105(d).

[205] *Id.* § 1798.105(d)(1).

[206] *Id.* § 1798.105(d)(2)–(3).

[207] *Id.* § 1798.120.

[208] *Id.* § 1798.120(a).

[209] *Id.* § 1798.120(d).

[210] *Id.* § 1798.120(c).

[211] *Id.* § 1798.125(a)(1).

services to a consumer who, for example, opts out of the sale of personal information.[212] Likewise, a business may not provide a different level of service to a consumer who exercises the above rights.[213] A business may, however, provide a financial incentive to consumers who agree to the collection or sale of their data.[214] Second, businesses must provide conspicuous notice of consumers' rights and means to enforce those rights.[215] This includes including a conspicuous link on a business's webpage titled "Do Not Sell My Personal Information" and a toll-free telephone number to request information.[216] Finally, businesses must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" they collect.[217] If a business fails to do so, it could face civil penalties in the event of a data breach.[218]

Enforcement

The CCPA provides two enforcement mechanisms. Businesses that receive notice of noncompliance must cure the alleged violations within thirty days.[219] If a business fails to do so, it may be subject to penalties in a civil action brought by the California Attorney General.[220] To promote enforcement, the CCPA created a "Consumer Privacy Fund" to offset court and Attorney General costs.[221]

Second, the CCPA authorizes private rights of action in limited circumstances.[222] A consumer may bring a civil action against a business if that consumer's "nonencrypted and nonredacted" personal information is stolen or disclosed without authorization as a result of a business's failure to safeguard the information.[223] A consumer may recover damages, seek court orders directing a business to take certain action, and receive "[a]ny other relief the court deems proper."[224] Consumers may not, however, bring a civil action to enforce any other provision of the CCPA.[225]

CCPA and Contact Tracing

Although the CCPA could potentially cover a digital contact-tracing app, the circumstances under which it would apply are narrow. Because the CCPA only applies to for-profit businesses, it would not cover apps developed by state or local public health authorities.[226] It could, however, apply to a private contractor that develops and runs an application for a state or local agency. Similarly, whether the CCPA applies would depend on the type of data an app collects. Because

[212] *See id.* § 1798.125(a)(1)(A).

[213] *Id.* § 1798.125(a)(1)(C).

[214] *Id.* § 1798.125(b).

[215] *Id.* §§ 1798.130–1798.135.

[216] *Id.* §§ 1798.130(a)(1)(A), 1798.135(a)(1).

[217] *Id.* § 1798.150(a)(1).

[218] *Id.*

[219] *Id.* § 1798.155(b).

[220] *Id.* § 1798.155(c).

[221] *Id.* § 1798.160.

[222] *Id.* § 1798.150(a)(1).

[223] *Id.*

[224] *Id.* § 1798.150(a)(1)(A)–(C).

[225] *Id.* § 1798.150(c).

[226] *See id.* § 1798.140(c)(1).

the CCPA only applies to personal information and excludes information covered by HIPAA,[227] it likely would not cover applications that collect only an anonymous identifier or that link an anonymous identifier with a COVID-19 diagnosis. On the other hand, the CCPA could apply to apps that collect users' location data or other personal information to the extent that the collected information is not PHI subject to HIPAA.

Canada

Canadian privacy law consists of a body of federal, provincial, and territorial laws that work together to protect individuals' information based on the type of entity being regulated and the type of covered data at issue.[228] At the federal level, two laws—the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA)—govern the collection, use, and disclosure of personal information.[229] The Office of the Privacy Commissioner of Canada (OPC) enforces both laws and provides guidance on whether the laws apply to a given situation.[230] To that end, OPC has worked with the Canadian government to assess the privacy ramifications of *COVID Alert*, an exposure notification application that the government deployed on July 31, 2020.

Canada's Privacy Act

Like its U.S. analogue,[231] Canada's Privacy Act governs information held by government institutions.[232] It defines *personal information* as "information about an identifiable individual that is recorded in any form" and prohibits government institutions from collecting personal information "unless it relates directly to an operating program or activity of the institution."[233] It also requires government institutions to inform individuals of the purpose for which any information is collected[234] and limits the use, retention, and disclosure of any collected information.[235] For example, the Privacy Act specifies that government institutions must retain any information they collect for sufficient time to allow individuals "a reasonable opportunity" to access the information.[236] Likewise, government institutions may not use personal information for a purpose other than for which it was obtained, with the exception of enumerated circumstances in which the government may disclose the information, such as when "the public interest in disclosure clearly outweighs any invasion of privacy."[237]

[227] *Id.* §§ 1798.140(o)(1), 1798.145(c)(1)(A).

[228] *See Summary of Privacy Laws in Canada*, OFF. OF THE PRIV. COMM'R OF CAN. (Jan. 31, 2018), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

[229] *Id.*; *see also* Privacy Act, R.S.C. 1985, c P-21 (Can.) [hereinafter Can. Priv. Act]; Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.)

[230] *See* Can. Priv. Act §§ 29–35; PIPEDA §§ 11–13.

[231] *See infra* "The Privacy Act."

[232] Can. Priv. Act § 3.

[233] *Id.* §§ 3–4.

[234] *Id* § 5(2).

[235] *Id.* §§ 6–9.

