2021

Privacy in the Age of Contact Tracing: An Analysis of Contact Tracing Apps in Different Statutory and Disease Frameworks

Christopher S. Yoo
University of Pennsylvania Carey Law School

Apratim Vidyarthi
University of Pennsylvania

Author ORCID Identifier:

Christopher S. Yoo 0000-0003-2980-9420

ARTICLE

PRIVACY IN THE AGE OF CONTACT TRACING: AN ANALYSIS OF CONTACT TRACING APPS IN DIFFERENT STATUTORY AND DISEASE FRAMEWORKS

CHRISTOPHER S. YOO* AND APRATIM VIDYARTHI†

The Covid-19 pandemic is a historic pandemic that has affected the lives of virtually everyone on the globe. One approach to slowing the spread of the disease is to use contact tracing, facilitated by our internet-connected smartphones. Different nations and states have partnered to develop a variety of contact tracing apps that use different technologies and architectures.

This paper investigates how five contact tracing apps—Germany's Corona-Warn-App, Israel's HaMagen, North Dakota's Care19 Diary and Alert apps, and India's Aarogya Setu—fare in privacy-oriented statutory frameworks to understand the design choices and public health implications shaped by these statutes. The three statutes—the Health Insurance Portability and Accountability Act, the California Consumer Privacy Act, and the European Union's General Data Protection Regulation—provide different incentives to app developers across eight categories of design choices: notice and consent, consent requirements for medical data disclosed to third parties, location identifying technologies, data profiles and data collection, minimizing data categories collected, data sale and sharing with non-research third parties, third party and researcher access to data, and affirmative user rights. Each framework balances incentives to app developers with the need for governments to cater to pressing emergencies like public health needs. Some of the incentives in each framework end up favoring less privacy-protective design choices, whereas other provisions make it harder for public health authorities to flexibly respond to crises.

Finally, this paper investigates how these frameworks would fare with different disease variables, by applying the analysis above to three different diseases that could require contact tracing: SARS, Ebola, and HIV. Our

* John H. Chestnut Professor of Law, Communication, and Computer & Information Science and Founding Director of the Center for Technology, Innovation & Competition, University of Pennsylvania.

† Member of the J.D. Class of 2022, University of Pennsylvania Carey Law School.

conclusion is that the disease variables themselves will affect whether the balance tilts towards public health or privacy, and that the statutes give varying levels of flexibility to cater to more pressing emergencies.

INTRODUCTION

As of March 2021, the COVID-19 pandemic had claimed the lives of more than two million people, and infected more than one hundred million, making it a deadly, once-in-a-lifetime crisis.[1] The novel, interconnected nature of the contemporary global economy accelerated the transmission of an already infectious disease and exacerbated attempts to contain the contagion. Yet the expansive and advanced nature of the modern economy also ubiquitously features smartphones, the Internet, and data collection, which enhanced the effectiveness of an important tool for technologists and public health agencies to slow the spread of the pandemic: digital contact tracing.

The idea of contact tracing is not novel. Plague crosses, which were placed on buildings occupied by the victims of plague, served as a rudimentary mechanism for minimizing the risk of contagion in the seventeenth and eighteenth centuries.[2] During the AIDS crisis in the 1980s, public health officials debated the balance between contact tracing and discrimination against the LGBTQ community.[3] The trend continues in our latest health crisis, with digital contact tracing apps using the mobility and accessibility of Internet-connected smartphones to track and slow the spread of COVID-19.

But this latest iteration of contact tracing also raises concerns about data privacy inherent to all Internet-connected apps and devices. To fulfill their purpose of tracing the spread of a disease, contact tracing apps necessarily must collect some type of location and test result data and upload them to the Internet. Both location and test result data can be considered intimate and private, revealing the granular details of where users travel, with whom they associate, and what potential locations might have caused them to test positive. If an app is to collect such data, what design decisions help protect against the misuse of this data and mitigate concerns of surveillance? Do existing privacy regimes provide adequate guidance to guide developers as they balance the importance of protecting privacy against the need to perform critical public health functions through technology? Do such statutes provide

---

[1] World Health Org., *WHO Coronavirus (COVID-19) Dashboard*, https://covid19.who.int/ (last visited Mar. 9, 2021). We use the March figures for consistency across the other figures used in this paper.

[2] *See* FRANK M. SNOWDEN, EPIDEMICS AND SOCIETY 77 (2019) ("Searchers then marked the houses of plague victims with a cross daubed in red, sealed the premises, and posted a guard outside to thwart any attempt to enter or exit the sick house."). For a visual take, see MONTY PYTHON AND THE HOLY GRAIL (Python (Monty) Pictures 1975).

[3] NAT'L RSCH. COUNCIL, THE SOCIAL IMPACT OF AIDS IN THE UNITED STATES 30-34 (Albert R. Jonsen & Jeff Stryker eds., 1993).

adequate flexibility in addressing the changing needs of particular public health crises? And how do we balance the public health needs of preventing the spread of a deadly disease against individuals' privacy rights and expectations?

In this paper, we attempt to answer these pressing questions by using three leading privacy regimes—the Health Insurance Portability and Accountability Act (HIPAA), the California Consumer Privacy Act (CCPA), and the European Union's General Data Protection Regulation (GDPR)—as benchmarks for understanding what types of design choices they encourage for the developers of contact tracing apps. We measure the performance of five COVID-19 contact tracing apps from across the globe against the standards across eight design categories set forth in these three regulatory schemes. We then look at what these regimes cover and what they miss, and how they would fare in public health crises with different disease variables.

In Part I, we describe the statutory regimes and the apps we assess: Germany's Corona-Warn-App, Israel's HaMagen, North Dakota's Care-19 Diary and Alert apps, and India's Aarogya Setu app. In Part II, we look at eight factors in the statutes that implicate design decisions of each of these apps: notice and consent, consent requirements for disclosing medical data to third parties, location identifying technologies, data profiles and data collection, minimizing data categories collected, data sale and sharing with non-research third parties, access to data for research, and affirmative user rights. We assess how each of the apps measures up against the HIPAA, CCPA, and GDPR benchmarks in each of these eight categories. In Part III, we look at how disease variables affect some of these common factors assessed and analyze whether the statutes provide adequate flexibility to balance different public health concerns of three other diseases—SARS, Ebola, and HIV—against privacy.

Ultimately, we conclude that the three privacy regimes encourage app developers to make design choices that favor privacy while simultaneously allowing these apps to succeed at contact tracing. The statutes also provide some flexibility to accommodate public health concerns, often at the expense of individual privacy, under appropriate circumstances. Nonetheless, there are some aspects of privacy, like dignitary concerns, that are not captured by these statutes and that require a more complex framework to address.

I. BACKGROUND

A. *Regimes Analyzed*

We use three regulatory regimes from the U.S. and the EU as representative approaches to privacy. The first is the implementation of the privacy provisions of the federal Health Insurance Portability and Accountability Act (HIPAA).[4] The second is the California Consumer Protection Act (CCPA), which governs privacy and data issues for firms operating in, or interacting with, consumers in California.[5] The third is the General Data Protection Regulation (GDPR), which governs uses of data in the European Union. Taken together, these three regimes represent significantly different approaches that help understand how privacy regulations affect design decisions surrounding contact tracing apps. These regimes' different geographic and subject matter scope make it unlikely that all three fully apply to any of the apps we are studying. Even if not directly applicable, they provide useful benchmarks for assessing whether the apps we are studying protect privacy and how privacy regulations affect design decisions.

---

[4] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033, *reprinted in* 42 U.S.C. § 1320d-2 note; *see also* Dixie B. Baker, Jane Kaye & Sharon F. Terry, *Privacy, Fairness, and Respect for Individuals*, 4 eGEMs 8 (2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4827784/pdf/egems1207.pdf ("FIPPs included in the HHS guidance . . . have been implemented in the HIPAA Privacy Rule . . . .").

[5] In 2020, California passed California Proposition 24, known as the California Privacy Rights Act (CPRA), which is an amendment to the CCPA. Cameron F. Kerry & Caitlin Chin, *By passing Proposition 24, California voters up the ante on federal privacy law*, BROOKINGS (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/#cancel. The CPRA expands upon the scope of the CCPA, creating a privacy protection agency, governing both the sale and sharing of data (the latter of which was not addressed by the CCPA), and further limiting the use of sensitive personal information by businesses. *See generally* Cal. Sec'y State, *Proposition 24*, https://voterguide.sos.ca.gov/propositions/24/ (last visited Mar. 11, 2021). This paper does not use the CPRA as a benchmark. First, the law passed after we began writing this paper, and there is inadequate analysis about the legal, technological, and business implications of the act. Second, the CCPA's approach provides a better juxtaposition to the GDPR's. Finally, the CPRA's provisions do not come into effect until as far as 2023. *See* Cal. Sec'y State, *Text of Proposed Law: Proposition 24*, at 44, 70 https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf (last visited Mar. 11, 2021) (explaining how the act exempts some provisions for employee and business to business communications until January 1, 2023, and enforcement shall not begin until July 1, 2023).

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA called upon the Secretary of Health and Human Services to develop national standards for privacy in electronic health care records.[6] The standards applied the Fair Information Practice Principles (FIPPs) of notice, choice, access, and security developed in 1973[7] and included in the Privacy Act of 1974's statement of purpose[8] to Protected Health Information (PHI). One of the key design issues presented by HIPAA is whether the app or any recipient of the PHI is a covered entity. Covered entities are defined as health plans, healthcare clearinghouses, and healthcare providers that electronically transmit health information, and the business associates of covered entities to whom such information is sent.[9] Large, multifunction institutions may limit the application of HIPAA by declaring themselves to be hybrid entities and by identifying which components are health care components subject to HIPAA and which components are not.[10] For covered entities and their business associates, HIPAA's privacy rules govern the disclosure of PHI in treatment, payment, and operations.[11] Notably, HIPAA does not restrict the use or disclosure of PHI that has been properly deidentified,[12] such as by removing eighteen types of identifiers including names, locations, dates, device identifiers, and Internet Protocol addresses.[13]

To provide guidance regarding the application of HIPAA during COVID-19, the Department of Health and Human Services (HHS) released a notice in February of 2020,[14] which it followed up with a formal waiver exercising the statutory authority to waive enforcement of five designated provisions to provide greater flexibility in providing care to COVID-19 patients.[15] HHS's

---

[6] 45 C.F.R. § 164 (1996).
[7] *Id.*
[8] Pub. L. No. 93-579, § 2(b), 88 Stat 1896, 1896, *reprinted in* 5 U.S.C. § 552a note.
[9] 45 C.F.R. § 160.102(a) (1996). Healthcare clearinghouses are public or private entities that either process or facilitate the processing of health information; or does so by receiving transactions from a third-party entity. *Id.* § 160.103.
[10] *Id.* § 164.105(a).
[11] *Id.* § 164.104.
[12] *Id.* § 164.502(d).
[13] *Id.* § 164.514(b)(2)(i).
[14] U.S. Dep't of Health & Hum. Servs. Off. for Civ. Rts., *Bulletin: HIPAA Privacy and Novel Coronavirus* (Feb. 2020), https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf.
[15] U.S. Dep't of Health & Hum. Servs., *Waiver or Modification of Requirements Under Section 1135 of the Social Security Act* (Mar. 13, 2020), https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx.

Office of Civil Rights later issued administrative waivers governing telehealth, business associates, and community-based testing sites.[16]

2. California Consumer Protection Act (CCPA)

In 2018, California enacted the California Consumer Privacy Act (CCPA) to implement the California Constitution's right of privacy.[17] The Act is intended to give people the right to know what personal information is being collected about them, to know to whom that personal information has been sold or disclosed, to block the sale of their personal data, to access their personal information, and not to be penalized for exercising their privacy rights.[18] Despite this breadth, the statute does not apply to aggregated or deidentified information.[19] The statute applies only to entities that meet certain size thresholds and do business in California,[20] though in practice because many technology companies reside in California and because data may flow through such companies, the Act has wide applicability across the nation. Unlike HIPAA, CCPA does not provide for waivers during public health emergencies, and the California Attorney General responded to industry calls for delaying enforcement of the statute until January 2021 by emphasizing the importance of adhering to the statute during the COVID-19 pandemic[21] amid media reports that his office intended to begin enforcing it on July 1, 2020.[22]

---

[16] Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, 85 Fed. Reg. 22,024 (Mar. 17, 2020) (to be codified at 45 C.F.R. pts. 160, 164); Enforcement Discretion Under HIPAA To Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19, 85 Fed. Reg. 19,392 (Apr. 7, 2020) (to be codified at 45 C.F.R. pts. 160, 164); Enforcement Discretion Regarding COVID–19 Community-Based Testing Sites (CBTS) During the COVID–19 Nationwide Public Health Emergency, 85 Fed. Reg. 29,637 (Apr. 9, 2020) (to be codified at 45 C.F.R. pts. 160, 164).

[17] California Consumer Privacy Act, ch. 55, 2018 Cal. Stat. 1809 (codified as amended at CAL. CIV. CODE § 1798 (2020)).

[18] *Id.* § 1798.110.

[19] *Id.* § 1798.145(a)(5).

[20] *Id.* § 1798.140(d)(1) (2020).

[21] Press Release, Off. Att'y Gen., State of Cal. Dep't of Just., Attorney General Becerra Reminds Consumers of their Data Privacy Rights During the COVID-19 Public Health Emergency (Apr. 10, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-reminds-consumers-their-data-privacy-rights-during.

[22] *See, e.g.*, Marty Swant, *Citing COVID-19, Trade Groups Ask California's Attorney General To Delay Data Privacy Enforcement*, FORBES (Mar. 19, 2020, 3:13 PM EDT), https://www.forbes.com/sites/martyswant/2020/03/19/citing-covid-19-trade-groups-ask-californias-attorney-general-to-delay-data-privacy-enforcement/?sh=227783085c30

3. General Data Protection Regulation (GDPR)

In 2016, the European Union adopted GDPR to govern data collection, use, and sharing in the EU.[23] GDPR applies where data are processed through automated means and where structured sets of personal data are accessed by entities within the EU, or by entities accessing the data of subjects located in the EU.[24] It thus necessarily covers any Internet-based application that collects and processes data, including contact tracing apps.[25] However, not all data are covered by the GDPR: pseudonymization is one of the considerations that may authorize processing of personal data for a purpose other than that for which the personal data was collected without consent.[26] The statute also authorizes states to enact legislation to collect location data in ways that deviate from GDPR where necessary to safeguard public security, so long as it is an appropriate and proportionate measure for a democratic society and complies with applicable protections for fundamental and human rights.[27]

Like HIPAA, the European Data Protection Board has issued guidelines regarding the application of GDPR to location data and contact tracing apps.[28] The guidelines provide a synthesis of data collection and processing rules, but indicate general adherence to the GDPR's original clauses. They emphasize data minimization, data protection, anonymization, and purpose limitation.[29] The guidelines also recommend the voluntary use of contact tracing apps, rather policies that mandate the use of such apps, and recommend the use of "proximity information" (such as Bluetooth, *infra*) instead of the tracking of "individual movements."[30]

(reporting the government's intention to enforce the CCPA starting July 1 despite the COVID-19 pandemic).

