DATA PRIVACY & PUBLIC HEALTH

COVID-19 Contact Tracing Legislation Across All 50 States

ALBERT FOX CAHN, ESQ. AND
ELENI MANIS, PHD, MPA

APRIL 1, 2021

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

I. Introduction

Contact tracing is considered an important tool in combatting the spread of infectious diseases and has increasingly garnered attention as the world attempts to mitigate the impact of the COVID-19 pandemic. Contact tracing generally entails the collection of information from individuals who are determined to have the disease (or to have been exposed) so that their close contacts can be alerted to such potential exposure and prompted (or compelled) to self-isolate, thus reducing the possibility of subsequent infection. In the context of the COVID-19 pandemic, certain contact tracing programs that have been perceived by some as having been more effective than others, such as those implemented in certain nations in Asia, rely on scale, speed, and to a certain extent, compulsion: increased participation and ease of data sharing leads to a more significant impact. Yet factors that may make such initiatives more efficient can also come at the cost of consent, privacy, and individual rights, in particular as they relate to data privacy concerns, especially as these initiatives have evolved from relying on human contact tracers to relying on contact tracing technology.

Recognizing an urgent need for contact tracing in combatting the spread of COVID-19, however, certain state legislators have made efforts to implement data privacy legislation relating to COVID-19 contact tracing initiatives, with hopes that addressing privacy concerns might increase participation in such initiatives. This review presents a 50-state survey on the status of COVID-19 related contact tracing data privacy laws, with a particular focus on initiatives limiting or blocking law enforcement or immigration authority access to contact tracing data. Research was conducted in December 2020 and the status of the various legislation discussed in this review may have since changed.

Part I of this paper provides an overview of the privacy-related aspects of enacted contact tracing legislation. Overall, very few states have enacted such legislation. Although this section also discusses executive orders for additional context, our research did not include a comprehensive review of executive orders relating to contact tracing. Part II summarizes certain key components of pending or previously proposed legislation, again with a focus on privacy risk. Part III highlights certain other privacy protections relating to contact tracing disclosed on state websites or in the privacy policies of state-sanctioned contact tracing mobile applications. Greater detail on certain legislation is presented in Appendix A, which also includes a list of states that sponsor some type of exposure notification system based on the use of a mobile application.

II. Enacted Legislation

Preliminarily, privacy protection for personal information collected pursuant to state-administered contact tracing programs under existing federal law seems limited. Most notably, the Health Insurance Portability and Account Act of 1996 ("HIPAA"), establishes standards for the protection of certain health information. However, the extent to which HIPAA privacy protections apply to state-conducted contact tracing is not entirely clear and may vary from state to state, depending on how each state's health agencies and contact tracing efforts operate—in particular, depending on whether data collection is conducted by HIPAA-governed or HIPAA-exempt entities. Moreover, under HIPAA there are certain "permitted uses and disclosures" that authorize the disclosure of an individual's private health information. Among such permitted disclosures are twelve broadly defined "national priority purposes" including (i) for public health purposes, (ii) in a judicial or

administrative proceeding if the request for the information is through an order from a court or administrative tribunal, and (iii) to law enforcement officials for law enforcement purposes under certain circumstances, including pursuant to court orders, court-ordered warrants, subpoenas and administrative requests.

As noted above, contact tracing can raise several concerns, including with respect to consent, privacy and individual rights. These concerns are intertwined. From the perspective of individual rights, participation in contact tracing initiatives ought to be as voluntary as reasonably possible, and each voluntary participant ought to have the right to maintain the privacy of his or her personal information. In addition to protecting privacy rights, such protections can actually improve contact tracing efforts. Individuals who can be certain these rights are protected may be more inclined to participate in such initiatives, thereby generating efficiency. In reviewing contact tracing data privacy legislation that has been proposed or enacted, several aspects of legislative initiatives related to privacy assurance and protection: confidentiality, use restrictions (and especially restrictions on access to such data by law enforcement and immigration authorities), transparency, consent and data security, as well as various other data privacy provisions such as those related to data retention obligations and third-party contractors.

As of the time of our review, only three states have enacted legislation pertaining to contact tracing data privacy, and a fourth state has passed a resolution urging the governor to provide greater privacy protections for such data. New York passed NY A10500-C/S08450C in July of 2020 (codified at Public Health Laws Art. 21 Title 8 §§ 2180 - 2182), which was signed into law on December 23, 2020. This law ensures the privacy of contact tracing information by mandating that the identities of COVID-19 positive individuals not be disclosed to their close contacts and also implements a series of use restrictions. Contact tracing information may not be disclosed except as necessary to carry out contact tracing, and a record must be made of any permitted disclosure, including to whom such disclosure was made. Significantly, this law also prohibits law enforcement agencies or immigration authorities from engaging in contact tracing, and also prohibits contact tracers or contact tracing entities from providing contact tracing information to law enforcement agencies or immigration authorities. Though silent on whether participation is voluntary, the law provides that waiving confidentiality requires written consent. With respect to information security, the law includes a mandate for the Commissioner of Health of the State of New York (or the New York City Commissioner of Health and Mental Hygiene, as applicable) to implement security policies and procedures to ensure that contact tracing data be subject to technical safeguards, policies and procedures for the storage, transmission, use and protection of such data. Moreover, only de-identified data in the aggregate may be shared, and only for a public health purpose or for a public health research purpose. Additionally, any non-governmental contact tracing entity may only retain contact tracing data for a period of 30 days, after which that entity is required to either remove and return the data to the appropriate government contact tracing entity, expunge the data, or de-identify it.

Kansas has also enacted the relatively extensive COVID-19 Contact Tracing Privacy Act (ST 48-961/HB 2016), which was signed into law on June 8, 2020 (codified at Kansas Statutes §§ 48-961 - 962). This law provides that information collected during contact tracing may only be used for contact tracing, and must be destroyed when no longer necessary for contact tracing. Disclosure of the identity of a COVID-19 positive individual to a contact is prohibited. Additionally, contact tracing data collected by a third party may only be obtained by a state-engaged or state-employed

contact tracer and only with the consent of the infected person or contact whose information is disclosed. The law also permits a person to bring a civil action to enjoin violations of the act, and a knowing violation is treated as a misdemeanor. Notably, the enacted provisions carry an expiration date of May 1, 2021.

Additionally, though the Kansas law is silent on the use of contact tracing data by law enforcement or immigration authorities, it does prohibit the use of cellphone location data to identify or track the movement of persons, largely limiting contact tracing to be conducted by interviewing infected persons only either directly or indirectly, such as through computer-generated surveys. Given that participation is also made expressly voluntary, these two factors provide a certain level of protection by removing the surveillance aspect that often accompanies contact tracing technology, such as contact tracing mobile applications: what an infected person chooses to disclose to a contact tracer is at his or her discretion, and that person may also decline to participate entirely.

South Carolina, the third state that has enacted relevant legislation, also carries a similar restriction, prohibiting the use of any applications created for the purpose of contact tracing collection on a cellular device. Enacted on June 25, 2020 (and codified at South Carolina Act No. 142), the act also makes participation voluntary. The act carries certain other protections, requiring that any contact tracing technology utilized for data collection be limited to the collection of public health information only and be carried out and maintained in a decentralized manner, and also clarifies that compliance with HIPAA is mandated. However, the act does not expressly provide for any access restrictions or security measures with respect to the information collected.

Notably, Louisiana's legislature has passed a resolution (Resolution HCR93) calling on the governor to ensure that the individual liberty and rights of citizens are protected as the state administers contact tracing, with an emphasis on making participation voluntary and prohibiting the use of geolocation data or collecting personal information absent consent.