[236] *Id.* § 6(1).

[237] *Id.* §§ 7, 8(2).

In addition to the responsibilities the Privacy Act places on government institutions, it guarantees individuals the right to access personal information in the possession of government agencies.[238] There are, however, several exceptions to this right.[239] For example, a government agency may refuse to disclose information that "could reasonably be expected to threaten the safety of individuals."[240] An agency may also refuse to disclose certain types of professional information, such as information protected by attorney-client privilege[241] or medical records when disclosure of those records is not in the best interests of their subject.[242]

If an individual believes a government agency has improperly used or disclosed personal information concerning the individual, or if an agency refuses to allow an individual access to personal information in the agency's possession, the individual can file a complaint with the OPC.[243] The OPC may also initiate a complaint.[244] Once the OPC receives a complaint, it begins an investigation that culminates in a report of findings and recommendations.[245] Both an individual and the OPC may request judicial review of an OPC report of findings and recommendations in the Federal Court of Canada, but only in cases where a government agency has refused to provide access to personal information.[246]

PIPEDA

In contrast to Canada's Privacy Act, PIPEDA applies to personal information collected, used, or disclosed by *private* entities in the course of commercial activities.[247] Like the Privacy Act, it defines *personal information* as "information about an identifiable individual."[248] It applies to *organizations*—associations, partnerships, persons, or trade unions—that engage in commercial activity or "the operation of a federal work, undertaking or business."[249] Some organizations—including those subject to an analogous territorial privacy law, nonprofits, and journalists—are exempt from PIPEDA's requirements.[250]

Organizations subject to PIPEDA generally must adhere to ten *fair information principles*:[251]

[238] *Id*. §§ 12–17.

[239] *See id*. §§ 18–28.

[240] *Id*. § 25.

[241] *Id*. § 27.

[242] *Id*. § 28.

[243] *Id*. § 29(1).

[244] *Id*. § 29(3).

[245] *Id*. §§ 29–35.

[246] *Id*. §§ 41–42.

[247] PIPEDA §§ 2–4. Specifically, PIPEDA applies to *organizations*. *See id*. §§ 2, 4.

[248] *Id*. § 2.

[249] *Id*. § 4. PIPEDA defines *federal work, undertaking, or business* as an activity within the legislative authority of Parliament, as opposed to one of the territorial governments. *Id*. Such activities include inland and maritime shipping, air transportation, radio broadcasting, and banking. *Id*.

[250] *Id*. §§ 2, 4(1)(a), 4(2)(c).

[251] *Id*. § 5; *see PIPEDA In Brief*, OFF. OF THE PRIV. COMM'R OF CAN. (June 7, 2019), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

- *Accountability*—organizations must assume responsibility for personal information and designate an individual to ensure PIPEDA compliance and oversee day-to-day collection and processing of personal information;[252]
- *Identifying purposes*—organizations must identify (1) the purposes for any collection of personal information at or before the time of collection and (2) any new purposes before previously collected information is used for that purpose;[253]
- *Consent*—organizations must obtain individuals' informed consent prior to collecting, using, or disclosing personal information, except where "inappropriate";[254]
- *Limiting collection*—organizations must limit the collection of personal information to "that which is necessary for the purposes identified by the organization" and must use only "fair and lawful means" to do so;[255]
- *Limiting use, disclosure, and retention*—an organization must not use or disclose information for purposes other than those for which it was collected, unless the organization obtains consent or is required to do so by law, and an organization must destroy, erase, or anonymize personal information no longer needed;[256]
- *Accuracy*—organizations must ensure personal information is "as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used";[257]
- *Safeguards*—organizations must protect personal information with "safeguards appropriate to the sensitivity of the information"[258] and have a duty to notify the OPC and individuals of data breaches;[259]
- *Openness*—organizations must make their privacy policies and practices "readily available" to individuals;[260]
- *Individual access*—an organization must, on request, inform an individual of the existence, use, and disclosure of the individual's personal information and provide the individual access to that information;[261] and
- *Challenging compliance*—an organization must provide individuals with a mechanism to challenge the organization's compliance with PIPEDA and to receive and respond to complaints or inquiries about the organization's policies.[262]

[252] PIPEDA sched. I, § 4.1.

[253] *Id*. sched. I, § 4.2.

[254] *Id*. sched. I, § 4.3.

[255] *Id*. sched. I, § 4.4.

[256] *Id*. sched. I, § 4.5.

[257] *Id*. sched. I, § 4.6.

[258] *Id*. sched. I, § 4.7.

[259] *Id*. § 10.1.

[260] *Id*. sched. I, § 4.8.

[261] *Id*. sched. I, § 4.9.

[262] *Id*. sched. I, § 4.10.