[23] Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

[24] *Id.* arts. 2(1), 3, 4(2), (6).

[25] *Id.* arts. 2(1), 4(2), (6).

[26] *Id.* art. 6(4)(e).

[27] *Id.* art. 23(1)(e); *see also Statement on the processing of personal data in the context of the COVID-19 outbreak*, EUR. DATA PROT. BD § 1.3 (Mar. 19, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf ("Such exceptional legislation is only possible if it constitutes a necessary, appropriate, and proportionate measure within a democratic society.").

[28] *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,* EUR. DATA PROT. BD. § 1 (Apr. 21, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[29] *Id*. § 2.2.

[30] *Id*. § 1(8).

B. *Applications Analyzed*

We analyze five contact tracing apps against the three regulatory frameworks to see how they shape the privacy-related design decisions for these apps: Germany's Corona-Warn-App, Israel's HaMagen, North Dakota's Care19 Diary and Alert apps, and India's Aarogya Setu. These apps employ different geolocation technologies (Bluetooth versus Global Positioning System(GPS)/Cell Site Location Information (CSLI) data);[31] collect different types of data and store them in different ways, employ different application architectures, rely on different means to incorporate test results, and enjoy different levels of adoption in their respective jurisdictions.

[31] We note here that we use GPS and CSLI interchangeably. While there are differences as to the underlying computational mechanisms, some of the app developers use these terms interchangeably, and they implicate similar privacy concerns in comparison to Bluetooth. *See, e.g.*, Bhairav Acharya, Richa Goyal & Jaideep Reddy, *Cell Phone Location Tracking*, BERKELEY LAW, https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf (last visited Mar. 11, 2021) (describing the differences between the two methods, but then using the same legal analysis across both).

Table 1: App Summary

	Corona-Warn-App	**HaMagen**	**Care-19 Diary**	**Care-19 Alert**	**Aarogya Setu**
Country	Germany	Israel	U.S./North Dakota	U.S./North Dakota	India
Technology	Bluetooth	GPS/CSLI + Optional Bluetooth	GPS/CSLI	Bluetooth	GPS/CSLI + Bluetooth
Data Storage	Phone	Phone/ upload to government servers with consent	Phone/ upload to developers with consent	Phone/ upload to developers with consent	Upload to government database
Data Collected	Bluetooth	Location + Bluetooth	Location	Bluetooth	Name, phone number, health details, occupation, location, and Bluetooth
Developer	German Government/ Robert Koch Institute	Israeli Government/ GlobeKeeper	North Dakota/ ProudCrowd	North Dakota/ ProudCrowd	Indian Government
Test Reporting	QR codes/labs	Cross reference with government database	Outreach before use by state government	Outreach before use by state government	Self + cross reference with government database
Policy	Opt-in	Opt-in	Opt-in	Opt-in	Mandated
Penetration	25%	17%	Unclear	Unclear	12%

1. Germany: Corona-Warn-App

Germany's Corona-Warn-App is a decentralized contact tracing app developed by the Robert Koch Institute (RKI) in cooperation with the German government. It uses Bluetooth and the Apple/Google Exposure Notification System (ENS) to transmit random identification numbers that

are changed every ten to twenty minutes to other phones using the app.[32] If the app detects another user running the app within 1.5 meters of the current user for at least ten minutes, it records the day, time, and duration of the contact as well as the strength of the Bluetooth signal.[33] To report test results, users can use a QR code they receive from the testing facility to upload their test result to the app.[34] Users who test positive can send to the competent health authorities all of the pairwise location data over the preceding two weeks, combined with their test results. The health authorities then pass the information on to the transnational warning system.[35] The transnational warning system uses that information to generate lists of anonymous identifiers associated with positive tests along with an assessment of transmission risk and sends those lists to all app users.[36] The app then matches the identifiers in the list of infected people with those to which it has been in close proximity and calculates the risk that the user has been infected based on the date of contact and the signal strength.[37] The app collects consent only for usage of the app, for uploading their test results, and for the upload of Bluetooth pairwise data if the user tests positive, meaning it does not collect a broad data profile of the user.[38] Usage of the app is voluntary.[39] As of April 2021, the app had been downloaded 26.7 million times.[40]

2. Israel: HaMagen

Israel's HaMagen app is an open-source centralized contact tracing app created by the Israeli government in collaboration with Tel Aviv-based

---

[32] *Frequently Asked Questions about the Corona-Warn-App*, CORONA-WARN-APP OPEN SOURCE PROJECT, https://www.coronawarn.app/en/faq/ (last visited Oct. 2, 2020) [hereinafter *Corona-Warn-App FAQs*].

[33] *Id.*

[34] *Privacy Notice*, CORONA-WARN-APP OPEN SOURCE PROJECT § 6(b), https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf (last amended Dec. 15, 2021) [hereinafter *Corona-Warn-App Privacy Notice*].

[35] *Id.* § 6(c).

[36] *Id.* §§ 7, 10.

[37] *Id.* § 6(a); Svea Windwehr & Jillian C. York, *Germany's Corona-Warn-App: Frequently Asked Questions*, ELEC. FRONTIER FOUND. (June 17, 2020), https://www.eff.org/deeplinks/2020/06/germanys-corona-warn-app-frequently-asked-questions.

[38] *See Corona-Warn-App Privacy Notice*, *supra* note 34, § 5(a) ("[The] access data is processed to maintain and secure the technical operation of the app and the server system. You will not be identified personally as a user of the app and no user profile will be created.").

[39] *See* Windwehr & York, *supra* note 37.

[40] *Übersicht zu aktuellen und früherer Zahlen und Fakten zur Corona-Warn-App* [Overview of Current and Previous Facts and Figures About the Corona-Warn-App], ROBERT KOCH INSTITUT, https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/WarnApp_KennzahlenTab.html (last visited Apr. 3, 2021).

GlobeKeeper. Instead of relying on the Google/Apple ENS, HaMagen uses GPS, Wi-Fi, and Bluetooth data to track users' movements and store two weeks of location information on their devices.[41] In addition, once an hour, the app downloads an anonymized list of locations where the Ministry of Health has verified that COVID-19 patients have visited.[42] The app then cross references the users' locations history against the list without their location data ever leaving the device and notifies the user if they have been in close proximity with someone who has tested positive for COVID-19.[43] The app collects consent for usage of the app and for the collection of location and Bluetooth data. Users identified as verified COVID-19 patients may agree to have their location data transferred to the Ministry, where they will be examined within the framework of the epidemiological investigation and published without any identifying details, in order to alert the public about locations where infected people have been.[44] Media reports from November 2020 report that the app had been downloaded 2.5 million times, although technical problems and lack of confidence in the government's response to the pandemic caused usage to drop off substantially.[45] The terms of use specify that users shall have no claims for privacy violations as a result of using the app.[46]

3. North Dakota: Care19 Diary and Alert

The State of North Dakota, in conjunction with local tech company ProudCrowd, has developed two apps to support COVID-19 contact tracing. Care19 Diary helps users log their whereabouts, whereas Care19 Alert tracks a user's proximity to other users.[47] Originally deployed only in North Dakota, it is now also available in South Dakota and Wyoming.

---

[41] *Privacy & Pandemics: The Role of Mobile Apps (Chart)*, FUTURE OF PRIV. F. (Apr. 2020), https://fpf.org/wp-content/uploads/2020/04/Privacy-Pandemics-The-Role-of-Mobile-Apps.pdf [hereinafter *Privacy & Pandemics*]; *Privacy Policy and Information Security*, MINISTRY OF HEALTH § 2 (Mar. 21, 2020), https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/ [hereinafter *HaMagen Privacy Policy*].

[42] *HaMagen Privacy Policy*, *supra* note 41, § 2.

[43] *Id*. §§ 2-4.

[44] *Id*. § 8.

[45] Josh Mitnick, *How Israel's COVID contract tracing app rollout went wildly astray*, CIO (Nov. 2, 2020, 6:00 PM PST), https://www.cio.com/article/3591570/how-israels-hamagen-contact-tracing-app-rollout-went-wildly-astray.html.

[46] *Terms of Use*, HAMAGEN (July 27, 2020, 10:29 AM), https://govextra.gov.il/ministry-of-health/hamagen-app/terms-and-conditions-of-use-en/ [hereinafter *HaMagen Terms of Use*].

[47] *Care19*, N.D. STATE GOV'T, https://ndresponse.gov/covid-19-resources/care19 (last visited Nov. 14, 2020) [hereinafter *Care19 Webpage*].

The Care19 Diary app is a location logger that uses GPS-based technology developed by Apple and Google[48] to track and store two weeks of information[49] about locations that the user has visited for ten or more minutes.[50] The location data are stored anonymously on servers maintained by ProudCrowd and may be accessed temporarily by third parties for specific processing tasks, but is otherwise accessible only by the user.[51] For example, the app used to share data with Foursquare to convert longitude and latitude data into recognizable place names.[52] The app may also use the data to calculate a personal risk score and to create a map of app users' locations that will be shared only on an aggregated basis.[53] The state's Department of Health asks users who test positive for COVID-19 for consent to provide their location information to the Department using a random identifier so that the state government can contact trace and forecast the movement of the virus.[54] No profile is needed to use the app's services, though consent is required for data logging.[55] Usage of the app is voluntary. It has been criticized for inaccuracy[56] and for initially sharing individual codes and failing to disclose the sharing of personal identifiers with third parties.[57]

The Care19 Alert app is an exposure notification app launched in August 2020 based on the Google/Apple ENS.[58] It uses Bluetooth to check whether a user is near any other users every fifteen minutes using the ENS, and stores that information for up to two weeks, identified only through random tokens.[59] App users who test positive for COVID-19 have the option of pushing the "Notify Others" button, which transmits the pairs of keys that

---

[48] *Burgum: ND to launch second contract tracing app using technology developed by Apple and Google*, N.D (May 20, 2020, 6:39 PM), https://www.health.nd.gov/news/burgum-nd-launch-second-contact-tracing-app-using-technology-developed-apple-and-google.

[49] *Privacy Policy – Care19 Diary*, CARE19, https://care19.app/diary/privacy (last visited Nov. 24, 2020) [hereinafter *Care19 Diary Privacy Policy*].

[50] *Care19 Webpage*, *supra* note 47.

[51] *Care19 Diary Privacy Policy*, *supra* note 49.

[52] *Id.*; Geoffrey A. Fowler, *One of the first contact-tracing apps violates its own privacy policy*, WASH. POST (May 21, 2020) https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/.

[53] *Care19 Diary Privacy Policy*, *supra* note 49.

[54] *Id*.

[55] *Care19 Diary Application*, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.proudcrowd.care&hl=en_US&gl=US (last visited Nov. 14, 2020) [hereinafter *Care19 Diary App*].

[56] Jack Morse, *North Dakota launched a contact-tracing app. It's not going well.*, MASHABLE (May 26, 2020), https://mashable.com/article/north-dakota-contact-tracing-app/.

[57] Fowler, *supra* note 52.

[58] *Care19 Webpage*, *supra* note 47.

[59] *See Privacy*, CARE19, https://www.care19.app/alert/privacy (last visited Apr. 3, 2021) [hereinafter *Care19 Alert Privacy Policy*].

have been close proximity to one another to the National Key Server operated by the Association of Public Health Laboratories.[60] The National Key Server periodically pushes out lists of the keys associated with people with positive test results so that the app can determine whether a user is likely to have been exposed.[61] No profile is needed to use app services, though consent is required for data logging.[62] Data are stored on the app.[63] The app does share usage data needed for diagnostics with tools created by Google Firebase and Bugfender.[64] The Department regularly reports aggregate number of exposures and users.[65] Usage of the app is voluntary.

4. India: Aarogya Setu

India's Aarogya Setu is an open-source[66] app developed by the Indian Ministry of Electronics and Information Technology.[67] To register for the app, users must create an account and provide their phone number, age, gender, profession, travel history, and whether the user is a smoker, which is saved on a government server using a unique digital identifier (DiD).[68] The government uses this information to create anonymized, aggregated datasets for COVID-19 management to communicate to users the probability that they

---

[60] *Id.*; *Care19 Alert Application*, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.proudcrowd.exposure&hl=en_US&gl=US (last visited Nov. 14, 2020) [hereinafter *Care19 Alert App*]; *North Dakota announces launch of Care19 Alert app to help reduce spread of COVID-19 as students return*, N.D. (Aug. 13, 2020, 12:55 PM), https://www.health.nd.gov/news/north-dakota-announces-launch-care19-alert-app-help-reduce-spread-covid-19-students-return.

[61] *Care19 Alert App*, *supra* note 60; *Care19 Alert Privacy Policy*, *supra* note 59; *Care19 Webpage*, *supra* note 47.

[62] *Care19 Alert App*, *supra* note 60; *Care19 Alert Privacy Policy*, *supra* note 59.

[63] *Care19 Alert App*, *supra* note 60; *Care19 Alert Privacy Policy*, *supra* note 59.

[64] *Care19 Alert Privacy Policy*, *supra* note 59.

[65] *Id.*

[66] *See, e.g.*, Ishan Patra, *Aarogya Setu app is now open source: what does it mean?*, THE HINDU (May 27, 2020), https://www.thehindu.com/sci-tech/technology/aarogya-setu-app-is-now-open-source-what-does-it-mean/article31689459.ece (noting that the app has finally become open source). *But see Four months on, Aarogya Setu is still not open-source. WHY and WHEN is what the nation really wants to know!,* INTERNET FREEDOM FOUND. (Aug. 19, 2020), https://internetfreedom.in/aarogya-setu-should-be-open-source-now/ (noting that source code releases are slow, source code releases do not match the actual app, and such releases are missing server-side code and cloud deployment functions).

[67] Andrew Clarance, *Aarogya Setu: Why India's Covid-19 contact tracing app is controversial*, BBC (May 14, 2020), https://www.bbc.com/news/world-asia-india-52659520.

