ACT | The App Association

Filling in the Gaps Between Federal Privacy Silos

Healthcare privacy. As policymakers consider federal privacy legislation, there are known tradeoffs between keeping personal healthcare data private and making it portable. A long history of tension exists between privacy and portability in the health system, since portability requires entities to enable access to personal information, while privacy requirements require safeguards against unwarranted processing and disclosure. For example, people often assume that the "P" in the Health Insurance Portability and Accountability Act (HIPAA) stands for "privacy." This misconception is notable and ironic because of the conflicting purposes of portability and privacy. Meanwhile, the HIPAA privacy regulations promulgated by the Department of Health and Human Services (HHS) lack a foundation in statute. When Congress enacted HIPAA, it included a shot clock for Congress to set forth a privacy rule roadmap, but because Congress failed to do so by a certain date, HHS received the green light to design the so-called HIPAA "privacy rule" without the roadmap. In other words, HIPAA was not designed to give consumers more control of their healthcare data, it was drafted primarily to address the healthcare system's portability problem. That Congress legislated on portability, but not privacy, when it enacted HIPAA helps explain why the law would be suboptimal as a set of privacy mandates beyond the healthcare system.

Nonetheless, there remains a coverage gap, because HIPAA's privacy, security, and portability requirements only apply to protected health information collected and processed by "covered entities," which (most relevantly) include health providers that electronically transmit insurance claims. So, what should Congress do to address the growing universe of healthcare data HIPAA doesn't regulate? **Instead of stretching HIPAA beyond its current limits to address healthcare privacy, a new privacy law should subject healthcare data not otherwise subject to HIPAA to stricter requirements as part of a sensitive subset of personal information.**

Other federal privacy silos. Aside from HIPAA, there are a handful of other federal privacy regimes, including the Graham-Leach-Bliley Act (GLBA), which applies to "financial institutions;" the Children's Online Privacy Protection Act (COPPA), which mainly regulates the collection (and to a lesser extent, the processing or sharing) of data about children under 13, and applies to the general economy, but not to entities or data subject to other regimes like HIPAA, GLBA, or the Family Educational Rights and Privacy Act (FERPA), which regulates how schools receiving federal funds—and their contractors—treat students' education records. Around the edges of these laws, there are inevitably gaps in coverage where collection, processing, and transfer of data occurs in a manner that is for one reason or another not subject to these otherwise comprehensive privacy laws. **A privacy law of general applicability should mainly carve itself around these pre-existing regimes while subjecting the activities not otherwise subject to a federal law to a set of strong privacy requirements, thus filling the gaps.** However, to the extent Congress seeks to augment or update COPPA as part of this broader effort, it should also modernize COPPA's verified parental consent requirements.

Time is of the essence. Congress should not further delay a general federal privacy law for two main reasons, among others: 1) the states continue to enact privacy laws of the same scope, leading to inevitable incongruity between even seemingly consistent state laws; and 2) federal agencies are acting to fill the gaps, leading to confusion and agency overreach. On the first point, even recently-enacted privacy laws of general applicability in Colorado and Virginia—

though they have the same basic structure and general approach—include small differences that result in inconsistent compliance requirements. Compliance with state laws is, unfortunately, not simply a matter of complying with the "strictest" law on the books to ensure compliance with the others—they do not stack neatly together like Russian dolls. For example, Virginia's definition of "sensitive data" subject to stricter requirements is broader than Colorado's because it includes "precise geolocation data"—but Colorado includes slightly stricter requirements in other parts of the bill. Therefore, a company's compliance with both is not simply a matter of complying with the stricter of the two regimes, it involves designing a compliance program that fits Colorado for some aspects of it and Virginia for others. And if the company has enough California resident customers, it might need to design some of its compliance program to fit California's law in addition to Colorado or Virginia. From the company's perspective, this could mean that some parts of its program must fit California's *instead* of Colorado or Virginia, insofar as California's requirement is stricter than, but consistent with the other two, in order to fully comply with all three regimes.

To the second point, we have already seen an example of a federal agency seeking to fill the privacy gap in a controversial way. In a 2009 update to HIPAA, Congress required the Federal Trade Commission (FTC) to adopt rules penalizing vendors of personal health records not otherwise subject to HIPAA for failure to give timely notice to consumers of a "breach of security" of information about them. In September 2021, the FTC issued a policy statement interpreting the obligation to notify consumers of a security incident to mean that the FTC could bring cases against vendors for *purposeful* disclosures to third parties if those disclosures are unauthorized. Neither the statute nor the rule authorizes the FTC to punish companies in this context, so it would be surprising if courts allow the new interpretation to stand, which would leave consumers where they started—without adequate federal privacy protection of their healthcare data. But in the meantime, companies in the crosshairs must take the FTC's intentions seriously. After all, the FTC is working with the tools Congress has given it, which are inadequate to the task in this case. From our perspective, the answer is not for the FTC to create novel and tenuous interpretations of its existing rules nor is it to extend HIPAA to cover healthcare tools and services not currently subject to HIPAA. Congress must enact a single, federal law mandating that companies honor consumer privacy rights.

Policymakers Should Keep the Following Considerations in Mind in Crafting Any Changes to Federal Privacy Law:

- **Carve Out Existing Privacy Regimes Like HIPAA, GLBA, and FERPA.** Congress' principal privacy imperative is to establish requirements with respect to data and entities not otherwise subject to the existing regulatory silos. Congress established those laws separately and updating them deserves its own, separate set of inquiries.
  - **COPPA.** Thanks to recent revelations around the impacts of social media on children and teens, there is momentum in Congress behind updating or expanding COPPA. If such an update is part of broader privacy reform, it should also modernize the outdated verifiable parental consent construct.
- **Transparency, Access, and Control for Consumers.** Federal privacy requirements should require companies to honor reasonable consumer rights to transparency; access to data about themselves; the opportunity to correct information about themselves; the ability to seek deletion of data about themselves; and the right to object to transfer. They should also impose reasonable limitations on processing activities and adopt risk assessment provisions similar to those enacted in Colorado and Virginia. App Association members compete on privacy and work hard every day to develop better ways to communicate with their users about privacy and give them meaningful choices. **With the age of opaque behavioral advertising activities—and the manipulation-driven social media surveillance that feeds it—wearing out its welcome, Congress now has an opportunity to redirect services back to a consumer that is sick of being a product. A federal framework giving consumers meaningful control over data processing activities bounded by risk-based considerations would enhance your constituents' experience and would provide a strong basis for the next era of digital competition and innovation.**