However, certain states have turned to executive and agency orders to relax existing privacy protections in combatting the pandemic. For example, a Montana directive implementing certain executive orders provides for emergency services providers to be notified of contact with COVID-19 positive individuals, relaxing strict compliance with Montana healthcare information laws (though such disclosure nonetheless remains subject to HIPAA). Similarly, a Washington proclamation creates an exception permitting the disclosure of certain personal information that could be used for contact tracing, case investigation, or other public health purposes relating to COVID-19. New Mexico has also issued a public health order and an executive order that collectively require labs and entities submitting COVID-19 reports to include a variety of personal information in these reports to the Department of Health and the New Mexico Epidemiology and Response Division. Vermont has issued an executive order mandating compliance with contact tracing efforts, expressly requiring participation in such efforts.

III. Pending or Previously Proposed Legislation

A number of states have also introduced contact tracing data privacy legislation that has either failed or remains pending. Several of these bills contain provisions to ensure the confidentiality of any information collected and the voluntariness of participating in any contact tracing initiative, also to prohibit discrimination based on non-participation. Others specifically look to restrict the

use of location data, such as by prohibiting its use absent consent or expressly prohibiting the use of location data obtained from cellular devices. And while New York permits the use of location data for contact tracing purposes, a bill introduced in New York (S 8311) would ban the use of facial recognition technology for use in contact tracing.

A few states have introduced legislation specifically restricting the use of contact tracing data for law enforcement: a bill introduced in California (California A 1782), for example, would prohibit the use of information collected during contact tracing to enforce laws or orders created in response to the pandemic, or to investigate violations of such laws or orders; another bill in California (California A 660) would prohibit law enforcement from engaging in contact tracing; a bill introduced in New York (New York A10583/S8448-D) would prohibit the disclosure of emergency health data and personal information in response to a warrant or subpoena and bar admission of such information in court. Alabama has also introduced legislation prohibiting contact tracing data from being produced pursuant to a subpoena unless the subpoena is valid and accompanied by a valid protective order preventing further disclosure of the data. Conversely, a bill introduced in Hawaii (Hawaii HB 2572/SD1), for example, would expressly permit a governmental entity to obtain electronically stored data pursuant to a search warrant, although it also would prohibit the sale of contact tracing information absent consent. A bill introduced in Texas would prohibit the use of location data obtained from electronic devices for contact tracing purposes but would exempt law enforcement and other peace officers from this restriction.

IV. Other State Initiatives

Despite few laws having actually been enacted with respect to contact tracing data privacy, many states are nonetheless otherwise attempting to protect personal information collected during contact tracing. Contact tracing appears to fall under personal health information of the nature generally protected by state privacy laws and HIPAA (albeit subject to inherent limitations), and indeed many states provide disclosures that contact tracing information is generally kept confidential. In some cases, states go further and indicate such information will not be shared with law enforcement or immigration officials. However, in other cases, states specifically warn that information might be made available to law enforcement or other agencies. It is not entirely clear what level of protection such privacy assurances provide with respect to access to such information through warrant or subpoena.

Notably, many states have either implemented their own contact tracing mobile applications or encourage the use of certain such applications. Others have implemented or encourage the use of exposure notification mobile applications. A review of the privacy policies of these applications shows that they are generally based on Bluetooth technology to exchange anonymous tokens with other Bluetooth-enabled devices a user has been in proximity with to notify users of any potential COVID-19 exposure. According to such information, the token associated with each user is randomly generated and changes every few minutes. Users must opt in, and generally may only input a positive test result via a state department of health-issued, randomly generated PIN. Relying on Bluetooth allows such applications to operate without having to rely on geolocation data, and the use of tokens is intended to protect user anonymity. Consequently, according to such information provided, no personally identifiable data or geolocation data need ever be collected or stored. While these tokens do collect and share certain data such as the date, time, signal strength and duration of the proximity, many privacy policies of such applications also expressly state that

deleting the application from a device will also delete any associated data points; users thus also have the right to opt out at will.

V. Conclusion

Given how critical the ability to effectively trace and identify close contacts of COVID-19-positive individuals has become in combatting the pandemic, data privacy protections are equally essential. Close contacts who can be made certain their personal information is protected would likely be far more willing to share such information with public health departments. While contact tracing technology such as mobile applications have the ability to increase efficiency, users must be able to trust such technology. Moreover, with only three bills signed into law regarding contact tracing data privacy as of this review, the current state of legislation in this field may leave many wary, especially given that other states have turned to executive and administrative orders to require participation in contact tracing initiatives or to relax privacy protections with respect to personal health information afforded under pre-existing data privacy laws.

As of this review, New York has been the only state to enact legislation that prohibits the sharing of contact tracing data with law enforcement or immigration authorities, and to prohibit law enforcement or immigration authorities from engaging in contact tracing. Two other states have enacted legislation to ensure participation in contact tracing initiatives will be voluntary, and have largely prohibited the use of mobile contact tracing applications outright.

As vaccine availability increases and the prospect of herd immunity to COVID-19 grows, legislators may have fewer incentives to focus on contact tracing and data privacy. This fleeting urgency is underlined by the expiration dates of certain provisions in the legislation discussed in this paper. However, an increasing reliance on technology, together with a renewed focus on epidemic and pandemic preparedness highlights the pivotal role data privacy can play in protecting public health: having effective contact tracing protocols with adequate data privacy protections already in place can assist in efficiently providing for the isolation of exposed persons and in controlling future epidemics of infectious disease. Legislators would do well to ensure data privacy remains on their agendas, even as the pandemic increasingly appears to have an end in sight.

Appendix A

I. Enacted Legislation and Other State Initiatives

a. Enacted Legislation

i. Kansas (K.S.A. §§ 48-961 - 962 and Kansas Administrative Regulations § 28-1-41 and § 28-1-42).

Section 48-961 is titled the "COVID-19 contact tracing privacy act". It expires on May 1, 2021. The purpose of the statute is "to protect the privacy of persons whose information is collected through contact tracing and the confidentiality of contact data".

The statute provides that participation in contact tracing is voluntary and prohibits contact tracing conducted "through the use of any service or means that uses cellphone location data to identify or track, directly or indirectly, the movement of persons".

The statute requires contact tracers to execute, under oath, a form stating that he or she is familiar with the statute and the duties it imposes, including the duty of confidentiality. Contact tracers are prohibited from disclosing the identity of an infected person to a contact.

The statute provides that contact data shall be (A) used only for the purpose of contact tracing "and not for any other purpose"; (B) confidential and not disclosed "unless the disclosure is necessary to conduct contact tracing"; and (C) destroyed when no longer necessary for contact tracing.

Contact data collected by a third party may only be obtained by a contact tracer if (A) the disclosure has been consented to by the infected person or contact, or (B) the information is provided pursuant to a valid warrant.

In addition, the statute provides that the contact data collected shall not be produced pursuant to a subpoena "unless such subpoena is issued by a court and is accompanied by a valid protective order preventing further disclosure of such date".

A "knowing violation" of the statute is a class C nonperson misdemeanor.

Section 48-962 provides for sharing information during a public health emergency between the local health officers and first responder agencies. The information to be shared is limited to the address and period of quarantine, isolation or expected recovery of the person and is to only be used for the purpose of allowing the first responders to be alert to the need for protective equipment.

Two regulations were also enacted in connection with contact tracing:

Section 28-1-41 of the Kansas Administrative Regulations, which includes the oath that each contact tracer is required to execute. In relevant part, in the oath the contact tracer swears that he/she is familiar with the contact tracing statute and "the duty of confidentiality contained therein".