[68] *Aarogya Setu Application*, AAROGYA SETU, https://aarogyasetu.gov.in/ (last visited Nov. 14, 2020) (see sign up pane on app) [hereinafter *Aarogya Setu App*]; *Privacy Policy*, § 1(a), SWAREKSHA.GOV, https://web.swaraksha.gov.in/ncv19/privacy/ (last visited Nov. 24, 2020) [hereinafter *Aarogya Setu Privacy Policy*].

may have been infected with COVID-19, and to provide medical personnel information needed to carry out interventions.[69] The app uses both Bluetooth and GPS data to exchange identifiers and to record the time and location when an individual is within range of another app user, storing this information on the user's device.[70] The app also collects and locally stores users' location data every fifteen minutes.[71] The app gives users the option of taking self-assessment tests that ask about symptoms, underlying conditions, recent travel, and conduct likely to have resulted in exposure,[72] storing that information with the user's location data.[73] If a user tests positive or has a self-assessment test that indicates possible infection, the app will upload their location and proximity data to the server.[74] The government uses that data to identify areas where outbreaks are likely to occur and are likely to need more testing and treatment resources.[75] The government also notifies other users with whom the person who has tested positive has come into close contact.[76] Downloading the app is mandatory for citizens living in COVID-19 containment zones as well as for all working employees in both the private and public sectors.[77] As of November 14, 2020, the app was being used by more than 162 million users.[78] Although the source code was not initially available and the terms of service initially penalized reverse engineering and disclaimed all liability, the government has attempted to address those concerns.[79]

II. ASSESSMENT OF PRIVACY AND DESIGN FACTORS

We look at eight common factors across HIPAA, CCPA, and GDPR that influence the design of our five apps: notice and consent, consent for medical

[69] *Aarogya Setu Privacy Policy*, *supra* note 68, § 2(a).
[70] *Id.* § 1(b).
[71] *Id*. § 1(d).
[72] *Aarogya Setu App: Follow these simple steps to do a self-assessment*, INDIA TODAY (May 2, 2020, 15:41 IST), https://www.indiatoday.in/information/story/aarogya-setu-app-follow-these-simple-steps-to-do-a-self-assessment-test-1673656-2020-05-02.
[73] *Aarogya Setu Privacy Policy*, *supra* note 68, §§ 1(a)-(b), 2(d).
[74] *Id.* § 1(d).
[75] *Id.*
[76] *Terms of Service*, AAROGYA SETU (Nov. 12, 2020, 12:33 PM), https://www.aarogyasetu.gov.in/terms-conditions/.
[77] Clarence, *supra* note 67.
[78] *Aarogya Setu App, supra* note 68.
[79] *See* Arshad R. Zargar, *Privacy, security concerns as India forces virus-tracing app on millions*, CBS NEWS (May 27, 2020, 5:32 AM), https://www.cbsnews.com/news/coronavirus-india-contact-tracing-app-privacy-data-security-concerns-aarogya-setu-forced-on-millions/ (on source code); *Our analysis of Aarogya Setu's Updated Privacy Policy and Terms of Service*, SFLC.IN (May 26, 2020, 13:52), https://sflc.in/our-analysis-aarogya-setus-updated-privacy-policy-and-terms-service (on reverse engineering and liability).

data, location identifying technologies, data profiling and collection, minimization of data categories collected, data sale and sharing with non-research third parties, access to data for research, and affirmative user rights.

A. *Notice and Consent*

Notice and consent is a bedrock principle of privacy that informs data subjects about the kind of data the app would like to collect and asks them for consent to collect that data. A privacy notice is a document or language that defines how an organization, software, or application collects, processes, and transmits user data, and what data protection principles are applied.[80] Consent requires providing consumers with adequate information and the choice to agree to have their data be used in a specified manner, or otherwise not use the service or application.[81]

As an initial matter, HIPAA applies only to covered entities, which do not include apps and which data repositories can easily avoid being categorized as by complying with requirements to constitute a hybrid entity. Where HIPAA applies, it generally requires health providers or businesses performing certain functions on their behalf to obtain user consent before disclosing PHI to third parties.[82] HIPAA's consent requirement thus applies to disclosure of PHI shared by health providers but not to self-reported PHI (which is created on the app and not by the health provider). If a contact tracing app requires validation from a health provider, then HIPAA requires user consent before the app shares any PHI.[83]

In contrast to HIPAA's focus on PHI, the CCPA's consent requirements govern the collection of a broad range of personal information and not just health-related data.[84] CCPA requires apps to provide notice at or before the point of data collection.[85] The notice must include the purposes for which the information is being collected.[86] Relatedly, for-profit businesses must disclose the use, collection, and disclosure of personal information or

---

[80] *See, e.g.*, *Writing a GDPR-compliant privacy notice*, GDPR, https://gdpr.eu/privacy-notice/ (last visited Oct. 14, 2020) (defining privacy notices); FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (specifying factors that are necessary to satisfy adequate notice).
[81] *Id.* at 9.
[82] 45 C.F.R. § 164.508 (2013).
[83] Laura Bradford, Mateo Aboy, & Kathleen Liddell, *COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes*, 7 J.L. & BIOSCIENCES 1, 9 (2020).
[84] CAL. CIV. CODE § 1798.135 (2020).
[85] *Id.* § 1798.135.
[86] *Id.* § 1798.100(b).

personally identifiable information (PII).[87] IP addresses and location data are considered types of covered personal information[88] and thus are subject to the disclosure requirements. For contact tracing apps, this means that users must provide one-time consent for the app to collect geolocation data and IP addresses.

GDPR's consent requirements are stronger than CCPA's. Every controller—the entity that determines the purposes and means of processing personal data[89]—must have a lawful basis for processing of personal data.[90] In the case of contact tracing, this is most likely through user consent, though where carrying out a task is necessary for the public interest or in the exercise of official authority, no such consent is needed.[91] Consent must be for processing of personal data that is "necessary for the performance of that contract,"[92] and consent must be explicit, informed, and presented to the user in clear language.[93] The consent notice must provide information about the categories of personal data being processed, the purposes of processing, and the existence of data subjects' rights.[94] Users must also be allowed to withdraw their consent in a manner as easy as the mechanism for giving consent.[95] Finally, if consent is given to a public authority, that consent is not considered freely given.[96]

The German Corona-Warn-App easily fulfills the notice and consent standards of all three regimes. As a preliminary matter, because the German App is not a health plan, health care clearinghouse, or a health care provider, it is not a covered entity and is thus not subject to HIPAA. If the German authorities receiving the data perform any functions that render them a covered entity, they can avoid HIPAA's coverage by making the declarations needed to become a hybrid entity. If HIPAA were to apply, it would govern the sharing of certain PHI, including COVID test results, risk levels, and information about the onset of symptoms.[97] The fact that the app obtains consent before performing these functions and stores the data in an

[87] *Id.* §§ 1798.100(b), 1798.140(c).
[88] *Id.* § 1798.140(o)(1)(A).
[89] GDPR, *supra* note 23, art. 4(7).
[90] *Id.* art. 6(1)(a), (e).
[91] *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, EUR. DATA PROT. BD. § 4 (Apr. 21, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.
[92] GDPR, *supra* note 23, art. 7(4).
[93] *Id*. art. 7(1)-(2).
[94] *Id*. art. 13(1).
[95] *Id.* arts. 7(4) & 13(2)(c).
[96] *Id.* recital 43.
[97] *Corona-Warn-App Privacy Notice*, *supra* note 34, §§ 5(e), 6(b).

aggregated and anonymous manner satisfies the HIPAA standard.[98] The app also satisfies the CCPA benchmark of requiring consent when personal information is initially collected: the app requests consent for the use of the exposure notification framework, which allows the app to communicate between smartphones;[99] the app also requests consent for data collection and provides information on the necessity for collecting the date, duration, and signal strength when the user turns on exposure notification.[100] Finally, the app also satisfies the GDPR benchmark, since it requests consent for data processing and for data transfer.[101] The consent is explicit and provides information about the categories of data being processed, the purposes of processing, and user rights. This information is explicitly detailed in the privacy notice.[102] Additionally, the information collected is minimal (access data, exposure data, and health data), satisfying the "necessity" requirements. Finally, the app allows for the withdrawal of consent within the app, satisfying the need for a withdrawal option.[103]

The Israeli HaMagen app satisfies the level of consent required CCPA but may not satisfy that of GDPR. HaMagen is not subject to the HIPAA benchmark because it collects location data, not medical data, and stores the data locally without sharing them.[104] HaMagen also fulfills the CCPA benchmark because it requests consent to collect location data when signing up for the app.[105] On the consent screen, the app provides a document laying out the app's terms of use.[106] However, where the German app has multiple

---

[98] *See* Windwehr & York, *supra* note 37, at 2-3 ("[W]hen a person tests positive . . . the app will send all of the daily keys it has used during the past 14 days to a server after the infected user has given its consent to share that data."). Note that the app also requires consent when uploading the QR code that enables the sharing of a test result, which would satisfy HIPAA consent requirements at both the collection and upload stages.

[99] *Corona-Warn-App Privacy Notice*, *supra* note 34, § 2 ("All of the app's main features that require the transfer of your personal exposure or health data . . . will obtain your express consent in advance.").

[100] *Potentially confusing prompts when enabling Exposure Notifications*, GITHUB, https://github.com/corona-warn-app/cwa-backlog/issues/17 (last visited Nov. 24, 2020).

[101] *See Corona-Warn-App Privacy Notice*, *supra* note 34, § 3 ("[T]he [Robert Koch Institute] will only process your data [for the purposes of exposure logging and warning others] if you have given your express consent . . . .") (alteration in original).

[102] *See id.* §§ 5-13 ("What data is processed?").

[103] *See id.* § 12. ("How can you withdraw your consent?").

[104] *See HaMagen Privacy Policy*, *supra* note 41 and accompanying text (explaining the HaMagen app collects location data, which is stored on the user device).

[105] *HaMagen 2.0 App*, MINISTRY OF HEALTH, https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/ (last visited Nov. 24, 2020) (see consent screen after app installation) [hereinafter *HaMagen App*]. Note that the app also requests motion data for the supplemental functionality of collecting driving data, so that it does not conflate time spent in a vehicle with exposure in a public setting.

[106] *Id*.

consent requests, HaMagen requests blanket consent through a singular request screen. The failure to obtain consent for each different type of processing and transfer likely violates GDPR. The terms of use available on the Ministry of Health's website provide information about the categories of data being processed, the purposes of processing, and user rights in the privacy notice,[107] and the posted privacy policy indicates that the Ministry will request consent to share location information if the user tests positive.[108] But neither meets the GDPR standard of consent because the app does not lay these terms out clearly prior to asking for consent. Additionally, the app does not provide a mechanism for users to withdraw their consent, though location data consent can be turned off from the phone's settings. Finally, it is unclear whether consent given to the app is consent given to a public authority (which would not be considered freely given),[109] since the app's servers are owned and operated by the Ministry of Health.

Like the Israeli app, the North Dakota Care19 Diary and Alert apps likely provide the level of consent mandated by CCPA but may not comply with the requirements of GDPR. Similar to HaMagen, both Care19 apps do not collect health data, which exempts them from any HIPAA requirements. Specifically, since officials at the Department of Health are reaching out to those who test positive for them to consent to sharing their location, no PHI flows through the app.[110] Both apps also easily satisfy the CCPA benchmarks. Consent is required for collecting location data in the Diary app,[111] and consent is required for the Alert app to use Bluetooth for exposure notification.[112] Both apps describe in adequate detail the need for collecting their respective data, fulfilling the CCPA requirements. Both apps also likely satisfy key aspects of the GDPR benchmark for consent, since both request consent for data collection; this consent is explicit and provides information about data collected.[113] The apps also request consent for data transfer: if a user tests positive and the public health official calls and verifies the code on the app that allows the app to show a positive test result, then the user can

---

[107] *See HaMagen Terms of Use*, *supra* note 46 (describing how the HaMagen App collects data location, stores it on the user's device, and when it is released to the Ministry of Health for contract tracing).
[108] *HaMagen Privacy Policy*, *supra* note 41, § 8.3.
[109] *See Privacy & Pandemics*, *supra* note 41 ("[U]sers who are diagnosed as Corona patients (or their legal guardians) may allow for their information to be transferred to the Ministry of Health (including its employees, representatives and service providers).").
[110] *See Care19 Diary Privacy Policy*, *supra* note 54 ("Your data is identified by an anonymous code. If you test positive for Covid-19, health officials may ask if you will consent to sharing this code.").
[111] *Care19 Diary App*, *supra* note 55.
[112] *Care19 Alert App*, *supra* note 60.
[113] *Care19 Diary Privacy Policy*, *supra* note 49; *Care19 Alert Privacy Policy*, *supra* note 59.

notify others using the "Share Locations" button on the Diary app[114] and the "Notify Others" button on the Alert app.[115] However, the level of detail in the privacy policies of either app is not as explicit or clear as those in the German app, leaving the possibility that a regulator may find they do not satisfy the GDPR benchmark. In addition, the app does not have an explicit option for the withdrawal of consent, though location data consent can be turned off from the phone's settings, making the satisfaction of the GDPR benchmark further questionable.

Finally, the Indian Aarogya Setu app fares the worst of the five apps, possibly failing the CCPA consent standard and almost certainly failing to satisfy the level of consent required by GDPR. Like HaMagen and the North Dakota apps, the Indian app does not require the uploading of health data, instead relying on self-reporting, which takes it outside the scope of privacy protections mandated by HIPAA. Whether Aarogya Setu satisfies the CCPA benchmark is less clear. The app does request consent to collect location data when signing up for the app, explains the reasons for collecting location and Bluetooth data, and provides the terms of use.[116] However, the app does not provide an explanation for why it requests the demographic (age, sex, profession) and prior health data (such as whether the individual is a smoker).[117] Similarly, the app is even less likely to satisfy the GDPR benchmark, since it is unclear whether collection of demographic data is "necessary" for exposure notification. The privacy policy and consent screens also may not provide enough information for the consent to sharing this data to be considered "informed," and the purposes of processing this data remain unclear as well. Additionally, the app does not request consent for data transfer, though location data are uploaded to a server only if the user has self-reported as testing positive.[118] Although self-reporting a positive test may constitute implicit consent to transfer the data, GDPR requires explicit consent.[119] Finally, like the Israeli app, there is no option to withdraw consent, but consent can be withdrawn through the phone's settings, implicitly allowing for withdrawal rights. And similar to HaMagen, it is unlikely that consent is freely given, since the app and centralized servers are

---

[114] *Care19 Diary App*, *supra* note 55 (Notify tab).
[115] *Care19 Alert App*, *supra* note 60 (Protect tab).
[116] *Aarogya Setu App*, *supra* note 68.
[117] *Aarogya Setu Privacy Policy*, *supra* note 68, § 1(a).
[118] *Id*.
[119] Note that GDPR does not always require explicit consent. It permits processing necessary for the performance of a contract to which the data subject is a party. GDPR, *supra* note 23, art. 6(1)(b). Downloading the app could be considered a contract where the user agrees to provide data in exchange for being given outbreak/health alerts, though such a theory is untested in courts. If the theory holds, then data processing could be considered necessary to perform the contract, making it legal even without consent.

operated by the government. More importantly, downloading the app is mandatory for those currently employed and working, further calling into question how free the consent actually is.[120]

These three regimes affect design choices in different ways, as seen with how each of the apps fare in this category. HIPAA's exclusive focus on medical data exempts apps that rely on self-reporting positive tests, which is less reliable, creating a trade-off between more accurate contact tracing and greater protection of privacy. In contrast, CCPA's consent requirements are widely applicable but easy to satisfy with a request for blanket consent when downloading and setting up the app. GDPR's standards pose the most difficult design choices: requiring that the collection of data be "necessary" narrows the categories of data that can be collected by a contact tracing app, and thus limits the ability for developers to gather data unrelated to contact tracing. But because GDPR requires unbundled consent, apps may have multiple consent requests, either discouraging the user from using the app or forcing them to provide consent without adequately considering whether they care about the privacy implications of such consent. Finally, GDPR's requirement of withdrawal of consent introduces a design element that would likely not otherwise be included.