Organizations may use personal information without consent in limited circumstances, such as when necessary for law enforcement, litigation, or national security.[263] Notably, an organization may use personal information without an individual's knowledge or consent "if it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual."[264]

An individual who believes an organization has failed to comply with PIPEDA with respect to the individual's personal information may file a complaint with the OPC.[265] In addition, the OPC can initiate a complaint when there are "reasonable grounds to investigate a matter."[266] Once the OPC receives a complaint, it begins an investigation that culminates in a report of findings and recommendations but may not award damages to a complainant.[267] Complainants may seek review of the OPC's decision in the Federal Court of Canada.[268] Unlike the OPC, the Federal Court is authorized to award damages for breaches of PIPEDA.[269]

Digital Contact Tracing in Canada

On July 31, 2020, the Government of Canada began rolling out *COVID Alert*, a voluntary digital exposure notification app.[270] The app, currently limited to two provinces, uses mobile devices' Bluetooth radios to exchange randomly-assigned identifier codes.[271] It then periodically checks those codes against a database of codes from users who have reported positive COVID-19 test results.[272] If a user has been near one of the codes linked to a COVID-19 diagnosis, the app will notify the user of the potential exposure.[273]

Before the app's release, the OPC conducted a review to determine whether the app complied with Canada's privacy laws.[274] It concluded that, because the app does not collect personal information, only anonymous identifiers, Canada's Privacy Act likely does not apply to the app.[275] The OPC recognized, however, that the data collected by the app is "extremely privacy sensitive and the subject of reasoned concern for the future of democratic values" and that there

[263] *Id.* §§ 7–9.

[264] *Id.* § 7(2)(b).

[265] *Id.* § 11(1).

[266] *Id.* § 11(2).

[267] *Id.* §§ 12–13.

[268] *Id.* § 14.

[269] *Id.* § 16.

[270] *Download COVID Alert Today*, GOV'T OF CAN. (Sept. 15, 2020), https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html; *see also* Ivan Semeniuk, *Ottawa Launches 'COVID Alert' App That Notifies Users About Contact with Coronavirus Cases*, THE GLOBE & MAIL (July 31, 2020), https://www.theglobeandmail.com/canada/article-ottawa-launches-covid-alert-app-that-notifies-users-about-contact/; Emma Jacobs, *Canada Begins Rolling Out COVID Contact Notification App in Ontario*, N. Country Pub. Radio (Aug. 4, 2020), https://www.northcountrypublicradio.org/news/story/42046/20200804/canada-begins-rolling-out-covid-contact-notification-app-in-ontario.

[271] *Download COVID Alert Today*, *supra* note 270.

[272] *Id.*

[273] *Id.*

[274] *Privacy Review of the COVID Alert Exposure Notification Application*, OFF. OF THE PRIV. COMM'R OF CAN. (July 31, 2020) [hereinafter *Privacy Review*], https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/.

[275] *Id.* ("The Privacy Assessment affirms that COVID Alert does not collect any personal information, which suggests that the federal *Privacy Act* does not apply.").

was a low risk of re-identification in limited circumstances.[276] The OPC recommended modifying Canada's privacy laws to account for "a more nuanced approach" to whether the app's data is protected.[277]

Because the *COVID Alert* app is a government initiative that does not collect personal information, it does not appear to be subject to either Canada's Privacy Act or PIPEDA. However, other contact-tracing apps could be subject to those laws' provisions depending on who runs the applications and what information they collect. Canadian courts have recognized that the OPC has "jurisdiction to investigate complaints relating to the transborder flow of personal information, including flows across the U.S. border."[278] Thus, if a U.S.-based company collects a Canadian's personal information through a digital contact-tracing app, that company might be subject to PIPEDA with respect to that information.

European Union

Data privacy in the European Union is governed by the General Data Protection Regulation (GDPR), a comprehensive privacy and data security framework adopted in May 2016 and in force since May 2018.[279] The objectives of the GDPR are to (1) protect individuals' fundamental rights and freedoms, "in particular their right to the protection of personal data," and (2) ensure free movement of personal data in the European Union.[280] To that end, the GDPR imposes broad obligations on any entity that processes personal data, either through automated means or as part of a filing system.[281] It also guarantees individuals certain rights with respect to their personal data.[282] EU member states are responsible for establishing *supervisory authorities* to enforce the GDPR's provisions,[283] and individuals may lodge complaints with the supervisory authorities and seek judicial review of the authorities' decisions.[284]

Scope of the GDPR

The GDPR applies to the processing—including collection, storage, use, and disclosure—of personal data either (1) "wholly or partly by automated means" or (2) "which form part of a filing system or are intended to form part of a filing system."[285] It defines *personal data* as "any

[276] *Id.*; *see* Elizabeth Thompson, *COVID Alert App Could Result in Some People Being ID'd*, CBC (Aug. 5, 2020), https://www.cbc.ca/news/politics/covid-alert-app-privacy-1.5674392.

[277] *Privacy Review*, *supra* note 274.

[278] OFF. OF THE PRIV. COMM'R OF CAN., REPORT OF FINDINGS: COMPLAINT UNDER PIPIEDA AGAINST ACCUSEARCH INC., DOING BUSINESS AS ABIKA.COM ¶ 3 (July 27, 2009), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/2009_009_rep_0731/.

[279] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR], 2016 O.J. (L 119) 1; *Data Privacy in the EU*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (last visited Aug. 17, 2020).

[280] GDPR, *supra* note 279, art. 1, ¶¶ 2–3.

[281] *Id.* art. 2, § 1; *see id.* arts. 5–6.

[282] *See id.* ch. III.

[283] *See id.* ch. VI.

[284] *Id.* ch. VIII.

