Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Constitutional Authority to Regulate the Privacy of State-Collected Contact-Tracing Data

June 26, 2020

Amid the ongoing COVID-19 pandemic, several states have developed and promoted contact-tracing mobile device apps to identify individuals who may have had contact with infected persons. Additionally, the two largest manufacturers of mobile device operating systems, Apple (iOS) and Google (Android), have announced plans to release application programming interfaces (APIs) to "enable interoperability between Android and iOS devices using apps from public health authorities."

Several bills in the 116th Congress would regulate the privacy of information collected through such contact-tracing apps. (For a detailed comparison of these bills, see CRS Legal Sidebar LSB10501, *"Tracing Papers": A Comparison of COVID-19 Data Privacy Bills*, by Jonathan M. Gaffney.)

- S. 3663, the COVID-19 Consumer Data Protection Act of 2020, would (1) require certain covered entities that collect contact-tracing information to provide individuals with prior notice of such collection and the opportunity to opt-in to such collection; (2) prohibit the use of such information for purposes unrelated to tracking the spread of COVID-19; and (3) require covered entities to publicize their privacy and data security practices.
- S. 3749 and H.R. 6866, the Public Health Emergency Privacy Act (PHEPA), would prohibit certain entities from disclosing contact-tracing information for purposes unrelated to public health. The bill would also prohibit such information from being used for commercial advertising or marketing purposes, or to discriminate against individuals with respect to "goods, services, facilities, privileges, advantages, or places of accommodations." Covered entities include state governmental entities, although PHEPA specifically exempts public health authorities.
- S. 3861, the Exposure Notification Privacy Act (ENPA), requires operators of "automated exposure notification systems" (AENS) to limit enrollment in such systems to individuals who have provided affirmative express consent, to publicize the system's privacy policy, and to limit transfers of covered data to the minimum necessary to notify other users or a public health authority of potential exposures. ENPA also requires operators of an AENS

Congressional Research Service
https://crsreports.congress.gov
LSB10502

> to establish data security practices to protect the confidentiality, integrity, availability, and accessibility of covered data.

In general, the bills above limit coverage to entities subject to the jurisdiction of the Federal Trade Commission or explicitly exempt state public health authorities. Nevertheless, during the debate surrounding this legislation, questions may arise over Congress's authority to regulate state governments' collection and dissemination of the relevant information. As context for that potential debate, this Legal Sidebar examines constitutional limitations on Congress's regulation of state activity, particularly in the context of applying federal privacy protections to state-held information.

Federalism and the Anticommandeering Doctrine

Unlike the state governments, which enjoy a general police power, the federal government is limited to those enumerated powers provided to it in the U.S. Constitution. One such power that is particularly relevant to the instant analysis is the Constitution's Commerce Clause, which allocates to Congress the power "[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." The Supreme Court has interpreted the Commerce Clause as authorizing Congress to regulate "the channels of interstate commerce, persons or things in interstate commerce, and those activities that substantially affect interstate commerce."

Legislation that falls within the bounds of the Commerce Clause may still be unconstitutional if it breaches "the principles of federalism contained in the Tenth Amendment," which provides that "[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." Whether the Tenth Amendment restricts Congress's authority to impose generally applicable regulations on the activities of states and their instrumentalities has been an ongoing debate since the latter half of the 20th century.

Legal Background

In 1974, the Court decided *National League of Cities v. Usery*, holding that Congress may not use the Commerce Clause to dictate "how essential decisions regarding the conduct of integral governmental functions are to be made." But the Supreme Court expressly overruled *National League of Cities* in its 1985 decision in *Garcia v. San Antonio Metropolitan Transit Authority* after efforts to define the scope of "integral governmental functions" proved "both impracticable and doctrinally barren." On the other hand, following *Garcia*, the Court held in two cases that Congress violates the Tenth Amendment when it commandeers states to enact or administer a federal regulatory program. In *New York v. United States*, the Court struck down a federal law that compelled states "to provide for the disposal of the radioactive waste generated within their borders." Similarly, in *Printz v. United States*, the Court invalidated a provision of federal law that required "state and local law enforcement officers to conduct background checks on prospective handgun purchasers."

Regulating State Databases

After the *New York* and *Printz* decisions, the Supreme Court decided *Reno v. Condon* in 2000, a Tenth Amendment challenge to the Driver's Privacy Protection Act (DPPA). The DPPA generally restricts the sale and disclosure of personal information held by state motor vehicle departments (DMVs) without an individual's consent. The DPPA also restricts the resale and redisclosure of drivers' information by private parties who have obtained that information from a state DMV.

After first holding that the Commerce Clause properly encompassed the sale or disclosure of such personally identifiable information as a "thing in interstate commerce," the Court found no Tenth

Amendment concerns with the federal statute. Distinguishing the DPPA from the statutes struck down in *New York* and *Printz*, the Court held that

> the DPPA does not require the States in their sovereign capacity to regulate their own citizens. The DPPA regulates the States *as the owners of data bases*. It does not require the South Carolina Legislature to enact any laws or regulations, and it does not require state officials to assist in the enforcement of federal statutes regulating private individuals. We accordingly conclude that the DPPA is consistent with the constitutional principles enunciated in *New York* and *Printz*.

Most recently, in 2018, the Court's decision in *Murphy v. National Collegiate Athletic Association* reaffirmed the principle set forth in *Reno* that "[t]he anticommandeering doctrine does not apply when Congress evenhandedly regulates an activity in which both States and private actors engage."

Analysis

Questions about Congress's authority to regulate the privacy of information collected by state public health departments through contact-tracing apps are seemingly similar to those the Supreme Court addressed in *Reno v. Condon*. As noted above, the Court in *Reno* first concluded that pieces of personal information collected by state DMVs were "things in interstate commerce" that fell within the Commerce Clause's scope. Under this reasoning, courts would likely consider the information collected by state public health departments through contact-tracing apps to likewise be "things in interstate commerce" subject to federal regulation under the Commerce Clause.

In addition, *Reno* appears to suggest that the Tenth Amendment is generally not an obstacle to federal regulation of the sale and disclosure of personal information collected through contact-tracing apps if such regulation is applied "evenhandedly" to both state and private holders of this information. The rationale under which the *Reno* Court upheld the DPPA's privacy requirements—that the statute "does not require the States in their sovereign capacity to regulate their own citizens" but merely "regulates the States as the owners of data bases"—appears to be equally applicable to security and interoperability requirements imposed on public and private custodians of contact-tracing data. Consequently, applying the Court's reasoning in *Reno*, so long as such federal regulation of contact-tracing apps applies evenhandedly to both state and private actors, and does not also require states to enact legislation or refrain from enacting legislation, it would likely not raise constitutional issues under the Tenth Amendment.

Author Information

Edward C. Liu
Legislative Attorney

Disclaimer