Table 2: Notice and Consent Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	HIPAA	CCPA	GDPR
Corona-Warn-App			
HaMagen			
Care-19 Diary			
Care-19 Alert			
Aarogya Setu			

B. *Consent Requirements for Health Data Disclosed to Third Parties*

Health data are intimately linked to a person's bodily privacy and has historically been accorded a higher level of privacy protection than other types of data.[121] HIPAA, CCPA, and GDPR all accord high consent

[120] Clarance, *supra* note 67.

[121] *See, e.g.*, DeMay v. Roberts, 9 N.W. 146, 149 (Mich. 1881) (addressing the breach of privacy when a non-medical personnel witnessed a married and pregnant woman go into labor).

requirements regarding the disclosure of medical data to third parties, which necessarily has an impact on contact tracing apps for COVID-19 (and other diseases). For the purposes of this section's analysis, we operate on the theoretical assumption that each of the apps interfaces in some fashion with health data, even though in practice only the German app directly interfaces with medical data.

When it comes to PHI "collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services," CCPA defers to HIPAA.[122] Where HIPAA applies, its consent requirements for the sharing of medical data are strong: PHI collected by health providers or businesses performing certain functions on their behalf cannot be disclosed to third parties without consent of the data subject.[123] Thus, test results shared by health *providers* are subject to protection (e.g. consent), while self-reported data are not, since the latter is not data collected by health providers or their business associates. If a contact tracing app requires validation from a health provider, the HIPAA benchmark applies.[124]

GDPR requires explicit consent for the processing of health data,[125] defined as "personal data concerning health [including] all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject."[126] Special protections apply if the user has not provided explicit consent to health data being used for specified purposes unless processing is necessary or required to protect the "vital interests" of the data subject or unless processing is necessary for preventative or occupational medicine or in the "areas of public health, such as protecting against serious cross-border threats to health."[127] Positive diagnoses of COVID-19 are likely to fall under "sensitive data concerning health" (i.e. data that reveals information about an individual's health status), triggering extra protections.[128]

The German app complies with all three privacy regimes. It can easily avoid HIPAA's restrictions by ensuring that all entities connected with it are either noncovered entities or hybrid entities. If HIPAA were to apply, the German app does share certain PHI, including COVID test results, risk levels,

---

[122] CAL. CIV. CODE § 1798.145(c) (2020).
[123] 45 C.F.R. § 164.508 (2013).
[124] Bradford et al., *supra* note 83, at 9.
[125] GDPR, *supra* note 23, art. 9(1)-(2)(a).
[126] *Id.* art. 4(15); *id.* recital 35.
[127] *Id.* art. 9(1), (2)(c), (h), (i).
[128] *Id.* art. 4.

and information about the onset of symptoms.[129] Since the app obtains consent to collect proximity data and stores them data in an aggregated and anonymous manner, it satisfies the HIPAA standard.[130] The app also satisfies the GDPR standard because it requests consent, both in the app, and from the user when they get a test at a lab.[131] And even if explicit consent is not provided, the exceptions for public health would likely obviate the need for consent.

The Israeli app also appears to comply with all three privacy regimes. Although the Ministry of Health receives information about test results from laboratories and epidemiological investigations, declaring itself to be a hybrid entity would exempt it from HIPAA's requirements. Moreover, the fact that the lists of locations where verified coronavirus patients have visited are aggregated and anonymized means that they are not PHI. Verified patients may be asked to share the location data stored in the app with the Ministry, with the consent being sufficient to satisfy HIPAA and thus also CCPA. In contrast to this extensive analysis, we know that the app's functions fall into the public health exemption for GDPR, making it compliant.

Unlike the extensive HIPAA/CCPA analysis required for the Israeli app, both North Dakotan apps specifically request consent through the Department of Health. This specific consent fulfills the consent requirements required by HIPAA even if the Department of Health is not a covered entity. Further, as discussed above, because the consent requested by the Care19 apps complies the GDPR benchmark, they do not need the public health exemptions. In either case, the exemptions would lead to the GDPR benchmark being satisfied.

Finally, the Indian app presents a close case regarding HIPAA/CCPA compliance, because, like the Israeli app, it cross-references Bluetooth and GPS data with the location of users who tested positive. Because it is unclear whether the Indian Council of Medical Research (ICMR), which hosts the database of test results, would be considered a covered entity, it is unclear whether the app satisfies the HIPAA/CCPA standard. ICMR coordinates biomedical research, but its mandate also includes coordinating and implementing medical research.[132] Additionally, ICMR is associated with a

---

[129] *Corona-Warn-App Privacy Notice*, *supra* note 34, §§ 5(e), 6(b).

[130] *See* Windwehr & York, *supra* note 37 ("[W]hen a person tests positive . . . the app will send all of the daily keys that it has used during the past 14 days to a server after the infected user has given its consent to share that data.").

[131] The lab asks the user to consent to that data being shared when the user takes the test. *Corona-Warn-App Privacy Notice*, *supra* note 34, §§ 5(e), 6(b).

[132] *Mandate*, INDIAN COUNCIL OF MED. RSCH., https://icmr.org.in/about-us/about-icmr/mandate (last visited Jan. 22, 2021).

lab network and sample testing, indicating that the organization may also be conducting testing, which would make it a covered entity.[133] If ICMR has in-house tests that are added to the database which cross references positive tests with user location data, then ICMR's role subjects it to the HIPAA standard. It is unclear whether the tests themselves ask for user consent, like in the German case. Further, the app does not ask for consent for sharing positive test results, leading to further uncertainty about whether the app satisfies the HIPAA/CCPA standard. In contrast to this extensive analysis, the app's function would subject it to the public health exemption for GDPR, satisfying that benchmark.

In the context of consent for medical data, these analyses indicate the diverging incentives and implications of the HIPAA/CCPA and GDPR approaches. Whether a contract tracing app must comply with HIPAA depends on whether it constitutes a covered entity, which is an inquiry heavily influenced by legal definitions that can create rigidity that can slow app development during public health crises like COVID-19. Further, HIPAA's specific consent requirements are relatively stringent; when centralized data provided by a government agency that also administers tests are cross-referenced with user data, that creates complexity that indicates the need for specific consent. This may create a disincentive to have such a centralized system. In contrast, GDPR's exemptions for public health make it more flexible, despite its generally stricter approach to privacy regulation.

Table 3: Consent for Medical Data Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	HIPAA/CCPA	**GDPR**
Corona-Warn-App		
HaMagen		
Care-19 Diary		
Care-19 Alert		
Aarogya Setu		

C. *Location-Identifying Technologies*

Contract tracing apps employ two different approaches to tracking location. One approach uses technologies such as CSLI and GPS to track the app's absolute location, using either information about the nearest cell tower

[133] *ICMR Rapid Response Team for COVID-19*, INDIAN COUNCIL OF MED. RES., https://covid.icmr.org.in/rapid-response-team (last visited Jan. 22, 2021).

(CSLI) or geolocation information derived from satellites (GPS).[134] Another approach uses technologies such as Bluetooth to track an app's proximity to other devices that have Bluetooth enabled and are running the same app.[135] Thus, the former approach collects absolute location data, whereas the latter, proximity-oriented approach instead collects data about location relative to other users, rather than absolute location.

The privacy regimes under consideration take different approaches to the collection of location data. As noted above, apps and data repositories may avoid being subject to HIPAA by avoiding the activities that would bring them with in the definition of covered entity or by being designated a hybrid entity. Where HIPAA applies, it treats device identifiers, serial numbers, and Internet Protocol (IP) addresses used in connection with health information as identifiers that must be removed in order to make the data deidentified.[136] However, in this context the GPS/CSLI and Bluetooth data are not being used by health providers in association with medical data and are instead being collated through separate sources that prevent such information from being considered PHI.[137] Thus, this section will focus on the CCPA and GDPR's provisions regarding GPS/CSLI and Bluetooth data.

CCPA treats IP addresses and location data as types of covered personal information.[138] Thus, the collection of this information requires notice and consent.[139] CCPA does not apply to deidentified information, but it does prohibit re-identification of deidentified information.[140] Bluetooth signals *could* count as de-identified information under CCPA, since such signals fit within the category of information that can "reasonably identify, relate to, describe, be capable of being associated with, or be linked . . . to a particular consumer . . . ."[141] However, *how* contact tracing apps use Bluetooth indicates that it is possible for Bluetooth data to remain deidentified and

---

[134] On the similarities and differences between location tracking using CSLI and GPS, see *Carpenter v. United States*, 138 S. Ct. 2206, 2216-19 (2018).
[135] *See, e.g.*, Douglas J. Leith & Stephen Farrell, *Coronavirus Contact Tracing: Evaluating the Potential of Using Bluetooth Received Signal Strength for Proximity Detection*, TRINITY COLL. DUBLIN (May 6, 2020), https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf (describing Bluetooth contact tracing as measuring proximity between two users; this contrasts with GPS/CSLI, which look for absolute and not relative location data).
[136] 45 C.F.R. § 164.514(b)(2)(i)(M)-(O), (e)(2)(xii)-(xiv) (2013).
[137] *See* Bradford et al., *supra* note 83, at 9 n.47 (describing a possible workaround where covered entities can hire companies like Google or Apple to provide Bluetooth handshake data).
[138] CAL. CIV. CODE § 1798.140(o)(1)(A) (2020).
[139] *Id.* § 1798.135(o)(1)(G).120(b).
[140] *Id.* § 1798.140(h).
[141] *Id.*

escape CCPA scrutiny, whereas location data are always subject to CCPA regulations.

Similarly, GDPR considers location data to be PII, subjecting such data to GDPR protections and principles of lawfulness and consent, limited processing, accuracy, security, and deletion.[142] IP addresses may be considered "personal data" in some circumstances.[143] This is true even if the location data are encrypted, since the information is still "information in relation to an 'identifiable' natural person."[144] In *Breyer v. Bundesrepublik Deutschland*, the Court of Justice of the European Union ruled that even when information such as a dynamic Internet Protocol (IP) address[145] does not provide directly identifiable information about a data subject, if the dynamic IP address was used in combination with data held by a person's Internet Service Provider (ISP), then the dynamic IP address would be considered PII.[146] The court implicitly adopted a relativity test: if a piece of information does not identify a data subject directly but in the hands of a third party could be used to identify a data subject if combined with other data that the third party possesses, then in the hands of that third party, that information is PII.[147] Thus, while Bluetooth data are not generally considered personally identifiable, they can be considered so based on the entity that owns that data; and if so, it requires the same consent standards as GPS/CSLI data. *Breyer* effectively subjects Bluetooth to the same consent requirements as CSLI, meaning that under GDPR, contact tracing apps must follow the same consent requirements regardless of which mechanism of location tracking they follow. Even so, the principle of data minimization is also at play. The European Data Protection Board (EPDB) has taken the position that contact tracing apps require only deidentified proximity data and that the collection of location tracking information violates the principle of data minimization because "contact tracing apps do not require tracking the location of individual users."[148] Thus, the EPDB's view implies that the use of location

---

[142] GDPR, *supra* note 23, arts. 4-6.

[143] Case C-528/14, Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779 ¶¶ 31-49 (Oct. 19, 2016), http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&doclang=en.

[144] Bradford et al., *supra* note 83, at 6.

[145] A dynamic IP address is where the identifier assigned to a network-connected device periodically changes, in order to protect the privacy of the end-user.

[146] *Breyer*, ECLI:EU:C:2016:779, ¶ 49.

[147] *Id.*

[148] Eur. Data Prot. Bd., Guidelines 04/2020 on the use of location data and contract tracing tools in the context of the COVID-19 outbreak 7 ¶ 27 (adopted Apr. 21, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_enlinee-guida/guidelines-042020-use-location-data-and-contact-tracing_en [hereinafter EDPB Guidance on Contact Tracing]; Letter from Andrea

data is more violative of privacy than the use of Bluetooth data. Going further, the Board requires that any unique and pseudonymous identifiers must be renewed regularly.[149]

Here, the German app uses Bluetooth, rather than CSLI, to track contacts.[150] These data are encrypted using changing temporary keys through the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) and Temporary Contact Numbers (TCN) protocol.[151] By using encryption and the two protocols, the data being collected do not "reasonably" identify individuals, thereby satisfying the CCPA threshold for using information that cannot be linked to a user. In addition, every time the app exchanges data with the server system, it processes access data, including the IP address and the date and time of retrieval, although the IP address is conveyed only to a special access server, which discards the IP address before forwarding the data to the appropriate server.[152] Even so, the app still asks for consent in multiple places, satisfying CCPA's and GDPR's consent requirements.[153]

In contrast, the Israeli app uses GPS (with opt-in consent to using Bluetooth), for which CCPA requires consent.[154] But as we concluded above, the app satisfies the CCPA consent requirements. Conversely, although GDPR is technology agnostic, the Israeli app does not satisfy GDPR consent standards given the principle of data minimization, and therefore would fail the GDPR benchmark.

The North Dakotan apps are split: the Diary uses GPS data to track location, which without consent would violate CCPA.[155] Since the North Dakotan Alert app uses Bluetooth to track contacts, it likely satisfies the CCPA threshold even without asking for consent. While both apps adequately fulfill both the CCPA and GDPR consent requirements, because of the GDPR data minimization principle, the Alert app (which uses

---

Jelinek, Chair, Eur. Data Prot. Bd., to Olivier Micol, Head or Unit C.3 – Data Protection, DG for Justice and Consumers 2 (Apr. 14, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdfour-work-tools/our-documents/letters/edpb-letter-concerning-european-commissions-draft-guidance-apps_en.

[149] EDPB Guidance on Contact Tracing, *supra* note 148, at 9 ¶ 42.

[150] *See supra* note 37 and accompanying text.

[151] *Data Privacy and Security,* CORONA-WARN-APP OPEN SOURCE PROJECT, https://www.coronawarn.app/en/ (last visited Feb. 25, 2022); *About This Project*, *Corona-Warn-App*, GITHUB, https://github.com/corona-warn-app/cwa-documentation (last visited Feb. 25, 2022).

[152] *Corona-Warn-App Privacy Notice, supra* note 34, § 5(a).

[153] *Id.* § 3(a).

[154] *See supra* note 41 and accompanying text.

[155] *See supra* Sec. I.

Bluetooth) satisfies both CCPA and GDPR requirements, whereas the Diary app (which uses GPS) satisfies only the CCPA standard.

The analysis of the Indian app is similar to the analysis of HaMagen: since it uses both GPS/CSLI and Bluetooth, without consent the app would violate the CCPA standard.[156] However, since the app does request consent satisfactory to the CCPA standard, it passes the CCPA benchmark. In contrast, because the app does not satisfy the GDPR consent requirements and because the use of GPS/CSLI data violates the data minimization principle, despite the technology agnostic nature of GDPR, the Indian app fails that benchmark.