[285] *Id.* art. 2, ¶ 1, art. 4, ¶ 2.

information relating to an identified or identifiable natural person."[286] The GDPR applies to both *controllers*—who "determine[] the purposes and means of the processing of personal data"—and *processors*—who process personal data on behalf of a controller.[287] Notably, the GDPR applies to both private and governmental controllers and processors.[288] It also applies to activities outside the European Union, including (1) personal data processed outside the European Union by EU-based controllers or processors; and (2) personal data processed by non-EU controllers or processors concerning data subjects within the European Union in connection with commercial activity or behavior monitoring.[289]

Data Controllers' and Processors' Obligations

Under the GDPR, data controllers and processors must satisfy a number of obligations with respect to personal data. These obligations fall into seven broad categories: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability.[290] Furthermore, controllers and processors may only process personal data if one of the following lawful bases applies:[291]

- The data subject has given consent;[292]
- Processing is necessary for reasons related to a contract with the data subject;[293]
- Processing is necessary to comply with a legal obligation;[294]
- Processing is necessary to protect the vital interests of the data subject or another individual;[295]
- Processing is necessary to the public interest or to the exercise of official authority;[296] or
- Processing is necessary for legitimate interests that override the individual rights and freedoms of the data subject.[297]

Controllers and processors must "implement appropriate technical and organizational measures" to safeguard personal data and must notify the appropriate supervisory authority and affected individuals in the event of a data breach.[298]

---

[286] *Id.* art. 4, ¶ 1.

[287] *Id.* art. 4, ¶¶ 7–8.

[288] *Cf. id.* art. 2, ¶ 2(b), (d) (excluding processing by member states in connection with national security and law enforcement activities). Although the European Union and its institutions are not directly covered by the GDPR, the GDPR requires the European Union to adapt its governing privacy regulations to conform with the GDPR's principles and rules. *Id.* art. 2, ¶ 3.

[289] *Id.* art. 3, ¶¶ 1–2.

[290] *Id.* art. 5.

[291] *Id.* art. 6, ¶ 1.

[292] *Id.* art. 6, ¶ 1(a).

[293] *Id.* art. 6, ¶ 1(b).

[294] *Id.* art. 6, ¶ 1(c).

[295] *Id.* art. 6, ¶ 1(d).

[296] *Id.* art. 6, ¶ 1(e).

[297] *Id.* art. 6, ¶ 1(f).

[298] *Id.* arts. 25, 28, 32–34.

Beyond these general obligations, the GDPR prohibits the processing of "special categories" of personal data, including race, sexual orientation, political opinions, religious beliefs, and biometric data, unless a controller or processor satisfies even stricter requirements.[299] For example, a controller or processor may process these special categories of data only if an individual provides *explicit*—as opposed to general—consent or if necessary for certain permissible purposes, such as legal proceedings, serving a substantial public interest (including public health emergencies), or to protect the interests of an individual who is unable to give consent.[300]

Individual Rights

In addition to the obligations that the GDPR places on data controllers and processors, it also guarantees a number of rights to individuals with respect to their personal data. These include rights of *transparency* as to how controllers and processors use their data and *access* to data held by controllers and processors, including the right to know the purpose for which data is processed and any recipients of the data.[301] Individuals also have rights of *rectification*—or correction of errors—and *deletion* of covered data, including the *right of erasure* or *right to be forgotten* when a controller no longer has a legitimate need to retain the data.[302] Finally, individuals have a right to *object* to how controllers process their personal data, absent "compelling legitimate grounds for the processing which override the interests, rights and freedoms" of the individual.[303]

Enforcement

The GDPR requires EU member states to establish independent *supervisory authorities* to enforce and promote the GDPR within each state.[304] The supervisory authorities have broad investigative and corrective powers, including the ability to impose fines and order the suspension of data processing.[305] In addition, the GDPR established a European Data Protection Board to ensure uniform application of the GDPR across EU member states.[306] The GDPR guarantees individuals several enforcement mechanisms, including (1) lodging complaints with EU member states' supervisory authorities;[307] (2) seeking judicial review of a supervisory authority's decision;[308] and (3) seeking a judicial remedy against a controller or processor in the courts of an EU member state.[309]

[299] *Id.* art. 9, ¶ 1.
[300] *Id.* art. 9, ¶ 2.
[301] *Id.* arts. 12–15.
[302] *Id.* arts. 16–17.
[303] *Id.* art. 21.
[304] *Id.* arts. 54, 57.
[305] *Id.* art. 58.
[306] *Id.* arts. 68, 70.
[307] *Id.* art. 77.
[308] *Id.* art. 78.
[309] *Id.* art. 79.