Section 28-1-42 of the Kansas Administrative Regulations lists the information that a contact tracer may collect, requires the contact tracer to inform the person that he/she is under no compulsion or prohibition from participating in contact tracing, and has the text which the contact tracer is to use when advising a person.

ii. New York (NY A10500-C (S08450C)) (codified at Public Health Laws Art. 21 Title 8 §§ 2180 – 2182)

This statute provides for the confidentiality of contact tracing information from the identification of individuals who have come in contact with an individual with a confirmed or probable diagnosis of COVID-19. Further, it prohibits law enforcement agents or entities or immigration authorities from being contact tracers or providing contact tracing information to a law enforcement agent or entity or immigration authority.

iii. South Carolina (HJR 5202) (codified at South Carolina Act No. 142)

Pursuant to this joint resolution authorizing the expenditure of federal funds disbursed to the state in the Coronavirus Aid, Relief and Economic Security Act, South Carolina prohibits local health departments from using mobile contact tracing applications. Any contact tracing technology utilized for data collection must be limited to the collection of public health information only, and must be carried out and maintained in a decentralized manner. Participation in any contact tracing initiative must be voluntary.

b. Resolutions

i. Louisiana (LA HCR 93)

House Concurrent Resolution in which the Legislature of Louisiana urges and requests the governor to ensure that the individual liberty and rights of citizens are protected as the state administers contact tracing. In particular, requests the governor to ensure that participation in contact tracing is voluntary and to prohibit the following unless the person subject to the action specifically consents to it: (1) tracking the person's movements through mobile phone geolocation or any other means, electronic or otherwise; (2) data mining that would facilitate the tracking of a person's movements; and (3) the collection of personal identifying information through contact tracing.

c. Selected Executive and Administrative Orders

i. Montana (Directive implementing Executive Orders 2-2020 and 3-2020)

The Directive relaxes certain privacy protections, including strict compliance with the Montana Government Health Care Information Act, to allow for emergency services providers to be notified of contact with COVID-19 positive individuals. Such disclosure nonetheless remains subject to HIPAA.

ii. New Mexico (Public Health Order and Executive Order 2021-001)

Pursuant to the Public Health Order and Executive Order, labs and submitters submitting required COVID reports must include certain personal information in such reports to the Department of Health and to the New Mexico Epidemiology and Response Division.

iii. Vermont (Addendum 8 to A&R Executive Order 01-20)

Pursuant to this Executive Order, Vermont requires compliance with contact tracing efforts; participation is mandatory. Failure to comply may result in referral to the Office of the Attorney General for enforcement.

iv. Washington (Proclamation 20-64)

The Washington Proclamation creates an exception for the disclosure of certain personal information that could be used for contact tracing, case investigation, or other public health purposes relating to COVID-19, including dates of birth, photographs, telephone numbers, email addresses, street addresses and other contact information. The disclosure of personal information for reasons not relating to public health is otherwise prohibited.

II. State-Sanctioned Contact Tracing Mobile Applications

i. CA Notify

ii. CO Exposure Notifications

iii. COVID Alert CT

iv. COVID Alert DE

v. COVID Alert NY

vi. COVID Alert NJ

vii. COVID Alert PA

viii. DC CAN (District of Columbia)

ix. MD COVID Alert

x. MI COVID Alert

xi. COVIDaware (MN)

xii. COVID Trace (NV)

xiii. Slow COVID NC Exposure Notification App

xiv. Care19 Alert System (used by ND, SD and WY)

xv. Crush COVID RI App

xvi. Healthy Together App (UT)

xvii. COVIDwise Exposure Notification App (VI)

xviii. WA Notify Exposure Notification App

xix. WI Exposure Notification App

Contact Tracing Legislation: Summary[1]

I. ENACTED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
1.	KS	ST 48-961 (HB 2016) (*Enacted/Signed 6/8/20*)	COVID-19 contact tracing privacy act: to protect the privacy of persons whose information is collected through contact tracing and the confidentiality of contact data.	Prohibits disclosure of the identity of the infected person to a contact Data only to be used for contact tracing and must be destroyed when no longer necessary for contact tracing Expires May 1, 2021	Prohibits the use of "cellphone location data to identify or track, directly or indirectly the movement of persons"	Expressly makes participation voluntary and no contact or infected person shall be compelled to participate		Contact data collected by a third party may only be obtained by a state-engaged/employed contact tracer with the consent of the infected person or contact whose information is disclosed A person may bring a civil action to enjoin violations Knowing violations are misdemeanors
2.	NY	NY A10500-C / S08450C (*Passed Senate/Assembly 7.23.20; signed 12.23.20*)	Provides for the confidentiality of contact tracing information from the identification of individuals who have come in contact with an individual with a confirmed or probable diagnosis of COVID-19		Contact tracing information may not be disclosed except as necessary to carry out contact tracing Must make record of any permitted disclosure, including to whom it was made No law enforcement agency or immigration	Requires written consent to waive confidentiality	Commissioner to implement security policies and procedures Deidentified data may be shared only for a public health purpose or a public health research purpose	Any non-governmental contact tracing entity must, within 30 days (i) remove data and return to appropriate government contact tracing entity; (ii) expunge data; or (iii) de-identify data

[1] Research was conducted in December of 2020. Further updates to the status of contact tracing data privacy legislation may have occurred since.

	State	Legislation (Bill, Status)	Summary	Data Privacy Protections	Use Restrictions	Transparency, Consent and Access	Security, Encryption and De-Identification	Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)
I.	**ENACTED LEGISLATION**							
					authority may engage in contact tracing No contact tracer or contact tracing entity may provide contact tracing information to a law enforcement agent or entity or immigration authority			
3.	SC	HJR5202 (*signed into law 6/25/20*)	Prohibits local health department from using mobile contact tracing applications	Requires HIPPA compliance	Prohibits use of any applications created for the purpose of contact tracing collection on a cellular device Any contact tracing technology utilized for data collection is limited to collection of public health information only; must be carried out and maintained in a decentralized manner	Participation must be voluntary Department of Health and Environmental control to conduct a public awareness campaign to explain use of contact tracing and individuals may decline to participate		
II.	**ENACTED RESOLUTIONS**							
4.	LA	LA HCR93 (*Passed 6/1/20*)	Resolution requests the governor to ensure that individual liberty and rights are protected as the state administers contact tracing					

III. SELECTED EXECUTIVE ORDERS					
	State	**Order**	**Summary**	**Data Privacy Protections**	**Miscellaneous (Security, Data Retention, Third Party Contractors, Private Right of Action, etc.)**
1.	MT	Directive implementing Executive Orders 2-2020 and 3-2020	Relaxes certain privacy protections. Emergency services providers are to be notified of contact with COVID-19 positive individuals (suspending strict compliance with the Montana Government Health Care Information Act (GHCI)). While conducting communicable disease investigations and notifying contacts, state and local public health officials will give priority to notifying emergency services providers of their potential exposure.	Entities subject to the GHCI must remain aware that disclosures made pursuant to the MT Directive remain subject to HIPAA, Privacy Rule (located at 45 CFR Part 160 and Subparts A and E of Part 164).	Federal changes allowing for notifications are integrated into state law for the duration of the emergency such that sanctions and penalties against covered hospitals that do not comply with certain provisions of the HIPAA Privacy Rule are waived to the limited extent that these provisions would conflict with or preclude disclosures allowed by the federal waiver of HIPAA authorities intended to provide flexibility during this emergency. Also, to the extent that any other statute or administrative rule would preclude disclosures consistent with this Directive and allowed by federal law, including the recent federal waivers of the HIPAA Privacy Rule, strict compliance is suspended during the emergency.
2.	NM	Public Health Order and Executive Order 2021-001	Labs and submitters submitting required COVID reports must include in such reports all information required including (1) patient's name, date of birth/age, gender, race/ethnicity, address, phone number, occupation to the Department of Health and (2) patient name, email address, patient's employer and employer's address and phone number, name of patient's school if applicable and its address to the New Mexico Epidemiology and Response Division.		
3.	VT	Addendum 8 to A&R Executive Order 01-20	Vermonters required to comply with contact tracing efforts; failure to comply may result in referral to Office of the Attorney General for enforcement		
4.	WA	Proclamation 20-64	Prohibits disclosure of personal information for reasons not relating to public health		