While CCPA distinguishes between CSLI and Bluetooth indirectly (by virtue of identifiability), consent allows app developers to escape that distinction, and any app that satisfies the consent requirement for collecting data satisfies CCPA. Note, however, that app developers *could* escape the need for consent under the CCPA standard if they used an adequately encrypted or deidentified version of Bluetooth, which would make such an app more usable. In contrast, prior to the guidelines for contact tracing apps, GDPR did not provide this kind of flexibility regardless of technology. Since Bluetooth-based contact tracing does not collect absolute location data and is implicitly more privacy friendly than GPS/CSLI-based contact tracing, CCPA's approach promotes a more privacy-friendly technology, as do the updated EPDB guidelines favoring Bluetooth rather than CSLI. However, the European standard relies on the principle of data minimization rather than the bedrock principle of requiring consent for identifiable information generally.

Table 4: Location Identifying Technologies Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	CCPA	**GDPR**
Corona-Warn-App		
HaMagen		
Care-19 Diary		
Care-19 Alert		
Aarogya Setu		

[156] *See supra* note 70 and accompanying text.

D. *Data Profiling*

Data profiles compile or collate data from disparate sources in order to identify individual users' preferences, behaviors, attitudes, and characteristics, and to predict future trends for consumer behaviors. In the context of contact tracing, the creation of a data profile would require linking the limited location and testing information gathered from an app with other user/consumer preference data (such as purchasing data, demographic data, and income and economic data) in order to build a stronger understanding of each individual user. The creation and proliferation of such profiles creates privacy concerns, both in terms of the breadth of knowledge that companies have about consumers and in terms of the kinds of information that can be deduced about a consumer by combining different types of information that individually do not reveal much.[157] Both GDPR and CCPA address the creation of data profiles; HIPAA does not.

Under CCPA, personal information is defined in a broad manner that implicates the creation of data profiles. Data collected for "short-term, transient use" fall under the business purpose exception and are not subject to the consent requirements mentioned above "provided that the personal information . . . is not used to build a profile about a consumer."[158] Contact tracing data could easily fall under this exception. Additionally, CCPA defines "personal information" to include information that could identify, relate to, or describe "inferences drawn . . . to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[159] Thus, personal information collected using contact tracing apps that helps identify consumer trends by adding to a pre-existing data profile will be subject to CCPA regulations, such as notice and consent, deletion, and access requirements.

Under GDPR, the data minimization principle applies: only data pertaining to the purpose for which it is being processed can be collected.[160]

---

[157] For example, the knowledge about a consumer's zip code or their birthday individually may not be considered harmful. However, a collated data set that includes both zip codes and birthdays of individuals significantly increases the probability that the consumer's name and identity can be determined. *See, e.g.*, Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000), https://dataprivacylab.org/projects/identifiability/paper1.pdf ("[C]ombinations of few characteristics often combine in populations to uniquely or nearly uniquely identify some individuals.").

[158] CAL. CIV. CODE § 1798.140(d)(4) (2020).

[159] *Id.* § 1798.140(o)(1)(K).

[160] GDPR, *supra* note 23, art. 5(1)(c).

In addition, GDPR has broad prohibitions on data profiling, and notes that data subjects have the

> right not to be subject to a decision . . . based solely on automated processing . . . . Such processing includes "profiling" that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to [analyze] or predict aspects concerning the data subject's . . . personal preferences or interest . . . [behavior], location or movements . . . .[161]

In contrast to CCPA, this means that the collection of broad personal data unrelated to the original purpose of processing, collected in order to create a data profile, is strongly discouraged and has no exemption for transient purposes. Consumers can, however, opt-*in* to data profiling through consent; nonetheless, the default is that data profiling is prohibited.[162] However, in some ways, GDPR's standard is narrower—and thus easier to satisfy—than the CCPA's standard, because under GDPR, the collection of less related data must be with the *intent* to predict or analyze behavior, whereas the CCPA's standard is that *any* data that allows for *inference* about consumer behavior require the higher consent and affirmative user rights standards.

Of the five apps analyzed, the German, Israeli, and both North Dakotan apps satisfy the CCPA and GDPR standards by not creating a consumer data profile. The German app's minimalist approach requires only consent for the collection of Bluetooth data and the upload of daily keys and no other personally identifiable information.[163] Similarly, the Israeli app simply asks for consent to use location data but does not ask for any personally identifying information.[164] The same is true for both North Dakotan apps.[165]

The Indian app, in contrast, collects far more data about the individual than the other four apps. First, as mentioned above, the app requires the creation of a profile prior to its activation, including requesting a user's phone number and input about their travel, occupation, and certain health factors, such as whether they smoke. Such information goes beyond the location data collected in the other three apps. Occupational information and past travel information can indicate information about the individual's personal characteristics and trends and could help link the data subject to a pre-existing data profile, should the government (which owns the app) choose to create

---

[161] *Id.* recital 71.
[162] *Id.* art. 22(2)(c).
[163] *See supra* note 37 and accompanying text.
[164] *HaMagen App*, *supra* note 105 (see consent screen after app installation).
[165] *Care19 Diary App*, *supra* note 55; and *Care19 Alert App*, *supra* note 60 (see consent screens after app installation; no personally identifiable information is requested).

one. Because the app creates a data profile that satisfies CCPA's notice requirements but does not satisfy GDPR's notice requirements, the app passes the CCPA benchmark and fails the GDPR benchmark.[166]

Thus, apps that require the bare minimum data (e.g. Bluetooth or GPS/CSLI data) and do not require any personally identifiable information easily satisfy the CCPA and GDPR benchmarks. Under CCPA, these apps could also escape any consent requirement through the business purpose exception, making the apps easier to use but also less transparent. The same is not true for GDPR, where consent will always be required. Ultimately, both regimes' data profiling requirements can be satisfied by notice and consent, which indicates that it may be fairly easy for app developers to use location data to help build data profiles. The ease with which this standard can be satisfied may reduce the public's trust in contact tracing apps and thereby reduce such programs' efficacy. A data profiling threshold that is less reliant on notice and consent may better influence the public's decision to use contact tracing apps.

Table 5: Data Profiling Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	CCPA	GDPR
Corona-Warn-App		
HaMagen		
Care-19 Diary		
Care-19 Alert		
Aarogya Setu		

E. *Data Minimization*

Some privacy regimes require data minimization, which limits the number of categories of data being collected by the app. HIPAA does not have a data minimization principle. In contrast, CCPA permits the collection, use, retention and sharing only of data that are "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed" and to other disclosed purposes compatible with those purposes.[167]

Similarly, GDPR provides that data processors and controllers may collect only the personal data only for specific purposes and may not process

[166] *See supra* notes 116-120 and accompanying text.
[167] CAL. CIV. CODE § 1798.100(c) (2020).

them further.[168] Additionally, processing of personal data must have a lawful basis for every controller, so that any additional data controllers must also obtain consent from the data subject.[169] These strong protections mean that contact tracing apps must have strong justifications for each field of user data being collected and cannot collect an overbroad range of data.

The results for all apps for data minimization are similar to, but slightly different from, the results for data profiles. The German, Israeli, and North Dakotan apps collect location or pairwise location data, as mentioned previously, and link data subjects to test results. Thus, the two fields of data necessary for contact tracing—location and test results—are the two data fields being collected in these apps. *Because* only two data fields are required for contact tracing services, the creation of an account in a contact tracing app would violate CCPA's and GDPR's data minimization requirements, in addition to violating GDPR's prohibition on data profiling. Note also that the data minimization principle in the EPDB's latest guidelines states that Bluetooth data does not violate the data minimization principle, while GPS/CSLI data does.[170] Thus, as noted in Section II.C, HaMagen, Care19 Diary, and Aarogya Setu would fail the GDPR benchmark.

There are also instances in which an app can fail GDPR's data minimization requirements without creating a data profile. For example, HaMagen may further violate GDPR's data minimization requirement: it is unclear whether it is necessary to collect motion data, which is used to exclude location data where the user may be traveling in a car.[171] Similarly, if the German app were to collect non-COVID-19-related health data, such as sleep data, that would likely violate GDPR's data minimization requirement but satisfy the data profiling benchmark, but possibly satisfy CCPA if sleep data are used for purposes compatible with contract tracing. There are also instances in which an app can fail the data profiling requirement, while succeeding on the data minimization requirement. For example, the German app could simply link the contact tracing data to a preexisting data profile while collecting no more information than required for contact tracing, failing the data profile standard but succeeding on the data minimization requirement.

This logic is also why the Indian app further fails in minimizing the data categories being collected: as mentioned, it collects phone numbers, prior health data, occupational, and travel data, all of which are not required for contact tracing (as exemplified by the other three apps). However, it remains

---

[168] GDPR, *supra* note 23, art. 25(2).
[169] *Id.* art. 6(1).
[170] *See supra* note 148 and accompanying text.
[171] *HaMagen App*, *supra* note 105.

to be seen what the European Courts' interpretations of strong justifications are: would the Indian apps' justifications for collecting non-location and test result data fulfill the as-yet-undecided threshold for what justifications are valid?

The data minimization benchmark creates an incentive for app developers to create genuinely privacy-protective apps, in contrast to the data profiling requirement, which is easily defeated by notice and consent. Note, however, that the functionality of the app defines what "minimal" data are, and an app that brands itself as more than just a contact tracing app—for example, an app that also aims to prevent community spread—may be able to collect more data than just the location and test result data for a simple contact tracing app.

Table 6: Data Minimization Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	GDPR
Corona-Warn-App	
HaMagen	
Care-19 Diary	
Care-19 Alert	
Aarogya Setu	

F. *Data Sale and Sharing with Non-Research Third Parties*

Data sale and sharing refers to the transfer of data to third parties. The former is done through the exchange of money, whereas the latter may be due to existing partnerships, other business transactions, or business agreements. Data sale and sharing enable the creation of data profiles that aggregate data from different sources by entities outside of the app owner/creator. In this section, we address data sale and sharing with non-research third parties. Research exemptions are addressed in the next section.

HIPAA, CCPA, and GDPR all address data sale and sharing. HIPAA's restrictions on the sale and sharing of PHI require explicit consent with high penalties associated with violations of this provision. HIPAA mandates that covered entities and business associates not sell PHI,[172] unless the covered entity tells the data subject that "the disclosure will result in remuneration" and the data subject opts-in to authorize the sale of that data.[173] The

[172] 45 C.F.R. § 164.502(a)(5)(ii) (2013).
[173] *Id.* § 164.508 (a)(4).

regulations also lay out specific limits on what constitutes valid authorization, creating a strict and well-defined bar for the sale of PHI.[174]

CCPA's requirements are weaker, mandating opt-out rights or consent for the *sale* of any personal information.[175] It also prohibits businesses from retaliating against consumers who refuse to consent to the sale of their data.[176] However, this prohibition does not apply to the sharing of data for business purposes, such as short-term transient use of data or research for technological development.[177] It also does not apply to businesses handling the personal information of fewer than 50,000 consumers and businesses making less than $25 million in annual revenue.[178] Both exceptions mean that the regulations around data sale and sharing are moderately restrictive and that apps simply need to have an opt-out field to prevent the sale of their data.

GDPR requires controllers collecting personal data to inform the data subject of any recipients of personal data.[179] Controllers that do not obtain personal data directly from the data subject must inform the original data subject of any recipients of their personal data and any other envisaged disclosures to other recipients.[180] Data subjects have the right to receive confirmation from the controller about whether it is processing any of their personal data, information of any recipients of their personal data (particularly those in third countries or international organizations), and details of their rights under GDPR.[181] Further, any processing by joint controllers must be transparent.[182] Additionally, GDPR permits data transfers to third countries (all countries outside the European Economic Area) subject to a long list of requirements.[183] Despite these standards, the regulation does

---

[174] *Id.* § 164.508 (b)(1).
[175] CAL. CIV. CODE § 1798.120(a), (b) (2020).
[176] *Id.* § 1798.125.
[177] *Id.* § 1798.140(d); (t)(1)(C).
[178] *Id.* §§ 1798.135(a), .140(c)(1)(A), (B).
[179] GDPR, *supra* note 23, art. 13(1)(e).
[180] *Id.* art. 14(1)(e), (3)(c).
[181] *Id.* art. 15(1)-(2).
[182] *Id.* art. 26(1)-(2).
[183] *See id.* arts. 44, 45, 46, 49(1) (stating that data transfer to third countries is allowed only if the Commission has decided that third country ensures an adequate level of protection; the transfer is made subject to appropriate safeguards, such as legally binding and enforceable instruments between public authorities, binding corporate rules, standard data protection clauses, an approved code of conduct, or an approved certification mechanism; or the processing has received the data subject's consent, is necessary for the performance of a contact between the data subject and the controller, is necessary for important reasons of public interest, or is necessary to protect the vital interests of the data subject or of other persons); *see also id*. art. 27(1)-(2) (stating that controllers and processers not established in the EU must designate a representative within the EU unless their processing is occasional,

not limit the kinds of information or the amount of information being shared with a data processor. Thus, GDPR's standards for how data are shared or sold are ambiguous and have large carve-outs that make the regulation's protections moderately strong. However, since GDPR's text governs both data sale and *sharing*, it is more protective than the CCPA standard.

All of the apps we are studying can avoid HIPAA's mandates by making sure they fall outside the definition of a covered entity or by being designated a hybrid entity. If HIPAA does apply, since all five apps eventually have medical data provided to them (the German app requires reporting it through a private testing facility, whereas the other four apps receive test results from government entities), the analysis is easy. None of the apps indicate that they are selling data or sharing *medical* data with third parties, which means that all four would satisfy the HIPAA standard. Because no data are being *sold*, the CCPA's low benchmark would also be satisfied. Similarly, for GDPR, while each of the apps does share data with third parties, each of the apps also is performing a "task carried out in the public interest"[184]—preventing the spread of disease—so this data sharing is likely exempted. Even if the apps' functionalities do not satisfy the "public interest" requirement, each of the apps provides notice about the sharing of data for necessary purposes in their privacy policies, satisfying the GDPR benchmark.

The German app's privacy notice states that the app "will only pass on your data collected in connection with your use of the app to third parties if the [app operator] is legally obliged to do so," indicating that *any* data—including medical data—is [sic] not being sold or shared, which satisfies the GDPR benchmark.[185] Similarly, because the data are not being sold, it satisfies both the HIPAA and CCPA benchmarks.

For the Israeli app, neither its terms of use nor its privacy policy explicitly refers to the sale of data. The privacy policy states that "information about your locations is only stored on your device and is not forwarded," indicating that the data are not being shared or sold, satisfying all three regimes.[186] The only exception is verified users who consent to transferring their location to the Ministry. Because the government is the app developer and not a third party, no heightened privacy requirements exist.[187]

---

does not include special categories of data specified in Article 9, and is unlikely to result in a risk to the rights and freedoms of natural persons or is a public authority or body).

[184] *Id.* art. 6(1)(a), (d), (e).

[185] *Corona-Warn-App Privacy Notice*, *supra* note 34, § 10.

[186] *HaMagen Privacy Policy*, *supra* note 41, § 3.

[187] *Id.* § 1.

The North Dakotan Care19 Diary app shares only anonymized location data with third parties, and thus any such sharing complies with HIPAA.[188] The app's privacy notice states that the app shares data with third parties such as Foursquare, Google, and Bugfender "for specific data processing tasks."[189] Because the data are shared and not sold, the CCPA benchmark is easily satisfied. And because this information is shared only after obtaining notice and consent, the GDPR benchmark is also easily satisfied.

