Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

"Tracing Papers": A Comparison of COVID-19 Data Privacy Bills

June 22, 2020

As COVID-19 continues to spread, many public health authorities are turning to *contact tracing*—measures to identify, notify, and monitor infected individuals' contacts—to track potential COVID-19 exposure. Along with conventional techniques, technology companies, including Google and Apple, are developing digital contact-tracing and exposure notification tools. In addition, Congress has appropriated emergency funds to help facilitate contact-tracing efforts. But the idea of using personal information—including cell phone and location data—to track COVID-19 exposure has prompted groups such as the ACLU to raise privacy concerns and call for the protection of individuals' privacy and anonymity.

In response, Members of Congress have introduced four data privacy bills addressing digital contact-tracing and exposure notification:

- the COVID-19 Consumer Data Protection Act of 2020 (CCDPA), S. 3663, introduced by Senators Roger Wicker, John Thune, Jerry Moran, Marsha Blackburn, and Deb Fischer on May 7, 2020;
- the Public Health Emergency Privacy Act (PHEPA), companion bills S. 3749 and H.R. 6866, introduced, respectively, by Senators Richard Blumenthal and Mark Warner and Representatives Anna Eshoo, Janice Schakowsky, Suzan DelBene, Yvette Clarke, G.K. Butterfield, and Tony Cardenas on May 14, 2020; and
- the Exposure Notification Privacy Act (ENPA), S. 3861, introduced by Senators Maria Cantwell and Bill Cassidy on June 1, 2020.

This Sidebar describes the main components of each bill and examines key differences among the proposals before identifying several issues for Congress. For a general background on contact-tracing technology, see CRS In Focus IF11559, *Digital Contact Tracing Technology: Overview and Considerations for Implementation*, by Patricia Moloney Figliola. For a discussion of Congress's authority to regulate the privacy of state-collected contact-tracing data, see CRS Legal Sidebar LSB10502, *Constitutional Authority to Regulate the Privacy of State-Collected Contact-Tracing Data*, by Edward C. Liu. For an overview of existing federal privacy laws, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh. For a comparison of general data privacy legislation in the 116th Congress, see CRS Legal Sidebar LSB10441, *Watching the Watchers: A Comparison of Privacy Bills in the 116th Congress*, by Jonathan M. Gaffney.

Congressional Research Service
https://crsreports.congress.gov
LSB10501

Key Provisions and Major Differences

The CCDPA, PHEPA, and ENPA would each take a similar approach to regulating contact-tracing data. Under each bill, a *covered entity* would have to take certain steps before and after collecting *covered data*, and each bill would grant certain rights to individuals over collected data. In addition, each bill would create enforcement mechanisms to ensure covered entities comply with their obligations with respect to covered data. But the bills contain several major differences, including the types of entities they cover and the precise rights they afford to individuals. While the CCDPA and PHEPA apply specifically to the current COVID-19 pandemic, the ENPA is not limited to the current public health emergency. The ENPA, however, applies only to data collected by an *automated exposure notification service*, which it defines as a tool for "digitally notifying, in an automated manner, an individual who may have become exposed to an infectious disease." The key provisions of each bill are discussed below, and **Table 1** summarizes their main differences.

Covered Data

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

Covered Entities

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

Covered Entities' Obligations

The bills would each impose obligations on covered entities with respect to covered data. Each bill would require a covered entity to

- not *disclose* or *transfer* an individual's data for any purposes other than those enumerated in the bills (CCDPA § 3(a), (b); PHEPA § 3(a), (c); ENPA § 5);
- publish a *privacy policy* to provide *notice* as to the type of data the entity collects, the purpose of the collection, how the entity will use collected data, and an individual's rights with respect to the data (CCDPA § 3(c)(1); PHEPA § 3(e); ENPA § 4(b));
- obtain an individual's *affirmative express consent* before collecting that individual's data (CCDPA § 3(a); PHEPA § 3(d)(1); ENPA § 4(a));

- Provide an individual with the right to *opt out* of collection by withdrawing consent (CCDPA § 3(d); PHEPA § 3(d)(2); ENPA § 4(a)(1)(B));
- *delete* an individual's data on request or after a set period, such as the end of the COVID-19 emergency under the PHEPA or on a 30-day rolling basis under the ENPA (CCDPA § 3(e); PHEPA § 3(g); ENPA § 6); and
- *safeguard* an individual's data by adopting appropriate data security measures (CCDPA § 3(h); PHEPA § 3(b); ENPA § 7).

Along with these obligations present in all three bills, there are several additional protections common to two of the three bills. For example, both the CCDPA and PHEPA require covered entities to *minimize* the data they collect and to provide a mechanism for an individual to *correct* inaccurate data. Also of note, the PHEPA and ENPA prohibit discrimination against an individual based on covered data.