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
1.	AL	AL S-1 Introduced (*Prefiled Bill – First Read 2.2.21*) AL HR 107 Failed	Establishes contact tracing and privacy protections		The bill provides that Contact data shall be used only for the purpose of contact tracing and that the State Health Officer, a county health officer, or a contact tracer may not produce contact data pursuant to a subpoena unless the subpoena is issued by a court and is accompanied by a valid protective order preventing further disclosure of the contact data.			
		Website (No contact tracing app)	Notice of Privacy Practices link at the COVID-19 page of the Alabama Department of Public Health allows disclosure, stating that: "we can use or share health information about you for law enforcement purposes or with a law enforcement official." Link		Use of information is permitted for law enforcement purposes.			
2.	CA	CA A 660 (*failed, Senate*)	Use restrictions on contact tracing data		Data may only be used to facilitate contact tracing			Private right of action for violations Data to be deleted within 60 days

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
					Law enforcement cannot engage in contact tracing			
3.	CA	CA A 1782 (*failed, Senate*)	Enacts TACT PACT Act (Technology Assisted Contact Tracing Public Accountability and Consent Terms Act)	Prohibits discrimination based on participation or non-participation Personal information may not be used for enforcement of laws or orders pertaining to or created in response to a public health purpose, or investigations into violations of such laws or orders	Public entity that is not a public health entity will not offer contact tracing Any personal information to be used only for facilitating response to immediate public health purpose Cannot offer contact tracing that collects, uses, retains or shares geolocation data	Must provide means to revoke consent; may revoke consent at any time Must provide mechanism for users to access, correct and delete personal information Must disclose categories of data collected, used or disclosed and the specific public health purpose for each category Entity offering contact tracing must issue public report every 90 days Entities offering contact tracing that are not affiliated with a public health entity must disclose so	Encryption required to extent practicable Cannot associate data with data otherwise collected or maintained for other purposes without consent Cannot reidentify or attempt to reidentify deidentified, anonymized or aggregated data	Private right of action for violations Data to be deleted within 60 days, except data used solely for research Limitations on data collection and use by third party contractors; security and data breach requirements; must provide source code

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
4.	HI	HI HB 2572 / SD1 (*Engrossed 3/3/20, adjourned sine die*)	Prohibits the sale of contact tracing information without consent. Amends provisions relating to electronic eavesdropping law.	Permits a governmental entity to obtain electronically stored data pursuant to a search warrant.		A governmental entity must provide notice to the person whose data has been obtained, but may seek to delay the required notice period.		
5.	MN	MN H.F. No. 4665 (*Introduced 5/11/20*)	Mandatory contact tracing prohibited, employee health tracking prohibited, data classified, and civil penalties imposed.					
6.	MN	MN S.F. No. 4500 (*re-referred 5/16/20*)	COVID-19 testing and contact tracing bill of rights					
7.	MN	MN H.F. No 164 (*Introduced 6/19/20*)	Mandatory contact tracing prohibited, employee health tracking prohibited, data classified, and civil penalties imposed.					
8.	MO	MO HB566 (*Prefiled 12/21/20*)	Prohibits requirement to participate in contact tracing					
9.	NJ	AR167 (*referred 6/15/20*)	Establishes Assembly Select Committee on COVID-19 Contact Tracing Data Privacy	Review requirements and best practices to ensure privacy of personal information,	Review authorized uses of contract tracing data and use restrictions		Review mandatory protocols and best practices for collecting, storing and restricting	Review length of time that contact tracing data may be retained by a contact tracing entity

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
				including HIPPA compliance			access to contact tracing data Review appropriate measures to prevent data mining	Review mandatory protocols and best practices regarding the destruction of contact tracing data
10.	NJ	A4170 / S2539 (*Passed Assembly 7.30.20, received by Senate 8.3.20*)	Restricts use of certain data collected for purposes of contact tracing related to COVID-19 pandemic.		Contact tracing health and location data may only be used for purposes of completing contact tracing			Civil penalty for violation Personal information to be deleted within 30 days Public health entities must publish name(s) of any third party contractors Contractors may only use data for contract tracing
11.	NY	NY A10583 / S8448-D (*Passed Senate 7/23/20*)	Imposes requirements relating to the collection and use of emergency health data and personal information and the use of technology to aid during the COVID-19 public health emergency; requires entities using technology to get consent from individuals	Emergency health data and personal information can never be disclosed in response to legal process or admissible in any judicial or administrative proceeding	Data to be collected at minimum level of identifiability reasonably needed De-identified information may be shared with public health authorities	Individuals have right to "opt in" to data collection Individual has right to correct any inaccuracies in information collected about them	Must implement security procedures that ensure confidentiality, integrity and availability of emergency health	Data deleted when purpose of transaction is satisfied or within 30 days, whichever occurs first Exposure notification information to auto-delete every 14 days

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
			and to disclose certain information including the right to privacy and who will have access to the data.			Privacy policy to clearly state what emergency health data or personal information is being collected, processed and disclosed, and for what reasons Must publish transparency report every 90 days	data and personal information Must limit access to such data to personnel whose use of the data is necessary to operate the program Must record who accessed data, date of access, and purpose of access Must hire neutral third party auditor to conduct annual protection audits	Right of action for violation; enforcement by attorney general
12.	NY	NY S08327 (*Recommit 8/11/20*)	Protects people's privacy during contact tracing by creating the crimes of unlawful dissemination of contact tracing information and unlawful use of a surveillance drone and requires certain privacy measures be implemented in contact tracing applications	Sets out conditions under which a person would be guilty of unlawful dissemination of contact tracing information or use of a surveillance drone		The use of applications created for the purpose of collecting contact tracing information must be voluntary. The user of any application must give explicit consent (which consent is revocable) to the application being downloaded, used, or providing any information	Any information stored or transmitted by an application shall be stored or transmitted in an encrypted manner as to prevent access by an unauthorized person. Any information collected by an	Any person in violation of these requirements who used an application involuntarily or without informed consent or who disclosed information improperly shall be liable to the person whose information was used.

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
						collected to any person. following receipt of a conspicuous, plain language explanation of the application.	application must be completely deleted, destroyed and erased and no further information may be collected after the state public emergency has ended.	
13.	NY	NY A10462 (*referred to health 5/18/20*)	Establishes the test, trust, and certify act to establish a protocol for COVID-19 testing, contact tracing, and immunity certification and to protect individuals' right to privacy	Pursuant to the protocol, information related or pertaining to an individual's immigration status, banking status, financial affairs, or criminal or policing record is to be deemed to be sensitive personally identifiable information, and not to be procured from the individual at any point throughout the tracing and certification process.			Applications or agencies supporting tracing, testing, and certification protocols must not require use of any centralized, third-party private platform or digital cloud infrastructure as central data storage for the purposes of implementing the protocol.	The collection and storage of tracing and certification data for the implementation of the protocol is to be supported using a decentralized database, in order to facilitate: (a) The protection of personal health records and individual identity, and the preservation of self-sovereignty over one's own personal biometric data; (b) The maximization of data integrity and security through encryption and verification of personal health records; and

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
								(c) Accessibility to published data and data provenance, to ensure the transparency of tracing data inputs.
14.	NY	NY A 687 *(Introduced to Assembly Health Committee on 1/6/21)*	Imposes requirements for the collection and use of emergency health data and personal information and the use of technology to aid during the COVID-19 public health emergency, requires entities using technology to get consent from individuals and to disclose certain information including the right to privacy and who will have access to the data.	The bill permits persons or applications collecting data ("Covered Entities") to obtain freely given, specific information from individuals to process their personal information or emergency health data. It would be unlawful for a Covered Entity to collect, process or disclose emergency health data unless it was freely and specifically given or it is to protect against malicious or illegal activity or to detect or respond to security incidents or threats. All emergency health data and personal information could only be collected at the minimum level identifiably reasonable for completion of the transaction disclosed and			All Covered Entities would be subject to annual data protection audits, conducted by a neutral third party auditor, evaluating the technology utilized and the development processes for statistical impacts on classes protected under section 296 of article 15 of the executive law, as well as for impacts on privacy and security as set out in the bill.	Emergency health data and personal information would need to be deleted when the initial purpose for collecting or obtaining such data is satisfied or within 30 days, whichever occurs first, except that proximity tracing or exposure notification data which shall be automatically deleted every 14 days. Emergency health data and personal information could be disclosed only as necessary to provide the service requested by an individual. A Covered Entity could share aggregate, de-identified data with public health authorities. The attorney general could bring an action in

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
				affirmatively consented to. A Covered Entity would need to provide the individual with a privacy policy at a fourth grade reading level or below and create transparency reports at least once every 90 days.				the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce the provisions of the proposed act.
15.	NY	NY S 8311 *(Introduced to Senate Committee on Internet and Technology on 5/11/20; Failed - Adjourned)*	Bans the use of facial recognition technology in the tracking of the coronavirus.	It would be unlawful for any person or any state agency, department, or office to obtain, retain, access or use facial recognition technology to track persons infected with or exposed to COVID-19.				