The Care19 Alert app shares only anonymized location data with third party processors, which generally falls outside of HIPAA's scope.[190] Further, the app's privacy notice states that the app "uses Google Firebase Analytics to collect usage data," but that it "does not capture the Apple or Google Advertiser Ids."[191] The lack of further representations about nondisclosure in the privacy policy leaves it unclear whether Care19 Alert satisfies CCPA (because of the lack of clarity) or GDPR (because of the inadequate detail in the notice).

Finally, the Indian app notes that the data collected will "only be used by the Government of India," which is the app's developer, so no third party sharing is implicated.[192] The app's privacy policy also explicitly notes that the data collected will not be used for purposes other than contact tracing and will only be used by the app creator (the Indian government), implying that health data will not be shared or sold to third parties.[193] Effectively, the app satisfies all three benchmarks.

Data sale and sharing effectively amounts to the transfer of usage and location data from the original app owner to third parties, allowing third-parties to use data for other purposes, including marketing, the building of consumer profiles, behavioral analytics, and general consumer, market, health, and location trends. The protections embodied in the three regimes add caveats to the transfer of such data to third parties. Each of the three

---

[188] *Care19 Diary Privacy Policy*, *supra* note 49.
[189] *Id.* Note, however, that Foursquare is a "digital marketing service," and it is unclear whether the location data being shared with it is for the purpose of marketing or for other reasons. Tim Starks, *Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better*, POLITICO (July 6, 2020, 7:00 AM EDT) https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601.
Even if it were for marketing purposes—though the privacy policy, *supra*, denies that by stating that "location data is private to you"—it is unclear whether the use of this data with Foursquare would still qualify the North Dakotan app as under the public issue exemption. *Care19 Diary Privacy Policy*, *supra* note 49.
[190] *Care19 Alert Privacy Policy*, *supra* note 59.
[191] *Id.*
[192] *Aarogya Setu Privacy Policy*, *supra* note 68, § 2(a).
[193] *Id*. § 6.

standards creates different incentives for app developers: the HIPAA benchmark forbids the sale or sharing of medical data without opt-in consent; the CCPA standard prohibits the sale of data but permits the sharing of data for business purposes; and GDPR regulates the sharing of data but also allows for public interest exceptions. The incentives created here are obvious: medical data sharing is the most difficult and discouraged, whereas other shared data are not covered even by notice and consent requirements under CCPA, and data sharing for public health purposes is unlikely to be covered either. Beyond the type of data, the sensitive information contained in contact tracing apps can easily be sold or shared once a user gives consent or opts-in, which many users agree to without reading the fine print. This reflects the broader concern that the existence of information in this form could be shared given the status quo consumer practices of the information economy, which raises skepticism about contact tracing apps broadly.

Table 7: Data Sale and Sharing with Non-Research Third Parties Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	HIPAA	CCPA	GDPR
Corona-Warn-App			
HaMagen			
Care-19 Diary			
Care-19 Alert			
Aarogya Setu			

G. *Access to Data for Research*

Researchers can access stored user data for myriad reasons. In the public health context, both individual and aggregate data may be useful in tracking down individual cases and in understanding broader geographic and demographic trends in the spread of disease. In this context, we consider whether researchers have access to (1) deidentified or pseudonymized data and (2) individual user data. CCPA, HIPAA, and GDPR all address researcher access to data.

HIPAA includes exemptions for research and public health. Covered entities may disclose deidentified and limited datasets for the purpose of research or public health, as long as there is "a data use agreement between the covered entity and the limited data set recipient."[194] Covered entities may

[194] 45 C.F.R. § 164.514(e)(3)(i), (4) (2013).

also use individual PHI for research, public health, health care operations, or research purposes, subject to appropriate restrictions.[195] Thus, HIPAA's regulations in this area are moderately strong, since they require deidentification and limitations of the data being used.

CCPA also creates exemptions for research. For example, the obligation to make certain disclosures for sales of personal information "for a business purpose"[196] does into include "internal research for technological development and demonstration."[197] In addition, the statute does not require businesses to comply with consumer's requests to delete personal information used for "public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws" if that deletion would impair the research and the consumer has provided informed consent.[198] And researchers can access deidentified or pseudonymized data.[199] CCPA's definition of "research" further requires that research uses be compatible with the business purpose for which the personal information was collected, pseudonymized and deidentified, made subject to technical safeguards and business processes that protect against reidentification and inadvertent release of deidentified information, and that such information not be used for any commercial purpose.[200]

In addition, CCPA requires businesses to disclose the categories of third parties to whom the business sells personal information[201] and to obtain notice and consent before doing so.[202] "Third party" is broadly defined as a person that is not directly collecting personal information from consumers or is not receiving consumer data pursuant to a contract,[203] where "person" is defined to include only private entities.[204] "Sell" is defined as communicating personal information for "monetary or other valuable consideration."[205] In a scenario where an app shares data with researchers for research, it is ambiguous whether the business is receiving "monetary or other valuable consideration," and it may vary depending on whether the researching entity is considered a third party or a business partner. For deidentified or

---

[195] *Id.* § 164.512(b) & (i)(1) (2013).
[196] CAL. CIV. CODE § 1798.115(a)-(c) (2020).
[197] *Id.* § 1798.140(d)(6).
[198] *Id.* § 1798.105(d)(6).
[199] 45 C.F.R. § 164.502 (a)(5)(ii)(B)(2)(i) & (ii) (2013).
[200] CAL. CIV. CODE § 1798.140(s) (2020).
[201] *Id.* §§ 1798.110(a)(4), (c)(4), 1798.115(a)(2).
[202] *Id.* § 1798.120(a)-(c).
[203] *Id.* § 1798.140(w).
[204] *Id.* § 1798.140(n).
[205] *Id.* § 1798.140(t)(1).

pseudonymized data, it is likely that such data is exempt, creating few or no restrictions. For individual data such as PHI, it is possible that one of the research exemptions apply, and that consent requirements do not, creating a moderately strong restriction.

In contrast to CCPA, GDPR's restrictions on research access are weak. The regulation's basic principles permit processing for "scientific or historical research purposes" subject to appropriate safeguards,[206] such as data minimization. Data minimization includes pseudonymization and deidentification,[207] where pseudonymization is defined processing data "in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such information is kept separately and . . . [such] data are not attributed to an identified or identifiable natural person."[208] Member states may provide for derogations of users' rights to access data, rectify data, restrict processing of data, and object to particular uses of data that may render impossible or seriously impair the scientific research.[209]

A number of GDPR's general provisions also have implications for research. As a general matter, processing by third parties must be necessary for the purpose of their legitimate interests except where those interests are overridden by the data subject's interests or fundamental rights and freedoms of the data subject,[210] where "third party" is defined to include public authorities and agencies.[211] One of GDPR's recitals specifies that "anonymous information, including for statistical or research purposes" does not constitute personal data subject to GDPR's restrictions.[212] To be considered anonymous, the information cannot relate to a natural person, which is a high threshold.[213] GDPR also recognizes processing "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" as a lawful basis for processing which does not need consent.[214] Effectively, for deidentified data or aggregate data, the consent and purpose limitation requirements are not likely not to apply.

---

[206] GDPR, *supra* note 23, art. 5(1)(d)-(f).
[207] *Id.* art. 89(1); *see also id.* recital 156 (describing safeguards of data minimization).
[208] *Id.* art. 4(5); *see also id.* recital 156 (noting the pseudonymization of personal data as a safeguard).
[209] *Id.* art. 89(2).
[210] *Id.* art. 6(1)(f).
[211] *Id.* art. 4(10).
[212] GDPR, *supra* note 23, recital 26.
[213] *Id.* art. 4(1).
[214] *Id.* art. 6(1)(e).

The research associated with the German app likely complies with all three privacy regimes. The German app asks for consent to agree to share usage data, which is information to improve the effectiveness of the app and to improve statistics about the pandemic.[215] If consent is given, usage data are compiled into anonymized statistics.[216] By requesting specific consent before sharing usage data and protecting data through aggregation and anonymization, the app satisfies the requirements of HIPAA, CCPA, and GDPR. CCPA also specifically exempts research to improve the product.

A similar analysis applies to the Israeli, North Dakotan, and Indian apps: Because no medical data are shared (including with researchers), each app passes (or rather escapes) the HIPAA standard. Since the Israeli and Indian apps do not sell or share any data with any *third party*, they also escape the CCPA and GDPR standards. HaMagen does collect some information to monitor and improve the app's functionality, but the gathering of that information falls within CCPA's exception for research to improve the technology, and the company also escapes CCPA and GDPR provisions by collecting the data anonymously and (according to the privacy notice) and by sharing only with the app developers.[217]

Finally, the Care19 apps' developers are not the states' health departments, who could be considered researchers. Nonetheless, location data are shared—not sold—anonymously with state health departments, who use such data to track the spread of COVID-19. For the Diary app, health officials ask for consent to access recent locations.[218] For the Alert app, anonymized data about aggregate exposures is shared with the state's department of health.[219] Because the health authorities are not paying for access to this data, both apps likely satisfy the CCPA and GDPR standards. Both Care19 apps also collect usage data on app crashes, diagnostic data for reliability and support purposes, and general usage data, such as the screens that are viewed most often and the adoption rate for new versions of the app, all of which fall within the CCPA's exception for research to improve the technology.[220]

In the Indian app's case, the data will "only be used by the Government of India in anonymized, aggregated datasets for the purpose of generating

---

[215] *Corona-Warn-App Privacy Notice*, *supra* note 34, § 6(f).
[216] *Id*. § 5(e). The specific process used for anonymization is through rolling proximity identifiers that change in short intervals. Additionally, the data are stored locally, so even the anonymized data are not shared with a third party until necessary. *See generally id*.
[217] *HaMagen Privacy Policy*, *supra* note 41, § 13.
[218] *Care19 Diary Privacy Policy*, *supra* note 49.
[219] *Care19 Alert Privacy Policy*, *supra* note 59.
[220] *Id.*; *Care19 Diary Privacy Policy*, *supra* note 49.

reports, heat maps, and other statistical visualisations."[221] However, where users test positive, the users' data will be shared with "persons carrying out medical and administrative interventions necessary."[222] Here, we assume that the aforementioned persons are part of the Indian government, and thus not a third party. If such persons are third parties, then further research is needed into the relationship between those carrying out medical interventions and the app developer, the Indian government.

The takeaway from this section is twofold: first, for contact tracing apps and their background infrastructure, the three regimes provide large carve-outs that mean that businesses conducting research (CCPA), covered entities (HIPAA), and public agencies and other institutions (GDPR) can all circumvent the consent, deletion, and accountability requirements that otherwise would apply. However, it is easier for apps to share deidentified or anonymized data, as compared to individual user data, which are still subject to some regulations such as board approval (HIPAA), or ambiguous clauses (CCPA). Second, where the research is being conducted by the app developer—which can be a government agency with whom sharing PHI is generally concerning, as with the Israeli and Indian apps' cases—this benchmark does not apply. Effectively, the regimes err towards public interest and public health when it comes to research, and app developers could easily provide pseudonymized or aggregated data to public health entities without issues of liability.

Table 8: Researcher Access to Data Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	HIPAA	CCPA	GDPR
Corona-Warn-App			
HaMagen			
Care-19 Diary			
Care-19 Alert			
Aarogya Setu			

H. *Affirmative User Rights*

User-controlled post-collection changes, or affirmative user rights, include the rights to amend and delete data once they have been collected,

[221] *Aarogya Setu Privacy Policy*, *supra* note 68, § 2(a).
[222] *Id.*

and the right to be forgotten. In contact tracing apps, these rights would require apps to have the option to amend or delete collected data, either where they are stored on the user's phone, or on a centralized server. HIPAA, CCPA, and GDPR all include these rights.

HIPAA provides subjects with the right to access[223] and amend their PHI.[224] In practice, this means that PHI collected by a health provider and transmitted to an app should be accessible and amendable by the users at the point of input (i.e. the health clinic or health department). Because all five apps are essentially reporting apps that are not the *source* of test data but rather collect test data from third parties (health clinics or government agencies), each app's architecture allows it to escape the HIPAA benchmark. Specifically, even if the app could amend the individual's PHI in the app, the original test result data reside outside the boundaries of the app, either on a health provider's database or a government database.[225] Thus, since the apps are separate from the entities that conduct testing and do not store the original testing data, the HIPAA benchmark does not apply where the app is operated or developed by an entity other than a test result provider or healthcare provider.

CCPA requires the option for users to access[226] and delete their data at the data subject's request (though it provides no time frame for implementing this right is provided).[227] Notably, CCPA does not require the right to rectify data.

In addition to the rights to access and rectification right mandated by HIPAA and the rights to access and deletion required by CCPA, GDPR also mandates storage limitation, the right to restrict automatic processing, the right to data portability, and the right to object to automated individual decisionmaking.[228] Of the three privacy regimes, GDPR provides the most complete list of affirmative user rights.

---

[223] 45 C.F.R. § 164.524(a)(1) (2014).
[224] *Id.* § 164.526(a) (2001).
[225] We note that both for HaMagen and Aarogya Setu, the agencies/government ministries that collate data and conduct tests are separate from the organizations that are running the apps, creating enough of a separation that the apps are not accessing test data that were natively created on the app. Rather, a separate entity (a lab, hospital, or ministry-affiliated organization) conducts the testing, and the app is simply a means of reporting that testing. This two-step process means that the apps themselves escape HIPAA scrutiny. A canonical example of where the app is subject to HIPAA scrutiny is if the app was run by a hospital, clinic, or an organization that administered tests.
[226] CAL. CIV. CODE § 1798.100(d) (2018).
[227] *Id.* § 1798.105(a).
[228] GDPR, *supra* note 23, arts. 15, 16, 17, 18, 20, 21.

With respect to affirmative user rights, the German app largely complies with all three privacy regimes. If HIPAA were to apply, the Corona-Warn-App acknowledges users' rights to access and amend their data.[229] The German app allows users to delete contact journal entries "at any time."[230] Positive lists, which have random IDs that indicate positive test results and pairwise location data, are deleted from server systems within twenty-one days.[231] The app also allows users to delete contact journal entries containing various types of information "at any time," although data that has already been transmitted to other smartphones cannot be deleted.[232] Users can also delete the association of the random ID with their phone by deleting the app from their phone.[233] While this does not satisfy the "request" requirement under CCPA, it still provides users with an option to delete their data, or have them eventually be deleted, thus passing the CCPA and GDPR benchmarks of right to deletion and erasure, although in a roundabout way. And as required by GDPR, it acknowledges users' key rights under GDPR[234] and allows users to withdraw consent.[235]

The Israeli app satisfies CCPA by providing access and deletion options. First, it allows users to look at exposure history in the app, satisfying the access requirements.[236] Further, users can delete the app, which would delete all information on the device.[237] Deletion of the app does not have any impact on information that verified COVID-19 patients have agreed to share with the government, but that information has been anonymized and thus does not fall under the scope of any of the three privacy regimes. HaMagen does not appear to support the other user rights required by GDPR, including the right to rectification, the right to restrict automatic processing, the right of data portability, and the right to object to automated individual decisionmaking.