Contact Tracing and the GDPR

As part of a coordinated, EU-wide response to the COVID-19 pandemic, most EU member states have launched or are developing national contact-tracing apps.[310] In addition, the European Data Protection Board has developed guidelines on the use of location data in contact-tracing apps,[311] and the European Commission has issued guidance on data protection standards with respect to COVID-19-related apps.[312] Notably, the European Commission has determined that location data is "not necessary for the purpose of contact tracing and advises [member states] not to use location data in this context."[313] In June, EU member states reached an agreement to make their mobile contact-tracing apps interoperable, so that users throughout the European Union can continue to use their home state's app when traveling to other member states.[314] The technical standards underlying this agreement mandate that no geolocation data be used, only proximity information "exchanged in an encrypted way that prevents the identification of an individual person."[315]

Given the extraterritorial reach of the GDPR, it is possible that U.S.-based contact-tracing apps could be subject to the GDPR's requirements in limited circumstances. For example, if an individual installs a U.S. contact-tracing app and then travels to the European Union, any data collected by that application in the European Union would likely fall under the scope of the GDPR.[316] In addition, an EU company that deployed an app in the United States would likely also be subject to the GDPR's requirements.[317]

Legislation in the 116th Congress

In response to the ongoing COVID-19 pandemic, five data privacy bills addressing digital contact tracing and exposure notification have been introduced in the 116th Congress:

- The COVID-19 Consumer Data Protection Act of 2020 (CCDPA),[318] introduced by Senators Roger Wicker, John Thune, Jerry Moran, Marsha Blackburn, and Deb Fischer on May 7, 2020;

---

[310] *See Coronavirus Response*, EUR. COMM'N, https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response_en (last visited Sept. 22, 2020); EUR. COMM'N, MOBILE APPLICATIONS TO SUPPORT CONTACT TRACING IN THE EU'S FIGHT AGAINST COVID-19: PROGRESS REPORTING JUNE 2020 at 4 (2020), *available at* https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf.

[311] *See* EUR. DATA PROT. BD., GUIDELINES 04/2020 ON THE USE OF LOCATION DATA AND CONTACT TRACING TOOLS IN THE CONTEXT OF THE COVID-19 OUTBREAK (2020), *available at* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en.

[312] *Coronavirus: Guidance to Ensure Full Data Protection Standards of Apps Fighting the Pandemic*, EUR. COMM'N (Apr. 16, 2020) [hereinafter *Eur. Comm'n Guidance*], https://ec.europa.eu/commission/presscorner/detail/en/ip_20_669; *see also* Commission Implementing Decision (EU) 2020/1023 of 15 July 2020, amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic, 2020 O.J. 227/I.

[313] *Eur. Comm'n Guidance*, *supra* note 312.

[314] *Coronavirus: Member States Agree on an Interoperability Solution for Mobile Tracing and Warning Apps*, EUR. COMM'N (June 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043.

[315] *Id.*

[316] *See* GDPR, art. 3, ¶ 2(b).

[317] *See id.* art. 3, ¶ 1.

[318] COVID-19 Consumer Data Protection Act of 2020 (CCDPA), S. 3663, 116th Cong. (2020).

- The Public Health Emergency Privacy Act (PHEPA),[319] companion bills introduced, respectively, by Senators Richard Blumenthal and Mark Warner and Representatives Anna Eshoo, Janice Schakowsky, Suzan DelBene, Yvette Clarke, G.K. Butterfield, and Tony Cardenas on May 14, 2020;
- The Exposure Notification Privacy Act (ENPA),[320] introduced by Senators Maria Cantwell and Bill Cassidy on June 1, 2020; and
- The Secure Data and Privacy for Contact Tracing Act of 2020 (SDPCTA),[321] introduced by Representatives Jackie Speier, Diana DeGette, Debbie Dingell, Andre Carson, Nanette Diaz Barragan, Stephen F. Lynch, Jamie Raskin, Michael F.Q. San Nicolas, Mark Takano, and Alcee L. Hastings on July 1, 2020.

This section describes the main components of each bill and examines some key differences among the proposals.

Key Provisions and Major Differences

The CCDPA, PHEPA, and ENPA would each take a similar approach to regulating contact-tracing data. Under each bill, a *covered entity* would have to take certain steps before and after collecting *covered data*, and each bill would grant certain rights to individuals over collected data. In addition, each bill would create enforcement mechanisms to ensure that covered entities comply with their obligations regarding covered data. But there are several major differences among the bills, including the types of entities they cover and the precise rights they afford to individuals. While the CCDPA and PHEPA would apply specifically to the current COVID-19 pandemic,[322] the ENPA would not be limited to the current public health emergency.[323] The ENPA, however, would apply only to data collected by an *automated exposure notification service*, which it defines as a tool for "digitally notifying, in an automated manner, an individual who may have become exposed to an infectious disease."[324]

In contrast, the SDPCTA would authorize the CDC to award grants to eligible state, tribal, and territorial public health authorities to establish contact-tracing programs, including digital contact-tracing solutions, or incorporate digital contact tracing into existing programs.[325] As a condition for the use of grant awards for digital contact tracing, the SDPCTA would require public health authorities to satisfy several requirements, including obtaining users' voluntary, informed consent;[326] limiting the data collected;[327] and providing for the deletion of data.[328]

The key provisions of each bill are discussed below, and **Table 1** summarizes their main differences.

[319] Public Health Emergency Privacy Act (PHEPA), S. 3749, 116th Cong. (2020); PHEPA, H.R. 6866, 116th Cong. (2020).

[320] Exposure Notification Privacy Act (ENPA), S. 3861, 116th Cong. (2020).

[321] Secure Data and Privacy for Contact Tracing Act of 2020 (SDPCTA), H.R. 7472, 116th Cong. (2020).