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
16.	OH	OH SB31 (*Passed House 5/28/20, Failed Senate 6/3/20; Sent to Conference Committee 9/16/20*) See also OH HB61 (*Passed Senate 6/10/20, Failed House 6/11/20; Sent to Conference Committee 8/27/20) which provided for same requirements.*	Imposes various restrictions on contact tracing.		Any contact tracing effort may not establish or authorize penalties for refusal to participate, including withholding medical treatment based on the refusal.	Records created during contact tracing are not public records.	Any contact tracing effort cannot be mandatory; participation to be voluntary and require written consent.	
17.	TX	TX HB888 (*Prefiled 12/21/20*)	Prohibits the use of location data obtained from mobile phones or other personal electronic devices for contact tracing		A health authority, or a contact tracer may not use location data obtained from a cell phone, or other device through which personal wireless services are transmitted, to identify or track directly or indirectly the movement of individuals for contact tracing purposes Law enforcement and other peace officers exempt; such data may be obtained by the	Individuals may voluntarily permit an agency to use wireless location data	Prohibits use of third-party data storage to keep available an individual's location data	

IV. PENDING OR PREVIOUSLY PROPOSED LEGISLATION								
	State	**Legislation (Bill, Status)**	**Summary**	**Data Privacy Protections**	**Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, Private Right of Action, etc.)**
					government with the issuance of a valid warrant			
18.	UT	H 5001 c (*failed 6/18/20 – House*)	Enact provisions relating to the collection, storage, use, and retention of certain electronic information or data related to COVID-19.		Prohibits collection of location information absent consent			Prohibits contractors from sharing data with anyone other than contracting government entity Contractors must implement and maintain procedures to prevent unlawful use or disclosure and destroy or de-identify records containing covered data

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
1.	AK	Website (No contact tracing app)	Alaska Department of Health and Social Services (DHSS) Covid-19 website states that information is confidential. "Case investigators and contact tracers are trained in HIPAA regulations and DHSS ensures private information of positive cases and close contacts is kept confidential. All users who have access to the disease surveillance system maintained by DHSS, where information from case investigation and contact tracing is kept, sign a confidentiality statement acknowledging restrictions on access."			
2.	AZ	Website (No contact tracing app)	Arizona Department of Health Services (DHSS) Covid-19 website states that contact tracing information is confidential. "All information obtained during case investigation and contact tracing activities are kept **private** and **confidential**."			
3.	AR	Website (No contact tracing app)	No statements specific to confidentiality of information.			
4.	CA	California Website Contact tracing program: CA Notify	California COVID-19 website states that contact tracing information will be kept confidential and that tracers will not ask immigration status. However, the privacy policy of the California Department of Public Health states that contact tracing information can be disclosed pursuant to a judicial order or warrant. "Your identity and health information that you provide to a contact tracer is always kept confidential. It will not be shared with anyone who may have been exposed." However: "Pursuant to California law, the information collected shall be confidential and shall be collected in a manner that protects your privacy. However, it			

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
			could be disclosed pursuant to a judicial order, judge-signed warrant, or to the California State Auditor."			
5.	CO	Website (Contact tracing program is CO Exposure Notifications)	Public health officials will not share an individual's information with other entities. "Only certain people at your local public health agency and the state health department can see your information. It is only used to reach out to your contacts with important information about testing and next steps. Public health will not share your information with other entities or outside organizations."			
6.	CT	Website (Contact tracing program is Covid Alert CT)	The Connecticut website describing contact tracing states that information will not be shared with police or immigration services. "The only purpose for collecting this information is to provide you, and the people you may have had contact with, information and resources to keep you and your community safe. Contact tracers will never: • Identify persons as the source of information within a community; • Give names or contact information to employers, the police, or immigration services."			
7.	DE	Website (Contact tracing program is Covid Alert DE)	The relevant state privacy policy states that protected health information can disclosed pursuant to a court order or subpoena or other legal demand. The Delaware Health & Social Services/Division of Public Health Notice of Privacy Practices, effective April 14, 2003, notes that personal information can be shared for various reasons, including: "For court order, or in some cases in response to a subpoena or other legal demand;" and "For law enforcement activities in limited situations, such as when there is a warrant for the request, or when the information is needed to locate a suspect or stop a crime…"		The exposure notification app disclosure states, "The COVID Alert DE app protects your privacy and does not collect or share any personal information that can identify you."	

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
8.	DC	Website (Contact tracing program is DC CAN)	Website does not appear to have specific privacy information re: contact tracing.			
9.	FL	Website (No contact tracing app)	The Florida Health website notes that "Public health professionals tasked with contact tracing are experts in protecting client confidentiality, counseling, cultural competency, and more."			
10.	GA	Website (No contact tracing app)	General statement regarding confidentiality of contact tracing information. "What you need to know about: COVID-19 Contact Tracing" states: "Contact tracing is confidential — the identity of the person who tests positive information about others who may have been exposed are kept confidential per HIPAA. (HIPAA is the law that protects an individual's personal health information.) Georgia's contact tracing does not use GPS or Bluetooth technology to track movements."			
11.	HI	Website	The Hawaii COVID-19 website provides an assurance of privacy of contact tracing information and includes a Q&A that states as follows: "Is the information I provide confidential? Yes. Your identity and health information is always kept private. It will not be shared with anyone who may have been exposed. No one will ask about your immigration status during testing, care or follow-up calls. You will never be asked for your Social Security number or payment information. Hawai'i's strict privacy laws protect your information. The Hawai'i State Department of Health maintains data with strict privacy and security storage standards. The data is only collected and stored for use by the Hawai'i Department of Health."	The Hawaii COVID-19 website includes a Q&A that states as follows:		No contact tracing app

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
12.	ID	Website (No contact tracing app)	Idaho websites do not appear to have any particular contact tracing-related privacy disclosures.			
13.	IL	Website	Private health information is secured and always kept completely confidential. No sensitive data like social security numbers is collected. Information not exchanged with anyone, including law enforcement, credit collection, or immigration agencies. Names always kept confidential and will not be revealed, even to close contacts.	Contact tracing is carried out primarily by the local health departments.	Data are anonymized and analyzed at an aggregate level – no individuals would be traced back with the data shared.	The Illinois Contact Tracing Collaborative was initiated in May, 2020. The program is advised by a non-profit, Partners in Health, a Massachusetts based organization.
14.	IN	Website	Discussions with health department staff are confidential. Personal and medical information will be kept private.	Contact tracing is done by state health department contact tracers		
15.	IA	Website	Information provided to contact tracers is protected by HIPAA Iowa Department of Health privacy policy and terms and conditions and states that "[y]our information will be protected and analyzed ONLY by those authorized access."	Contact tracing is done primarily through the "TestIowa" program, which is administered by the Department of Health and a third-party company.		The data being collected under the contact tracing initiative will only be retained in the short-term to aid the State of Iowa in responding to the pandemic. Until this pandemic is deemed "over" the state will continue to analyze the data."
16.	KS	N/A	No information provided.			