The North Dakotan apps also support a number of affirmative user rights. The Diary app allows users to look at their location history.[238] Users can delete their data either by selecting the "erase data" button in the app or by

---

[229] *See Corona-Warn-App Privacy Notice*, *supra* note 34, § 13 (acknowledging users' right to access under GDPR Article 15 and right to rectify under GDPR Article 16).
[230] *Id.* §§ 3, 5(f), 6(b), 9(a), 12, 13.
[231] *Id.* §§ 9(b), 13.
[232] *Id.* §§ 3, 5(f), 9, 12, 13.
[233] *Id*.
[234] *See id.* § 13 (acknowledging users' rights under GDPR Articles 15, 16, 17, 18, 20, and 21).
[235] *Id*.
[236] *HaMagen App*, *supra* note 105 (see "Exposure History" option under the main menu).
[237] *HaMagen Terms of Use*, *supra* note 46.
[238] *Care19 Diary App*, *supra* note 55 (see "Visits" screen); *Care19 Diary Privacy Policy*, *supra* note 49.

waiting fourteen days for the data to be deleted from the servers.[239] Users may also use their "About" screen to see and delete all data collected through the app.[240] As such, the Diary app satisfies the right to access mandated by all three regimes and the right to erasure required by CCPA and GDPR, but not the right to rectify mandated by HIPAA and GDPR or the other user rights mandated by GDPR. In contrast, the Care19 Alert app provides access to past exposure checks but does not provide direct access to pairwise location data,[241] which is problematic under both CCPA and GDPR. Even so, users remain free to delete the app and the accompanying data at any time.[242] Although the app does not provide a mechanism for deleting the information that infected users have shared with others, that information has been pseudonymized and thus is not covered by any of the three regimes. But like HaMagen, the app does not support the other rights required by GDPR, including the right to rectification, and so the North Dakotan apps fail the GDPR benchmark.

Finally, the Indian app likely passes the CCPA standard. The app allows users to "see recent contacts."[243] However, it is unclear how far the "recent contacts" go, and whether users can see data from the beginning of collection. Further, the app deletes all of the information provided by the user from government servers within 30 days if users cancel their registration on the app, satisfying both CCPA's right to deletion and GDPR's right to erasure.[244] The Indian app gives users "the right to access [their] profile at any time to add, remove, or modify any registration information."[245] But the right to rectify appears to apply only to registration and not to the other information shared with the app, and the app does not support the other rights mandated by GDPR, thus failing the GDPR benchmark.

The array of affirmative user rights is inconsistent across the three regimes, with GDPR providing the most affirmative rights. As the most privacy protective regime, each of the apps fails the GDPR's benchmark of the right to amend data. This creates a complex set of choices for app design. Providing the option to amend location data is a complex endeavor, especially

---

[239] *Care19 Diary Privacy Policy*, *supra* note 49.
[240] *FAQs About the Care19 Diary App*, COVID-19 IN S.D. (2020), https://covid.sd.gov/care19app.aspx.
[241] *Care19 Alert App*, *supra* note 60 (see "Exposures" screen).
[242] Press Release, Wyo. Gov. Mark Gordon, Wyoming Launches COVID-19 Exposure Notification App with New Bluetooth Technology (Aug. 14, 2020), https://governor.wyo.gov/media/news-releases/2020-news-releases/wyoming-launches-covid-19-exposure-notification-app-with-new-bluetooth-tech.
[243] *Aarogya Setu App*, *supra* note 68 (see "Your Status" screen).
[244] *Aarogya Setu Privacy Policy*, *supra* note 68, § 4(b).
[245] *Id.* § 4(a).

since the location data are not created by the user, but by phone hardware. Further, amending such location data creates a means for users to change their whereabouts, and make contact tracing less effective. Yet, GDPR clearly requires this option, indicating that its set of affirmative rights may not be right for public health-related issues.

Another design decision indirectly implicated by affirmative user rights is how data are stored. Data collected by contact tracing apps can either be stored on the user's phone or transferred to a server in the cloud. If data are retained on the user's phone, the application architecture is likely decentralized, with data being transferred to the cloud only for processing. If data are stored on the cloud, the architecture is centralized, with data storage, processing, and notifications all arising from the cloud. The centralized or decentralized nature of the app's architecture affects privacy, since data stored on a user's phone are either inaccessible or less accessible to third parties compared to data stored on a server in the cloud. Here, the German app is wholly decentralized, whereas the other four apps are centralized in some way. The affirmative rights of access, deletion, and amendment are easier in a decentralized system, since the data are on the phone and can be deleted immediately; whereas deletion on a centralized server takes time depending on whether the system processes data in real time or in batches, and depends on the frequency and location of backups (among other complications).[246] Thus, CCPA's deletion and access rights slightly favor a decentralized system rather than a centralized one.

GDPR also creates the need for accountability mechanisms, which have to do with the right to lodge complaints with a supervisory authority, the right to seek remedies, receive compensation,[247] and with the requirement for controllers to maintain records of, inter alia, the purposes of processing, descriptions of the data being processed, and the categories of recipients to whom processed data are disclosed.[248] This requirement creates the incentive for a centralized system which more holistically and easily tracks the creation, use, and removal of data. In short, the GDPR's affirmative rights of access, deletion, and amendment prefer a decentralized app architecture;

[246] A real-time system is one in which data on the cloud are updated in real time once a user makes a request. A batch system is one that stores requests and processes them periodically, in order to improve efficiency and reduce the burden on the system and its connections to different users. Laura Shiff, *Real Time vs Batch Processing vs Stream Processing*, BMC MACHINE LEARNING & BIG DATA BLOG (May 13, 2020), https://www.bmc.com/blogs/batch-processing-stream-processing-real-time/.
[247] GDPR, *supra* note 23, 77-84.
[248] *Id.* art. 30.

whereas its provisions on accountability leans toward a centralized app architecture.

These regimes thus create conflicting incentives for app developers. Instinctively, decentralized apps are more privacy-friendly since data are stored natively on the user's phone. But accountability mechanisms might be easier to implement in a centralized system, as would researcher access to user data. This conflicting set of incentives means there is a clear trade-off between privacy and statutory compliance.

Table 9: Affirmative User Rights Summary

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A

	HIPAA	**CCPA**	**GDPR**
Corona-Warn-App			
HaMagen			
Care-19 Diary			
Care-19 Alert			
Aarogya Setu			

I. *Summary*

The array of factors discussed provide a complex set of incentives and pointers for app developers when designing contact tracing apps. Some of these incentives are almost contradictory in the context of these apps. And some privacy-focused requirements in the regimes under review are easily defeated by others. For example, clearly worded notice and consent provisions give users the ability to easily give blanket consent to the sharing of their medical data, allow for data profiling, allow for additional data categories to be collected, and allow for data to be shared with third parties.

These factors also implicate application architecture and test reporting. The test reporting method affects what kinds of consent requirements and exceptions surrounding medical data apply. Further, because Bluetooth is less personally identifying than GPS/CSLI, it is preferable as a technology. Because decentralized storage allows for easier implementation of the right to access and delete data, it is the preferred system of storage. Finally, despite the extensive privacy protections created by each of these benchmarks, the nature of the actors also matters. If the app developer is the government, then there is minimal protection against the government's access of location and testing data, despite such information not being shared with third parties.

Finally, the regimes under review implicitly balance the need for privacy with the need for researchers to access this data for public interest and public health purposes. In the context of some public health crises, this might be preferable. In the context of less serious crises, it may not. The balance is subjective and provides flexibility at the cost of privacy.

Table 10: Summary Results

Key: Green = Pass; Yellow = Unclear; Red = Fail; Gray = N/A
H = HIPAA; C = CCPA; G = GDPR

	Notice and Consent			Consent: Medical Data		Location Identifying Technology		Data Profiling		Data Minimization	Data Sale and Sharing			Researcher Access			Affirmative Rights		
	H	C	G	H/C	G	C	G	C	G	G	H	C	G	H	C	G	H	C	G
Corona-Warn-App																			
HaMagen																			
Care19 Diary																			
Care19 Alert																			
Aarogya Setu																			

III. THE IMPACT OF DISEASE VARIABLES

The framework developed above provides a method for assessing how statutory privacy law influences different design decisions about contact tracing apps created for the COVID-19 pandemic. However, the importance and thresholds of each of these factors will vary based on the nature of the disease. Diseases that are more transmissible, more dangerous, or transmitted through different means may cause app developers and policy makers to make different choices regarding the trade-off between privacy and functionality.

In this section, we assess the robustness of our framework by analyzing the impact of different disease variables on select factors. We assess three different diseases, compared with the baseline of COVID-19: SARS, Ebola, and HIV. We look at the mode of transmission, incubation period, mortality

rate, and transmissibility or mean infection rate to see how these variables affect privacy considerations.

A. *Disease Parameters*

COVID-19 is a viral disease that is transmitted through respiratory droplets, and causes a variety of symptoms ranging from fevers to shortness in breath.[249] Symptoms can be felt anywhere from two to fourteen days after exposure.[250] The infection rate, defined as the number of people infected by an infected person, was estimated to be between 1.5-3.5%.[251] While evolving, at the time of writing, the pre-vaccination mortality rate from the disease was around 2%.[252]

SARS is a viral disease, similar to COVID-19, caused by a SARS-associated coronavirus.[253] It is also spread through respiratory droplets in the air. A major SARS outbreak took place in 2003.[254] The incubation period for SARS is half that of COVID-19, at around two to seven days.[255] However, the mortality rate is significantly higher, at 9.6%,[256] while the mean infection rate is around 3%.[257]

Ebola is a viral disease that causes fevers, internal bleeding, and death.[258] Major outbreaks of the disease have happened in 2021 and in 2014-16.[259] Transmission happens through contact with an infected individual's bodily fluids, though individuals not in close contact (within three feet) of an infected person are not at risk; individuals are not contagious until they begin

---

[249] Ctrs. for Disease Control & Prevention, *Symptoms of Coronavirus* (Feb. 22, 2021), https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html.
[250] *Id*.
[251] *Id*.
[252] *Coronavirus disease pandemic – Statistics & Facts*, STATISTA (Mar. 1, 2021), https://www.statista.com/topics/5994/the-coronavirus-disease-covid-19-outbreak/.
[253] *SARS Basics Fact Sheet*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/sars/about/fs-sars.html (last visited Mar. 4, 2021).
[254] *Id*.
[255] *Id*.
[256] *Fatality rate of major virus outbreaks worldwide in the last 50 years as of 2020*, STATISTA, https://www .statista.com/statistics/1095129/worldwide-fatality-rate-of-major-virus-outbreaks-in-the-last-50-years// (last visited Mar. 4, 2021).
[257] *Infection rates of viruses involved in outbreaks worldwide as of 2020*, STATISTA, https://www.statista.com/statistics/1103196/worldwide-infection-rate-of-major-virus-outbreaks/ (last visited Mar. 4, 2021).
[258] Ctrs. for Disease Control & Prevention, *Ebola Signs and Symptoms* (Nov. 5, 2019), https://www.cdc.gov/ vhf/ebola/symptoms/index.html
[259] Ctrs. for Disease Control & Prevention, *Ebola Outbreaks* (Feb. 23, 2021), https://www.cdc.gov/ vhf/ebola/outbreaks/index-2018.html.

having symptoms.[260] The virus can also survive on dry surfaces.[261] The incubation period varies from two to twenty-one days,[262] with a transmission rate of 0.14-4.37% depending on the population.[263] The disease is highly fatal, with a mortality rate of 25-90% (though mortality varies by region).[264]

Finally, HIV is an autoimmune disease that is transmitted sexually, through the sharing of needles, syringes, or other drug injection equipment, and through perinatal transmission.[265] The time it takes for HIV to be detectable after infection varies, from two weeks into the range of months.[266] The transmissibility of HIV depends on a variety of factors, is dependent on case-by-case factors, and is difficult to measure given the intimate nature of sexual activity and the lack of transparency and knowledge about partner infection status.[267] The range of infection rates, according to one study, could be between 0.04% and 1.4% depending on the type of sex; this study does not include transmission through needle sharing or perinatal transmission.[268] Mortality also varies depending on the geographic region, method of transmission, race, and other factors.[269] Current mortality rates in the U.S. are around 4.7 deaths per 1,000 infections, though the rate was around 9.1 deaths

---

[260] Ctrs. for Disease Control & Prevention, *Ebola Transmission* (Jan. 14, 2021), https://www.cdc.gov/ vhf/ebola/transmission/index.html.
[261] *Id*.
[262] *See* Ctrs. for Disease Control & Prevention, *Ebola Signs and Symptoms*, *supra* note 258.
[263] Saranya A. Selvaraj et al., *Infection Rates and Risk Factors for Infection Among Health Workers During Ebola and Marburg Virus Outbreaks: A Systematic Review*, 218 J. INFECTIOUS DISEASES S679, S683 tbl.3 (2018).
[264] Suresh Rewar & Dashrath Mirdha, *Transmission of Ebola Virus Disease: An Overview*, 80 ANNALS GLOBAL HEALTH 444, 444 (2014) (noting that case fatality rates vary from 44-90%); WORLD HEALTH ORG., *Ebola virus disease* (Feb. 23, 2021), https://www.who.int/news-room/fact-sheets/detail/ebola-virus-disease (noting that case fatality rates vary from 25-90%).
[265] Ctrs. for Disease Control & Prevention, *Ways HIV can be Transmitted* (Nov. 3, 2020), https://www.cdc.gov/hiv/basics/hiv-transmission/ways-people-get-hiv.html.
[266] *See, e.g.*, Ctrs. for Disease Control & Prevention, *About HIV* (Nov. 3, 2020), https://www.cdc.gov/hiv/basics/whatishiv.html (citing the initial symptoms as being experienced within two to four weeks); Philip Alcabes, Alvaro Muñoz, David Vlahov & Gerald H. Friedland, *Incubation Period of Human Immunodeficiency Virus*, 15 EPIDEMIOLOGIC REVS. 303, 303 (1993) ("[T]he lag period from infection to [detection] is . . . 2 weeks to 3 month . . . and rarely lasts more than 7 months.").
[267] James Wilton, *Risk of Exposure to HIV/AIDS*, STAN. HEALTH CARE, https://stanfordhealthcare.org/medical-conditions/sexual-and-reproductive-health/hiv-aids/causes/risk-of-exposure.html (last visited Mar. 6, 2021).
[268] *Id*.
[269] *See, e.g.*, Karin A. Bosh et al., *Vital Signs: Deaths Among Persons with Diagnosed HIV Infection, United States, 2010-2018*, 69 MORBIDITY & MORTALITY WKLY. REP. 1717, 1722 (2020) ("[D]ifferences still exist by gender, race/ethnicity, age, transmission category, and region.").

per 1,000 infections over the last ten years.[270] The historical peak of the disease varies, and mortality rates depend on the kind of study; a study of Israeli individuals infected with HIV found that 12% of infected patients died in 1996.[271]

Table 11: Disease Variables

Disease	Method of Transmission	Incubation Period	Infection Rate (%)	Mortality (%)
COVID-19	Airborne transmission through respiratory droplets	2-14 days	1.5-3.5	2.2
SARS	Airborne transmission through respiratory droplets	2-7 days	3	9.6
Ebola	Contact with infected bodily fluids	2-21 days	0.14-4.37	25-90
HIV	Sexually transmitted; sharing of needles; perinatal transmission	2 weeks to 7 months	0.04-1.4	0.47-0.91 (current) 12 (peak)

Note that SARS, Ebola, and HIV antedated the effective dates of both GDPR and CCPA. Regarding HIPAA, the SARS outbreak occurred at the same time that HHS issued the Privacy Rule implementing HIPAA. HHS issued a bulletin in November 2014 providing guidance on its application to Ebola but did not issue a statutory waiver.[272]

B. *SARS*

The primary differences between COVID-19 and SARS are the incubation period and the mortality rate. The reduced incubation period increases the efficiency of contact tracing, since an individual will encounter fewer contacts in a shorter incubation period, leading to fewer tertiary

[270] *Id*. at 1719.
[271] Zohar Mor, Rivka Sheffer & Daniel Chemtob, *Causes of Death and Mortality Trends of All Individuals Reported With HIV/AIDS in Israel, 1985-2010*, 40 J. PUB. HEALTH 56, 56 (2018). Note that this is one study and one statistical analysis, and other studies have different outcomes. We use this number simply for illustrative purposes, but acknowledge that the mortality of HIV-infected individuals varies based on a multitude of factors.
[272] U.S. Dep't of Health & Hum. Servs. Off. for Civ. Rts., Bulletin: HIPAA Privacy in Emergency Situations (Nov. 2014), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/hipaa-privacy-emergency-situations.pdf.

transmissions that need to be traced.[273] However, the increased mortality rate increases the need for contact tracing and researcher access so that public health-focused groups can optimize their response and reduce the number of deaths.