Enforcement

All three bills would vest enforcement with the FTC through agency and judicial proceedings. The bills would also allow state attorneys general to enforce the bills' provisions in court. The PHEPA would provide a new *private right of action* that would allow individuals to sue covered entities for violations. And the ENPA would preserve an individual's ability to use existing remedies under federal or state law to enforce its provisions.

Relationship to State Laws

Both the PHEPA and ENPA explicitly provide that their provisions would not preempt or supersede any state laws. In contrast, the CCDPA would prohibit states from adopting or enforcing any laws or regulations governing the use of covered data.

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

Provision	CCDPA, S. 3663	PHEPA, S. 3749 and H.R. 6866	ENPA, S. 3861
Covered Data—			
In general	*Covered data*: "precise geolocation data, proximity data, a persistent identifier, and personal health information" (§ 2(6)(a))	*Emergency health data*: "data linked or reasonably linkable to an individual or device, including [derived] data . . . that concerns the COVID-19 health emergency" (§ 2(8))	*Covered data*: "any information that is . . . linked or reasonably linkable to an individual . . . collected, processed, or transferred in connection with an automated exposure notification service" (§ 2(6))
Exclusions	Aggregate data, business contact information, de-identified data, employee screening data, and publicly available information (§ 2(6)(b)); data related to individuals permitted to enter a covered entity's physical location (§ 2(12))	Data that is not "linked or reasonably linkable" to an individual or device (§ 2(8))	Data that is not "linked or reasonably linkable" to an individual or device, including aggregate data (§ 2(6))

Provision	CCDPA, S. 3663	PHEPA, S. 3749 and H.R. 6866	ENPA, S. 3861
Covered Entities—			
In General	Any entity or person engaged in contact tracing that is subject to the FTC Act, a common carrier, or a nonprofit (§ 2(7))	Any entity or person engaged in contact tracing, including government entities (§ 2(4)(A))	An operator of an automated exposure notification service that is subject to the FTC Act, a common carrier, or a nonprofit (§§ 2(11), 10(a)(4))
Exclusions	Service providers (§ 2(7)(C))	Health care providers; persons engaged in de minimis collection; service providers; persons acting in their individual or household capacity; and public health authorities (§ 2(4)(B))	Public health authorities (§ 2(11))
Non-Discrimination	No protections	Covered entities must adopt reasonable safeguards against discrimination (§ 3(a)(3)); government entities may not use data to interfere with voting rights (§ 4)	Prohibits discrimination by any person or entity based on covered data (§ 8)
Enforcement	FTC; state attorneys general (§ 4(a), (c))	FTC; state attorneys general; new private right of action (§ 6)	FTC; state attorneys general; existing private rights of action (§ 10)
Preemption	Preempts state laws and regulations governing covered entities' use of covered data (§ 4(b)(3))	Adopts reasonable safeguards to prevent unlawful discrimination on the basis of emergency health data, but does not "preempt or supersede" other federal or state laws or regulations (§ 7)	Does not "preempt, displace, or supplant" state laws (§ 10(c))
Effective Period	Date of enactment through the last day of the COVID-19 public health emergency (§ 2(8))	Thirty days after enactment through the end of the COVID-19 public health emergency (§§ 2(13), 8)	Indefinitely, beginning on the date of enactment (§ 10(g))

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

Considerations for Congress

As state and local authorities consider whether to implement digital contact tracing or exposure notification to combat the COVID-19 pandemic, Congress may consider whether to enact a law governing the use of contact-tracing data to ensure uniformity and safeguard individuals' personal data. If Congress takes no action, digital contact-tracing and exposure notification solutions may be subject to existing federal and state privacy protections, including the Health Insurance Portability and Accountability Act (HIPAA) regulations and the California Consumer Privacy Act (CCPA). But existing federal privacy laws do not protect all contact-tracing data, and state laws—where they exist—impose a patchwork of requirements.

The CCDPA, PHEPA, and ENPA share a number of common provisions, suggesting some level of accord on how to regulate entities engaged in contact tracing. But the differences among the bills could make it difficult to reach agreement on final legislation. Two of the biggest divergences among the bills—whether to include a private right of action and whether to preempt state law—mirror differences in general data

privacy bills introduced at the end of 2019 and earlier this year. Those provisions were "key sticking point[s]" in the debate over general-applicability data privacy legislation, and Congress has yet to reach a consensus. To move forward with a contact-tracing privacy bill, Congress may have to reach a compromise with respect to these issues.

Author Information

Jonathan M. Gaffney
Legislative Attorney

Disclaimer