[322] *See* CCDPA § 2(8) (defining "COVID-19 public health emergency"); PHEPA § 2(13) (same).

[323] *See* ENPA § 2(3)–(4) (applies in cases of exposure to individuals diagnosed with "an infectious disease").

[324] *Id.* § 2(4)(A).

[325] SDPCTA § 2(a).

[326] *Id.* § 2(c)(1).

[327] *Id.* § 2(c)(2).

[328] *Id.* § 2(c)(3).

Covered Data

Each bill would generally protect specific categories of data collected or used for contact tracing or exposure notification. The CCDPA would apply to the narrowest set of data: "precise geolocation data, proximity data, a persistent identifier, and personal health information."[329] In contrast, the ENPA would protect any information linked or reasonably linkable to any individual or device collected, processed, or transferred as part of an automated exposure notification service.[330] The CCDPA, PHEPA, and ENPA would exclude certain data, including aggregate data that cannot identify a specific individual. The CCDPA would also exclude data collected by a covered entity concerning anyone "permitted to enter a physical site of operation" of the entity, including employees, vendors, and visitors.[331]

Covered Entities

Each bill applies to entities that engage in contact tracing or exposure notification or that develop tools that other entities use for contact tracing or exposure notification. Under the CCDPA and ENPA, for example, a *covered entity* would include any entity or person engaged in a covered activity that is (1) subject to regulation by the Federal Trade Commission (FTC), (2) a common carrier as defined in the Communications Act of 1934, or (3) a nonprofit organization.[332] The CCDPA does not apply to *service providers* that transfer or process data on behalf of covered entities but do not themselves collect covered data.[333] The PHEPA would cover a broader range of entities, including government entities, but excluding health care providers, public health authorities, service providers, and persons acting in their individual or household capacity.[334] In contrast, the SDPCTA would apply only to public health authorities who receive CDC grants to develop digital contact-tracing tools.[335]

Covered Entities' Obligations

Each bill would impose obligations on covered entities with respect to covered data. Specifically, the CCDPA, PHEPA, ENPA, and, where noted, SDPCTA would require a covered entity to:

- Not *disclose* or *transfer* an individual's data for any purposes other than those enumerated in the bills (also a requirement under the SDPCTA);[336]

[329] CCDPA § 2(6). The CCDPA defines *persistent identifier* as "a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time," including "a customer number held in a cookie, a static Internet Protocol (IP) address, a processor or device serial number, or another unique device identifier." *Id.* § 2(13).

[330] ENPA § 2(6).

[331] CCDPA § 2(6)(b)(iv) (excluding "employee screening data"); *id.* § 2(10) (defining *employee screening data* as "covered data of an individual who is an employee, owner, director, officer, staff member, trainee, vendor, visitor, intern, volunteer, or contractor of the covered entity" that is used "for the purpose of determining, for purposes related to the COVID-19 public health emergency, whether the individual is permitted to enter a physical site of operation of the covered entity").

[332] *See* CCDPA § 2(7); ENPA §§ 2(11), 10(a)(4).

[333] CCDPA § 2(7)(C).

[334] PHEPA § 2(4).

[335] SDPCTA § 2(c).

[336] CCDPA § 3(a), (b); PHEPA § 3(a), (c); ENPA § 5; SDPCTA § 2(h).

- Publish a *privacy policy* to provide *notice* as to the type of data the entity collects, the purpose of the collection, how the entity will use collected data, and an individual's rights with respect to the data;[337]
- Obtain an individual's *affirmative express consent* before collecting that individual's data (also a requirement under the SDPCTA);[338]
- Provide an individual with the right to *opt out* of collection by withdrawing consent;[339]
- *Minimize* the amount of data collected to only that necessary for the service (also a requirement under the SDPCTA);[340]
- *Delete* an individual's data on request or after a set period, such as the end of the COVID-19 emergency under the PHEPA or SDPCTA or on a thirty-day rolling basis under the ENPA;[341] and
- *Safeguard* an individual's data by adopting appropriate data security measures (also a requirement under the SDPCTA).[342]

Along with these obligations, several additional protections are common to several of the bills. For example, both the CCDPA and PHEPA would require covered entities to provide a mechanism for an individual to *correct* inaccurate data.[343] Also of note, the PHEPA, ENPA, and SDPCTA would prohibit discrimination against an individual based on covered data.[344]

Enforcement

The CCDPA, PHEPA, and ENPA would vest the FTC with enforcement authority through agency and judicial proceedings.[345] The bills would also allow state attorneys general to enforce the bills' provisions in court.[346] The PHEPA would provide a new *private right of action* that would allow individuals to sue covered entities for violations.[347] And the ENPA would preserve an individual's ability to use existing remedies under federal or state law to enforce its provisions.[348] In contrast, the SDPTCA does not have an enforcement provision per se; instead, it would condition the award of CDC grants on compliance with its guidelines.[349]

[337] CCDPA § 3(c)(1); PHEPA § 3(e); ENPA § 4(b).

[338] CCDPA § 3(a); PHEPA § 3(d)(1); ENPA § 4(a); SDPCTA § 2(c)(1)(A).

[339] CCDPA § 3(d); PHEPA § 3(d)(2); ENPA § 4(a)(1)(B).