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
17.	KY	Website	Information will be kept completely private and only used for public health purposes. No confidential information released to the public. If you are a person with COVID-19, any people you name as potential contacts will not be told who they were exposed to. Health care providers are required to report anyone with a positive COVID test "or someone who is highly likely to have COVID-19" to the local health department.	Contact tracing is done by the Kentucky Department of Public Health and Local Health Departments.		Kentucky uses a third party platform to manage the information it collects.
18.	LA	Website	All personal information collected by the LDH Contact Tracing program is protected in accordance with the State of Louisiana's Personal Information Protection Laws, including R.S. 51:3074, using an array of administrative, technical and physical security measures. Information collected by LDH through the LDH Contact Tracing program via SMS may be shared as provided for by state and federal law, including local health departments and contractors for purposes of facilitating contact tracing and the support of COVID-positive individuals and their close contacts.	The Department of Health website urges cooperation but notes that it is not mandatory. The Louisiana Department of Health manages contact tracing. It uses text messaging to provide information, which the recipient can opt out of.		The state has contracted with call centers that hire contact tracers directly.
19.	ME	Website	Individuals can sign up for the Sara Alert system or if contacted by a contact tracer their information is entered into the system. The information is kept private "just like a medical record". Individuals may ask that their data not be entered into the system. Contact tracers will not ask for Social Security numbers, immigration status or financial information.	The Maine Center for Disease Control and Prevention handles contact tracing through the Situational Awareness Response Assistant ("Sara") Alert System "in collaboration with other facilities".		Information entered into the Sara Alert System is deleted 14 days after a person ends quarantine.

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
20.	MD	Website MD COVID Alert Privacy Policy	"Contact tracers take extreme measures to protect the privacy of infected patients and maintain strict adherence to HIPAA regulations." Contact tracers will never ask for Social Security numbers, financial information or "personal details unrelated to COVID-19".	Maryland local health departments conduct contact tracing and the state has also contracted with "NORC at the University of Chicago, one of the largest independent social research organizations in the United States, to assist in contact tracing efforts". Maryland also uses MD COVID Alert in conjunction with its contact tracing efforts.		MD COVID Alert uses Bluetooth to notify participants that they have been exposed to someone who has tested positive. It is voluntary and requires downloading an app (on Google or Apple) or by enabling Exposure Notifications on a phone having iOS 12.5 or higher and selecting Maryland as the region.
21.	MA	Website	The Department of Health's contact tracing program is assisted by the Commonwealth Health Connector Authority ("CCA"), the quasi-public entity that serves as the Affordable Care Act's state-based exchange. The data collected is input in the state's epidemiologic network, MAVEN. The "script" for contact tracers includes a statement that the "information [from the individual contacted] will be provided to the Department of Public Health and your local board of health. We will not share it with anyone else."	The state has a contact tracing program called the "Community Tracing Collaborative" ("CTC"). Its objective is to build a "scalable, tech-enabled Contact Tracing corps".	The MAVEN system uses the same encryption technology used by the banking industry.	In addition to the CCA, the state works with Partners in Health, a non-profit organization, in carrying out the CTC.
22.	MI	Website	"MDHHS never collects or processes any personally identifiable information from the MI COVID Alert app. However, if the app user receives a push notification that they may have been exposed, MDHHS may have the virtual agent ask the app user for their name and phone number. This information would be used to connect app users to their local health department and may be used to enroll app users in contact monitoring."	The Michigan Department of Health and Human Services ("MDHSS") manages contact tracing. The state also utilizes the MI COVID Alert, an app based on the Google and Apple Bluetooth		

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
				exposure notification technology. Use of the MI COVID Alert app is voluntary.		
23.	MN	Website	The state's COVID website states that "[p]rotecting the health privacy of people is critical to public health. It is also state law." Individuals who test positive for COVID receive a privacy notice when contacted by MDH and have the right to refuse to give any or all information to MDH. Information that is provided "is shared with local public health officials and other public health staff working on the COVID-19 response." Regarding disclosure, the website states that "[t]o protect the health and safety of others, MDH may sometimes need to share your name and that you tested positive for COVID-19 with your school, child care, or workplace if you work in a health care setting. MDH will try to reach you by phone first to explain why your name may need to be shared." Similarly, addresses but not the names of people who tested positive are shared pursuant to an executive order of the governor with 911 dispatch centers, if the person agrees. The website states that "[l]aw enforcement is not allowed to use these addresses for any investigations, and address information is removed from dispatch records when the person is no longer able to infect others."	The Minnesota Department of Health ("MDH") oversees contact tracing.		
		COVID aware MN Privacy Policy	Per the FAQ page for the app: "COVIDaware MN does not collect, use, or store any personal identifiable information or location data. COVIDaware MN is designed to protect your privacy. Neither your identity nor your location is shared with the Minnesota Department of Health or other users."	The app uses Bluetooth to notify participants that they have been exposed to someone who has tested positive. Downloading it is voluntary and it can be deleted at any time.		
24.	MS	N/A	No information provided			

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
25.	MO	Website	The COVID-19 Technology Response System has 3 components: (i) the Electronic COVID-19 Case Reporting System, where anyone required to report positive case information enters that information which flows into the second component "EpiTrax", (ii) EpiTrax is a disease surveillance system that receives laboratory results for COVID-19 tests and is used by DHSS and local public health authorities, and (iii) the Missouri Advanced Contact Tracing System ("MO ACTS"), which is a centralized contact tracing system shared between DHSS and local public health authorities. MO ACTS "allows users to call, text, or email contacts and schedule, track, and visualize contact tracing efforts".	The Missouri Department of Health and Senior Services (DHSS) manages software called the COVID-19 Technology Response System.		
26.	MT	N/A	No information provided.			Montana does not appear to have an official contact tracing app.
27.	NC	Website	NC Department of Health and Human Services ("NCDHHS") has adopted the SlowCOVIDNC Exposure Notification App. Through Bluetooth, phones around each other exchange anonymous tokes every few minutes. If a person tests positive, they may obtain a unique PIN to submit in the app, which notifies those who have been in close contact in the last 14 days. Tokens will collect and share date, time, signal strength and duration of proximity. No location data or personally identifiable data will ever be collected or stored. There is a SlowCOVIDNC Privacy Policy. In general, NCDHHS has stated that any information that is shared with the COVID-19 Community Team through contact tracing is a private health record and is strictly confidential. Personal information will not be shared with other government agencies, and the names of individuals and contacts will not be released or shared.	Using SlowCOVIDNC is entirely voluntary, and a user can enable or disable it at any time. SlowCOVIDNC app is not intended for children under the age of 13, and SlowCOVIDNC does not knowingly allow a child under 13 to use the app. If a person is between the ages of 13 and 17, they can only use SlowCOVIDNC app if their parent or legal guardian has reviewed and agreed to the Terms	After opting-in to receive notifications, the app will generate an anonymous token for a device, which is a string of random letters which changes every 10-20 minutes and is never linked to identity or location, but is linked to date.	Community Care of North Carolina, in partnership with NC AHEC, has been engaged by the NCDHHS to hire and train staff to support existing contact tracing efforts of local health departments in NC.