Here, the exemptions of the three regimes provide adequate flexibility for responding to diseases like SARS that have more serious consequences and may require more serious public health interventions. We note that similar to COVID-19, it seems unlikely that individual PHI would be required in order to track symptoms, since the disease's mortality and transmissibility does not depend on demographic or geographic factors (unlike Ebola or HIV). Thus, we look to whether deidentified information is easily accessible by third parties.

HIPAA permits the disclosure of deidentified and limited datasets for public health purposes if a data use agreement is signed by the covered entity and the recipient of the data.[274] CCPA's standard is less privacy protective, exempting CCPA requirements for researchers accessing deidentified data, and providing leeway to businesses helping with statistical research in the public interest.[275] And the GDPR standard is the least privacy protective here, allowing for deidentified or aggregate data to be used for research if that is compatible with the originally identified purpose of data collection.[276] GDPR also has a public health exemption.[277] All three of the standards provide adequate flexibility to researchers to quickly tailor their public health response when dealing with a deadly disease like SARS.

C. *Ebola*

COVID-19 and Ebola differ in three primary ways: Ebola is harder to transmit, since it is not airborne and requires contact with an infected person's bodily fluids; Ebola's incubation period is longer; and its mortality is an order of magnitude higher.

The different mode of transmission means that contact tracing apps that use pairwise contact tracing through Bluetooth may be ineffective, since proximity to an infected individual is irrelevant to whether a user is infected.

---

[273] *See* Matt J. Keeling, T. Deirdre Hollingsworth & Jonathan M. Read, *Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19)*, 74 J. EPIDEMIOLOGY & CMTY. HEALTH 861, 861 (2020) ("Longer time scales would allow tertiary cases to be infected and potentially increase the scale of tracing required.").

[274] *See supra* note 194 and accompanying text.

[275] *See supra* notes 168 & 198 and accompanying text.

[276] We note here that there are implications to the strength and method of deidentification. *See supra* notes 206-214 and accompanying text.

[277] GDPR, *supra* note 23, art. 9(1) & (2)(c), (h), (i).

Instead, location-based tracking may be effective in tracking the absolute locations (rather than relative/pairwise locations) of individuals who eventually test positive, and then informing others who have been in those locations that they are at risk of having touched a bodily fluid. Pairwise location tracking would be ineffective since proximity matters less than being in the same physical location where an infected individual may have shared bodily fluids. In fact, pairwise location tracking may overestimate transmission and create false positives, since being near an infected individual does not guarantee or even implicate transmission.

CCPA considers location data as personally identifiable, requiring notice or consent.[278] Similarly, GDPR considers location data as personally identifiable, requiring notice and consent, limited processing, accuracy, security, and deletion rights.[279] However, GDPR provides app developers and operators with a way to work around the consent requirement, since data processing "necessary for the performance of a task carried out in the public interest" is alternative lawful basis for data processing.[280] While the other requirements of limited processing, accuracy, security, and deletion might still be required, the biggest hurdle of consent can be worked around. In contrast, CCPA explicitly prevents the waiver of consumer's rights under the act, meaning that CCPA provides less flexibility in this context, and would reduce the effectiveness of contact tracing by needing to ask users to consent to the collection and sharing of their location data.[281]

In addition to the impact on location identifying technology, the data categories collected may be different in the case of a disease that spreads via contact to bodily fluids. Because activities that involve the exchange of bodily fluids include intimate activities, including sexual activities, an effective contact tracing app may want to collect not just location data, but also the relationship and identity of partners who are likely to have come into contact with bodily fluids. The GDPR's principles of data minimization could be implicated in this process. Since GDPR allows only data necessary for the specific purpose of processing to be collected, the app developer or operator in this case would need to be able to justify why advanced partner tracking is needed.[282] Necessity also implies that a less privacy-intrusive mechanism for collecting this data is unavailable, so the developer would need to eliminate other, less-effective methods for collecting this data. And since the data

[278] CAL. CIV. CODE § 1798.135(o)(1) (2020).
[279] *See generally* GDPR, *supra* note 23.
[280] *Id.* art. 6(1)(e).
[281] CAL. CIV. CODE § 1798.192.
[282] *See generally* GDPR, *supra* note 23.

minimization clause has no waiver or flexible interpretation, the benchmark here is privacy-protective, but may hinder a public health response.

Note however that from a public health perspective, the long incubation period may make contact tracing inadequate as a response. However, because the mode of transmission is less dangerous than that of COVID-19 and other airborne diseases, the disadvantage of the long incubation period on contact tracing may be balanced by the fact that fluid transmission leads to fewer potential tertiary transmissions. In addition, because individuals are not contagious until symptoms develop, and because the symptoms of Ebola are so severe and unique, as compared to those of COVID-19—which in mild cases can be similar to the flu—contact tracing might still be effective in identifying individuals who are infected, and finding tertiary transmissions.

Finally, researcher access, as discussed under SARS, *supra*, is also implicated due to the high mortality of the disease.

D. *HIV*

COVID-19 and HIV are dissimilar in most ways, the most significant of which is the method of transmission. In addition, the incubation period of HIV is orders of magnitude longer than that of the other three diseases. These disease variables implicate the following factors: location and data minimization; consent for medical data; affirmative user rights; and researcher access to data.

Similar to Ebola, because HIV is transmitted not through the air, but through intimate activity like sexual activity and the sharing of needles, Bluetooth pairwise data are entirely irrelevant. However, location data are also irrelevant since being close to someone with HIV does not lead to an infection. Instead, contact tracing in this case requires a log of sexual partners or needles shared, and would be quite effective despite the long incubation period.[283] This is because the risk of tertiary transmission is lower due to the method of transmission: since airborne viruses intuitively spread quicker than viruses spread by direct or indirect sexual contact, it is less likely that HIV is spread so quickly that contact tracing becomes ineffective.[284]

Effective contact tracing thus requires tracking sexual partners, rather than location, raising a vastly more intimate set of privacy concerns. Informing at-risk third parties in the contact tracing process also implicates

[283] Of course, location data may be helpful in tracing such partners, but would violate the data minimization principle.

[284] Specifically, the number of individuals exposed to an average COVID-19-infected individual per unit of time is likely to be higher than the number of individuals exposed to an average HIV-infected individual in that unit of time.

the sharing of the data subject's medical data with a third party. Here, HIPAA requires explicit consent from the data subject for this data to be shared with a non-research third party and imposes severe fines for violations of this rule.[285] However, if the President declares an emergency and the Secretary of Health and Human Services declares a public health emergency, the Secretary can waive fines where covered entities do not comply with the patient's right to request privacy restrictions and to receive adequate notice.[286] Thus, statutory issues around HIPAA provide some flexibility with respect to notifying potential sexual partners of where the risk of HIV came from. In contrast to HIPAA, GDPR provides inherent flexibility in the form of a public health exemption that removes the need for consent for sharing such data, without needing to rely on the declaration of a public health emergency.[287] Finally, CCPA does not have restrictions on data sharing, and defers to the HIPAA standard regarding the disclosure of medical data. Effectively, all three regimes provide varying levels of flexibility that would improve the effectiveness of contact tracing, while reducing privacy for the data subject.

In addition, affirmative user rights are implicated, much in the same way that they are for the other apps. However, the privacy implications of an incorrectly reported HIV test are significantly worse than those of an incorrectly reported positive COVID-19 test, given the stigma associated with being found HIV positive. Since none of the regimes provide for a waiver for data correction and deletion, each of these regimes provides minimal flexibility towards app developers developing an HIV contact tracing app, which could hinder a quick public health response.[288] However, this inflexibility works in favor of privacy rights.

---

[285] *See supra* notes 122-123, 172-174 and accompanying text.

[286] *See* Project BioShield Act of 2004, Pub. L. No. 108-276, 118 Stat. 835 (2004) (specifying the authority of the Secretary of Health and Human Services in case of an emergency); 42 U.S.C. § 1320b-5 ("[T]he Secretary is authorized . . . to temporarily waive or modify the application of . . . sanctions and penalties that arise from noncompliance of [various requirements] of [HIPAA]."); *see also* U.S. Dep't of Health & Hum. Servs., *COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency* (Mar. 2020), https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf ("[W]hile the HIPAA Privacy Rule is not suspended during a public health or other emergency, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bioshield Act of 2004 (PL108-276) and section 1135(b)(7) of the Social Security Act.")

[287] *See supra* notes 127 & 183 and accompanying text (referring to conditions for exemption that remove the need for consent in data sharing).

[288] *See supra* Section III.H (discussing the rights to amend and delete data once they have been collected by all the regimes).

Finally, researcher access, as discussed under SARS, *supra*, is also implicated due to the high mortality of the disease.

IV. CONCLUSION

Contact tracing poses difficult questions about how strike the appropriate balance between the collective need for public health and the privacy interests of particular individuals. This balance varies not only in terms of the severity of the threat posed by different diseases, as discussed above, but also with the importance of the privacy interests at stake.

These privacy interests can generally be divided into two categories. One set of interests focuses on the rights individuals, either by creating a private sphere in which they engage in self-development or by giving them control over how their persona is presented to the outside world.[289] The other set views privacy from a more consequentialist perspective that focuses on the harms to society if privacy is not protected.[290]

Different aspects of contact tracing implicate these interests in different ways. On the one hand, location and disease information can raise direct personal concerns both by allowing public intrusion into what would otherwise be personal spaces and by preventing individuals from exercising control over the information about themselves that is presented to the world. The cost of insufficient privacy protection of these interests become manifest in the form of stunted personal development and dignitary harms. From a societal perspective, insufficient privacy protection can lead to lower levels of contact tracing apps utilization and the concomitant harm to public health.

The nature of these different interests in turn shape the importance of providing different types of data protection. Although the three regimes rely primarily on consent and deidentification as the primary mechanisms for protecting privacy, the differ in terms of their scope. HIPAA and CCPA protect against disclosures only by covered entities and businesses, respectively, in contrast to GDPR's more general approach of encompassing all controllers and processors of data. The distinctions drawn by HIPAA and CCPA imply that disclosures by these actors pose greater harms than disclosures by other actors. A comparison to the personal and societal

---

[289] *See, e.g.*, AURELIA TAMÒ-LARRIEUX, DESIGNING FOR PRIVACY AND ITS LEGAL FRAMEWORK 28-32 (2018) (defining privacy by the control of individual information access and dissemination restrictions).

[290] *See, e.g.*, *id.* at 33-38 (assessing privacy in terms of the harm brought about by information leakage).

interests in privacy would shed light on the propriety of this inference and the particular interests each regime tends to protect.

GDPR also explicitly provides a higher level of protection to what it terms special categories of personal data, including "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[291] HIPAA similarly focuses exclusively on PHI. Both approaches contrast with CCPA's protection of all "personal information" largely without regard to specific subject matter and reflect a recognition that not all types of personal information have the same privacy implications. Moreover, all of the regimes do not differentiate among different types of health information. In so doing, they overlook the fact that certain types of health information carry greater importance for privacy interests than others.

Lastly, GDPR provides the most capacious mechanisms for taking privacy interests into account. The importance of societal interests are reflected in its provision authorizing "processing . . . necessary for the performance of a task carried out in the public interest or in the exercise of official authority" as an alternative to consent.[292] It also permits the EU and Member States to enact legislation to restrict user rights under GDPR:

> when such a restriction represents the essence of the fundamental rights and freedoms and is a necessary and proportion measure in a democratic society to safeguard . . . important objects of general public interest of the Union or of a Member State, . . . including . . . public health.[293]

At the same time, GDPR explicitly accommodates personal interests by allowing justifications for processing to "overridden by the interests or fundamental rights and freedoms of the data subject."[294] HIPAA, in contrast, is less flexible, providing only for waivers of specific rules during times of national emergency. CCPA does not allow for waivers at all.

Thus, these regimes vary widely in the extent to which they can take different types of privacy interests into account. We see how the regimes emphasize different facets of privacy in how the different architectures and design decisions of each app in theory succeed and fail benchmarks posed by

---

[291] GDPR, *supra* note 23, art. 9(1).
[292] *Id.* art. 6(1)(e).
[293] *Id.* art. 23(1)(c).
[294] *Id.* art. 6(1)(f).

each regime. In future crises, HIPAA's strong blanket focus on PHI, the CCPA's emphasis on consumers' privacy against business entities, and the GDPR's more all-encompassing approach will shape how app developers choose technologies (Bluetooth or GPS/CSLI), application architecture (centralized or decentralized), what kinds of data are collected, sold, and shared, and how researchers interact with collected data.

In turn, these varying approaches to privacy will determine the effectiveness of developers, technologists, and policymakers' response to a public health crisis. A heavy focus on privacy may impact flexibility, resulting in a slower response. An overly flexible approach may give governments and researchers access to sensitive data that can cause genuine harm in the long term. No regime will have all the answers, and each will leave open questions and uncertainty about aspects of contact tracing or other public health responses that are unforeseeable, and each regime's oversight body will have to react appropriately. In conducting an analysis across different privacy regimes, different contact tracing apps, and in looking at different disease variables, we see how any technological response to a public health crisis requires nuance and a struggle with the complex and fragmented nature of statutory law. Our hope is that in future public health crises, as we harness the power of the internet, smartphones, and ever advancing technology, our lawmakers and privacy statutes take an interdisciplinary and multifaceted approach to protecting privacy and promulgating the needs of public health.