[340] CCDPA § 3(g); PHEPA § 3(a)(1); ENPA § 5(a)(1); SDPCTA § 2(c)(2).

[341] CCDPA § 3(e); PHEPA § 3(g); ENPA § 6; SDPCTA § 2(c)(3)(A).

[342] CCDPA § 3(h); PHEPA § 3(b); ENPA § 7; SDPCTA § 2(g).

[343] CCDPA § 3(f); PHEPA § 3(a)(2).

[344] PHEPA § 3(a)(3), (c)(2)–(3); ENPA § 8; SDPCTA § 2(c)(1)(B)–(C).

[345] CCDPA § 4(a); PHEPA § 6(a); ENPA § 10(a).

[346] CCDPA § 4(c); PHEPA § 6(b); ENPA § 10(b).

[347] PHEPA § 6(c).

[348] ENPA § 10(d).

[349] SDPCTA § 2(b).

Relationship to State Laws

Both the PHEPA and ENPA explicitly provide that their provisions would not preempt or supersede any state laws.[350] In contrast, the CCDPA would prohibit states from adopting or enforcing any laws or regulations governing the use of covered data.[351] The SDPCTA does not speak to its effect on state laws.

[350] PHEPA § 7; ENPA § 10(c).

[351] CCDPA § 6(b)(3).

Table 1. COVID-19 Data Privacy Bills: Comparison of Main Differences

Provision	CCDPA, S. 3663	PHEPA, S. 3749 and H.R. 6866	ENPA, S. 3861	SDPCTA, H.R. 7472
Covered Data—				
In general	*Covered data*: "precise geolocation data, proximity data, a persistent identifier, and personal health information" (§ 2(6)(a))	*Emergency health data*: "data linked or reasonably linkable to an individual or device, including [derived] data . . . that concerns the COVID-19 health emergency" (§ 2(8))	*Covered data*: "any information that is . . . linked or reasonably linkable to an individual . . . collected, processed, or transferred in connection with an automated exposure notification service" (§ 2(6))	*Contact-tracing data*: "information linked or reasonably linkable to a user or device" that "concerns the COVID-19 pandemic" and "is gathered, processed, or transferred by digital contact tracing technology" (§ 2(j)(2))
Exclusions	Aggregate data, business contact information, de-identified data, employee screening data, and publicly available information (§ 2(6)(b)); data related to individuals permitted to enter a covered entity's physical location (§ 2(12))	Data that is not "linked or reasonably linkable" to an individual or device (§ 2(8))	Data that is not "linked or reasonably linkable" to an individual or device, including aggregate data (§ 2(6))	N/A
Covered Entities—				
In General	Any entity or person engaged in contact tracing that is subject to the FTC Act, a common carrier, or a nonprofit (§ 2(7))	Any entity or person engaged in contact tracing, including government entities (§ 2(4)(A))	An operator of an automated exposure notification service that is subject to the FTC Act, a common carrier, or a nonprofit (§§ 2(11), 10(a)(4))	State, tribal, and territorial public health authorities who receive CDC grant funds to develop digital contact-tracing applications (§ 2(a)-(c))
Exclusions	Service providers (§ 2(7)(C))	Health care providers; persons engaged in de minimis collection; service providers; persons acting in their individual or household capacity; and public health authorities (§ 2(4)(B))	Public health authorities (§ 2(11))	N/A

Provision	CCDPA, S. 3663	PHEPA, S. 3749 and H.R. 6866	ENPA, S. 3861	SDPCTA, H.R. 7472
Non-Discrimination	No protections	Covered entities must adopt reasonable safeguards against discrimination (§ 3(a)(3)); government entities may not use data to interfere with voting rights (§ 4)	Prohibits discrimination by any person or entity based on covered data (§ 8)	Prohibits conditioning employment or government benefits on the use of digital contact-tracing applications (§ 2(c)(1)(B)-(C))
Enforcement	FTC; state attorneys general (§ 4(a), (c))	FTC; state attorneys general; new private right of action (§ 6)	FTC; state attorneys general; existing private rights of action (§ 10)	None per se; provides for revocation of CDC grant funds for non-compliance (§ 2(b)).
Preemption	Preempts state laws and regulations governing covered entities' use of covered data (§ 4(b)(3))	Adopts reasonable safeguards to prevent unlawful discrimination on the basis of emergency health data, but does not "preempt or supersede" other federal or state laws or regulations (§ 7)	Does not "preempt, displace, or supplant" state laws (§ 10(c))	N/A
Effective Period	Date of enactment through the last day of the COVID-19 public health emergency (§ 2(8))	Thirty days after enactment through the end of the COVID-19 public health emergency (§§ 2(13), 8)	Indefinitely, beginning on the date of enactment (§ 10(g))	N/A

Source: Created by CRS using information from CCDPA, S. 3663; PHEPA, S. 3749 and H.R. 6866; ENPA, S. 3861, and SDPCTA, H.R. 7472, as introduced.

Considerations for Congress

As state and local authorities implement digital contact-tracing apps to combat the COVID-19 pandemic,[352] Congress may consider whether to enact a law governing the use of contact-tracing data to ensure uniformity and safeguard individuals' personal data. If Congress takes no action, digital contact tracing may be subject to existing federal and state privacy protections, including HIPAA and the CCPA. But existing federal privacy laws do not protect all contact-tracing data,[353] and state laws—where they exist—impose a patchwork of requirements.[354] Moreover, depending on the type of information collected by an app, it may be subject to foreign and international laws in addition to domestic law.