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
				of Service on their behalf.		
28.	ND	Website	North Dakota uses the Care19 Alert for contract tracing. A user's phone and the phones around it will work in the background to exchange IDs via Bluetooth and periodically checks all the random IDs associated with positive COVID-19 cases against its own list. If there's a match, the app will notify the user with instructions from the public health authority. With respect to the Exposure Notifications FAQs from Google (which the North Dakota Care19 page links to): • Each user must opt in and opt out at any time. • The Exposure Notifications System does not share location data from the user's device with the Public Health Authority, Apple, or Google • Random Bluetooth identifiers rotate every 10-20 minutes, to help prevent tracking. • Exposure notifications are only done on the user's device. In addition people who test positive are not identified by the system to other users, or to Apple or Google. • The system is only used to assist contact tracing efforts by public health authorities. • Google and Apple will disable the Exposure Notifications System on a regional basis when it is no longer needed.	Users must opt in.	Once a user opts in, the Exposure Notifications System will generate a random ID for their device. To help ensure these random IDs can't be used to identify the user or their location, the IDs change every 10-20 minutes.	If a user decides to participate, exposure notification data will be stored and processed on device. No data is shared with public health authority unless a user chooses to report a positive diagnosis or is notified they have come into contact with a positive individual.
29.	NE	Nebraska Department of Health and Human Services	Per Title 173 (Communicable Diseases) (requiring medical providers and laboratories to report cases of COVID-19 to the Health Department) the Department may release de-identified patient data on hospital encounters to a public health authority (e.g. US Centers for Disease Control and Prevention) to assist the agency in fulfilling its public health mission. These data shall not be re-released in any form by the public health authority without the prior authorization of the Department. Authorization for subsequent release of the data shall be considered only if the proposed release does not identify a patient, physician or provider.			Hospitals may submit data directly to the Department or through a third party acting as their agent. Providers selecting this option are responsible for ensuring that all terms

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
			If a person is diagnosed with COVID-19, someone from the health department may call to: (i) discuss who the person has been around; (ii) ask where they have spent time while they may have been able to spread COVID-19 to others. Discussions with health department staff are confidential. To protect and safeguard the health of the citizens of Nebraska the Director or the Director's designee may authorize the collection of information as to enable contact with a patient, physician or provider based upon data authorized and submitted under Title 173.			of Title 173 are met by the third party. There does not appear to be an official contact tracing app.
30.	NH	Website New Hampshire COVID-19 Case Investigation and Contact Tracing Plan	NH is not currently using proximity tracking technology (i.e., smartphones) to support contact tracing (as of June 24/20). Case investigation and contact tracing information are provided to the public in data reports via press releases and made available on the NH COVID-19 website. Additionally, DPHS maintains a data dashboard that provides aggregated information from state COVID-19 data systems. Data release guidelines are used to ensure data are aggregated at an appropriate level to prevent constructive identification of individuals. The dashboard, which will expand to include additional data and analyses over time, is available at: https://www.nh.gov/covid19/dashboard/summary.htm All aspects of case investigation and contact tracing must be confidential and culturally appropriate. Every person working the COVID-19 response is trained in privacy, security, confidentiality and HIPAA. All staff involved in public health COVID-19 Response activities with access to such confidential information sign a confidentiality agreement acknowledging the legal requirements not to disclose protected health information.	The NH Plan was developed by the New Hampshire Department of Health and Human Services ("DHHS"), Division of Public Health Services ("DPHS"), Bureau of Infectious Disease Control. Efforts to locate and communicate with cases and close contacts are carried out in a manner that preserves the confidentiality and privacy of all involved. This includes protecting the identity of the patient with COVID-19 when notifying a close contact, and not giving confidential information to third parties (e.g., roommates, neighbors, family members) unless	Per the NH Plan, DPHS data and security protocols include requirements for password-protected computer access, as well as locked, confidential storage cabinets and proper shredding and disposal of notes and other paper records. Protocols include instructions for the protection of confidential data and confidential conversations in remote or offsite work locations (e.g. home) such as requirements to make phone or video-conferencing calls from a private location). Approaches to ensuring confidentiality and data security are included in staff training.	

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
				authorized to do so by law or patient consent.		
31.	NJ	NJ COVID-19 Information Hub COVID Alert NJ Data and Privacy Policy and Notice.	COVID Alert NJ does not use, track, or collect any geolocation or GPS data. Alerts do not share the identities of other users to one another, the New Jersey Department of Health, or any other entity. The random codes exchanged between phones cannot be associated with a specific person and change every 10-20 minutes to help preserve anonymity. The app also does not share the identity of positive cases with other app users or with Google or Apple.	The app is voluntary and may be uninstalled. Users must be at least 18 years old.		The app does not collect or store personal information including name, date of birth, address, phone number, email address or location in order to show exposure notifications. The following data processors provide services to the app: NearForm, Amazon Web Services and the Association of Public Health Laboratories.
32.	NM	N/A	No information provided.			City of Santa Fe is encouraging the use of NOVID contact tracing app.
33.	NV	Website COVID Trace Nevada Privacy Notice	The Nevada Department of Health and Human Services (the "DHHS") developed COVID Trace, a contact tracing mobile app that uses the Exposure Notifications System from Google and Apple. The app exchanges anonymous information with other phones in a person's vicinity using Bluetooth and can notify a person if they've come in contact with someone who has tested positive for COVID-19. The Exposure Notifications System does not collect or use the location from your device. It uses Bluetooth, which can be used to detect if two devices are near each other - without revealing where the devices are. The system does	COVID Trace app only works if a person opts in. Once opted in, a person can change their mind and turn it off at any time.	All data stored by the app on a user's phone is encrypted using the built-in encryption capability of each user's phone. Data is also encrypted when it is uploaded to State of Nevada servers.	Diagnosis keys and associated information is retained for 14 days. Upon confirmation of a match check, the information is deleted. Anonymous app metrics are retained by the State of Nevada for

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
			not share a person's identity with other users, Google, or Apple. Access to the technology is only granted to apps from public health authorities. These apps must meet specific criteria around privacy, security, and data use. The State of Nevada anonymizes any app metric data that it receives from app users. This anonymized data is shared with the DHHS. The DHHS will carry out statistical analysis on the data shared with it, which it will publish in line with its remit Department of Health, the Health Response, the State of Nevada, and to the public as appropriate.		The Contact Tracing feature uses a fully 'decentralized' privacy model, meaning that key and diagnosis key matches are made locally on user's phones. Matches are not made externally by the State of Nevada. This ensures there is no tracking of users' movements or contacts. The State of Nevada servers also use data encryption, modern firewalls and intrusion prevention.	a minimum of seven years and reviewed at that stage for extension or deletion depending on its health value. The Data Privacy Notice may be modified from time to time and once modified users will receive notification that this Data Privacy Notice has been updated through the app.
34.	NY	Website	New York State has partnered with Bloomberg Philanthropies, Johns Hopkins Bloomberg School of Public Health and Vital Strategies to create the NYS Contact Tracing Program. COVID Alert NY is a voluntary, anonymous, exposure-notification smartphone app. Users will get an alert if they were in close contact with someone who tests positive for COVID-19. The app will never collect, transmit or store your personal information and is completely anonymous. Location is never tracked. The app uses Bluetooth technology to sense when another person with the same app comes within 6 feet. A user's phone exchanges a secure code with the other phone to record that they were near. The full Data and Privacy Policy can be accessed directly within the app settings screen.	The app is voluntary and requires opt-in. A user can delete their personal information at any time. A user can choose to opt-out of sharing certain app metrics data at any time. Users must be aged 18 or older.	According to the NYS Department of Health ("NYSDOH") website, an app user's phone automatically shares the phone's IP address with the back-end server to log exposures. The app will use the IP address in its communication with the server to request exposure information but does not collect or store the phone's IP address itself. The server also does not store a user's IP address. This process ensures anonymity with all app users.	A limited set of aggregate app health metrics data is also generated from using the app and shared with the NYSDOH to supplement the contact tracing process. Any aggregate contact tracing data shared with NYSDOH from the app cannot be used to identify any individual app user. Any user that downloads the app from the Apple App Store or Google Play Store is subject to