No single federal law creates consistent, clearly applicable privacy protections for information that likely would be gathered and used in contact-tracing activities. In the context of digital contact tracing, state and local health departments conducting contact tracing and the app developers that assist them in that activity may not qualify as covered entities or business associates subject to HIPAA's requirements. Other federal laws, such as the FTC Act and Communications Act, may provide some privacy protections when HIPAA does not apply. Yet the reach of these laws is also limited. The FTC Act, for example, does not require entities to adopt particular privacy practices; it only takes enforcement action against corporate and private actors that it believes are engaged in unfair or deceptive conduct. Likewise, the Communications Act's CPNI protections are limited in scope and apply only to telephone carriers.

Pending legislation may offer a path forward. The CCDPA, PHEPA, and ENPA share a number of common provisions, suggesting some level of accord on how to regulate entities engaged in contact tracing. Two of the biggest divergences among the bills—whether to include a private right of action and whether to preempt state law—mirror differences in general data privacy bills introduced at the end of 2019 and earlier this year.[355] Those provisions were "key sticking point[s]" in the debate over generally-applicable data privacy legislation,[356] and Congress has yet to reach a consensus on these issues.

It also is not clear how much of an impact a law based on current legislative proposals would have on state-run digital contact-tracing apps. The CCDPA would apply only to private entities, and both the PHEPA and ENPA specifically would exclude public health authorities from their coverage (though the PHEPA would apply to other government entities).[357] And while the SDPCTA would cover apps developed by public health authorities, it would be limited to those authorities that receive CDC grant funds.[358]

---

[352] David Ingram, *Coronavirus Contact Tracing Apps Were Tech's Chance To Step Up. They Haven't.*, NBC NEWS (June 12, 2020, 7:49 AM), https://www.nbcnews.com/tech/tech-news/coronavirus-contact-tracing-apps-were-tech-s-chance-step-they-n1230211.

[353] Joy Pritts, *INSIGHT: Covid-19 Privacy Bills—Is There Room for Compromise?*, BLOOMBERG LAW (June 15, 2020, 4:01 AM), https://news.bloomberglaw.com/us-law-week/insight-55.

[354] *See* Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PROF'LS V(July 6, 2020), https://iapp.org/resources/article/state-comparison-table/.

[355] *See* Müge Fazlioglu, *Deja Vu? The Politics of Privacy Legislation During COVID-19*, INT'L ASS'N OF PRIV. PROF'LS (May 21, 2020), https://iapp.org/news/a/deja-vu-the-politics-of-privacy-legislation-during-covid-19/.

[356] Rebecca Kern & Daniel R. Stoller, *Bipartisan Privacy Talks Split With Second Senate GOP Bill (1)*, BLOOMBERG GOV'T (Mar. 12, 2020), https://about.bgov.com/news/bipartisan-privacy-talks-split-with-second-senate-gop-bill-1/.

[357] *See* CCDPA § 2(7); PHEPA § 2(4); ENPA § 2(11).

[358] SDPCTA § 2(a)-(c).

Should Congress choose to move forward with legislation regulating digital contact tracing, it may consider regulating public health authorities in addition to private entities. (For a discussion of whether Congress has the power to do so, see CRS Legal Sidebar LSB10502, *Constitutional Authority to Regulate the Privacy of State-Collected Contact-Tracing Data*, by Edward C. Liu.) Congress may also consider how other jurisdictions, such as Canada and the European Union, have interpreted their existing privacy laws with respect to digital contact tracing. Examining how those laws apply and where there are gaps in their coverage could potentially help Congress craft a law that reflects the unique challenges in regulating digital contact tracing.

Appendix A. Digital Contact Tracing Apps By State

As of September 24, 2020, the following states have either introduced or announced plans to introduce a digital contact tracing app.

In addition to these apps, Maryland, Nevada, Virginia, and the District of Columbia have all announced support for Exposure Notifications Express, a digital contact tracing solution that does not require a jurisdiction-specific app.

State	App Name	Technology Used	Status	Notes
Alabama	GuideSafe	Proximity	Released	
Arizona	Covid Watch Arizona	Proximity	Released	Available for University of Arizona students as part of phased rollout
Delaware	COVID Alert DE	Proximity	Released	
Nevada	COVID Trace	Proximity	Released	
New Jersey		Proximity	Announced	Pilot app currently being tested at college campuses and by state employees
North Dakota	Care19 Alert	Proximity	Released	
North Dakota	Care19 Diary	Location	Released	
Pennsylvania	COVID Alert PA	Proximity	Released	
Rhode Island	CRUSH COVID RI	Location	Released	
South Dakota	Care19 Diary	Location	Released	South Dakota and Wyoming use North Dakota's Care19 Diary app.
Wyoming	Care19 Alert	Proximity	Released	Wyoming uses North Dakota's Care19 Alert app.

Source: CRS review and analysis of available information.

Author Information

Jonathan M. Gaffney
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Eric N. Holmes
Legislative Attorney

Disclaimer