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
						Apple and Google's overall app store privacy policies. New York is working with Delaware, Pennsylvania, and New Jersey to ensure that the apps will work across state lines.
35.	OH	N/A	Limited information available on the Ohio Department of Health COVID-19 Contact Tracing page. There does not appear to be a contact tracing app.			
36.	OK	N/A	Oklahoma County Health Department ("OKHC")links to CDC page regarding contact tracing, but did not otherwise directly address this. OKHC announced there will be a contact tracing app, but information is not readily available.			
37.	OR	N/A	OHA states that in the context of contact tracing, local public or tribal health will reach out to a person's contacts and ask them to quarantine. Their privacy will be protected, and their contacts will not be told the identity of the COVID-positive person. OHA further states that this information will be treated like a private medical record that is strictly confidential and will not be shared with other agencies, including immigration officials. Oregon Health Authority ("OHA") is developing OR Exposure Notification Application, but it does not appear to be ready yet			

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
38.	PA	Website	Pennsylvania Department of Health ("PDOH") released COVID Alert PA which uses the Exposure Notification System provided by Apple and Google. When someone receives a positive diagnosis, they will receive a call from the PDOH, their county, or municipal health department and if they have the COVID Alert PA app on their phone, they will be asked if they are willing to enter a 6-digit validation code in the app. Once this is entered, the person will be given the option to share their random Bluetooth keys with other app users. Other app users' phones routinely check if they have ever been in close contact (e.g., within six feet for fifteen minutes or more) with a phone that shared those same Bluetooth keys. If there is a match, the app will let them. The app never collects or reveals the identity of any person using the app, and never reveals who has been diagnosed as positive for COVID-19. The app will never collect, transmit, or store personal information and is completely anonymous.	Use of the app is voluntary requires opt in. People 13 years old and older are encouraged to add the app to their phone to the fight. However, if a person is between the ages of 13 and 17, they must have a parent or legal guardian's consent to use the app.	The app does not use GPS, location services, or any movement or geographical information.	The following third-party companies provide services to the App for DOH: NearForm - the App developer that provides technical support and maintains the server that generates and verifies the validation codes; Amazon Web Services- provides cloud storage and cloud services for the symptom check-in data submitted; and Association of Public Health Laboratories - provides a national server for seamless interstate data sharing of diagnosis keys, which uses Microsoft Azure for cloud storage.
39.	PR	N/A	No information provided			
40.	RI	Department of Health Website:	Discussions with health department staff are confidential and will only be shared on a need-to-know basis, e.g., with a health care provider Name will not be shared with contacts			

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
		Contact Tracing	No questions regarding immigration status			
		Crush COVID RI app Privacy Policy	Pandemic response app, including features such as a location diary and symptom diary No personally identifiable information is stored in the app; opting in to sharing My Location Diary allows RI DOH staff to see the copy of the diary specifically associated with that user Data owned by users Personal/identifiable information never shared with contacts or any third parties (unless they are authorized contact tracing personnel or if sharing such information is legally required) Access limited to RI DOH staff trained in disease investigations and contact tracing GPS location data only used for public health purposes	Participation voluntary; users may opt to share GPS location data with RI DOH following a positive test result	Information stored locally on each device and may only be shared with RI DOH with user opt-in consent and permission Shared data stored anonymously on secure servers licensed by the State of Rhode Island	Users may dele app or location data in the app at any time Location data automatically deleted from each user's phone after 20 days
41.	SC	Department of Health Website: Contact Tracing	Participation is voluntary and confidential Contact tracers will not ask about immigration status Name and personal information not shared with contacts			
42.	SD	Department of Health Website: Contact Tracing	Information to be kept confidential; name will not be shared with contacts Information to be stored by health department and is subject to HIPPA			

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
		Care19 Diary App	Location logging app to facilitate disease investigation process should you test positive for COVID-19 Participation voluntary; users may opt out at any time App users assigned a unique Care19 Diary ID number that is not associated with any name, contact information or credit card Information is 100% anonymous; to be used in aggregated form Users may consent to make location data available to SD Dept of Health upon testing positive		Compliant with California Consumer Privacy Act	Users may delete app and any data collected by the app at any time
43.	TN	N/A	No information provided			
44.	TX	Department of Health Website: Contact Tracing Overview FAQ (Texas Health Trace – online system)	Information to be kept confidential and used for public health purposes only; will not be shared with contacts Information supplied through Texas Trace is confidential and to be used solely for public health	Participation voluntary		
45.	UT	Department of Health Website: Contact Tracing	Information considered private health information and will not be made public or shared with contacts Access restricted to Health Department		Information stored on secure database	

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
		Healthy Together App	Public health officials will only receive access to necessary health data Personal information only accessible by public health officials and a limited number of developer employees Utah may investigate GPS and location data to help understand transmission zones Only data required to combat COVID-19 will be shared with public health officials; no information shared outside the state	Participation voluntary Users own their data and may delete it at any time	Data protected by network security and State data security measures	Symptom data automatically deleted or de-identified after 30 days Developer must comply with State requirements for data security and encryption
46.	VT	Department of Health Website: Contact Tracing (no app)	Information will only be used to prevent the spread of COVID-19 Contact tracer does not enforce rules; "you will not get in trouble if you gathered with people or did not follow protocols"			
47.	VI	Department of Health Website: Contact Tracing	Information to be used only by public health and subject to strict confidentiality Contact tracers will not ask about immigration status COVIDWISE app generates anonymous tokens for each device that changes every 10-20 minutes Absent express consent, name or medical records will not be shared with contacts		Information protected in a secure system	
		COVIDWISE: official exposure	COVIDWISE does not collect, use or store any personal identifiable or location data Neither identity nor location shared with other users	Participation voluntary; positive test results accompanied by VDH-issued PIN that is required to be submitted		Participation may be terminated at will by deleting or uninstalling app from mobile device

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
		notifications app Privacy Policy FAQ	COVIDWISE app generates anonymous tokens for each device that changes every 10-20 minutes Does not collect geolocation or GPS data	when reporting a positive test result in COVIDWISE		
48.	WA	Department of Health Website: Contact Tracing	Information used only by public health agencies and individual information kept confidential Contact tracers will not ask about immigration status		Information protected in a secure system	
		WA Notify (Exposure Notification App) Privacy Policy	Random codes shared via Bluetooth between devices of WA Notify users when they are near each other Public Health will provide verification code together with a positive test result to input result into app Participation voluntary; no information will be shared unless user chooses to enter a verification code Automatically-generated logs used only for troubleshooting; do not include random codes or test result verification codes and cannot be used to tie either code back to you or your device Enabling additional analytics allows for limited aggregate data to be shared with public health for app improvements; does not include any personal information; enabling analytics is voluntary and can be turned off in the app WA Notify does not collect smartphone location data and does not collect or share information tying you or your smartphone to random codes or positive test result verification codes		WA Notify protects random codes using Google and Apple's Exposure Notification Framework Codes only stored on each device, not by WA Notify	Codes stored on each device for a maximum of 30 days Logs automatically deleted after 7 days Uninstalling app deletes all random codes stored on smartphone

V. STATE COVID-19 WEBSITES AND CONTACT TRACING APPS						
	State	**Source**	**Data Privacy Protections and Use Restrictions**	**Transparency, Consent and Access**	**Security, Encryption and De-Identification**	**Miscellaneous (Data Retention, Third Party Contractors, etc.)**
49.	WV	Department of Health Website: Close Contacts (no app)	Personal medical information is confidential; name will not be shared with contacts			
50.	WI	Department of Health Website: Contact Tracing	Information is confidential; name will not be shared with contacts Compliant with HIPPA and with the Wisconsin Electronic Disease Surveillance System (WEDSS)			
		WI Exposure Notification (launching 12/23/20)				
51.	WY	Department of Health Website: Contact Tracing (links to CDC Website)	Information is confidential and personal and medical information only shared on a need-to-know basis Names will not be shared with contacts			
		Care19 Alert and Diary Apps: FAQ	Care19 Alert uses information submitted through Care19 Diary to alert users of potential COVID-19 exposure No personal information collected; users may voluntarily and anonymously share positive test results			

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT