LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Dobbs Has Changed The Data Privacy Landscape

By **Allison Grande**

Law360 (June 22, 2023, 9:28 PM EDT) -- Since the U.S. Supreme Court scuttled abortion protections in its Dobbs decision a year ago, federal and state policymakers have turned up the heat on companies to put tighter restrictions on the collection and disclosure of personal health and location data, although the growing popularity of technologies that are fueled by mass data sets stands to threaten these efforts.

The high court's ruling in Dobbs v. Jackson Women's Health Organization sparked immediate concerns about the ability of tech companies to pass on sensitive information they amass about individuals' health, online searches, communications and location history to law enforcement for use in prosecutions in states where abortion is now outlawed.

In the year since that ruling, regulators and legislatures have played off this heightened attention to propose rules, launch enforcement actions and enact laws aimed at limiting how much data these companies can collect and curbing the access that third parties have to this information.

"Dobbs has really changed the debate and the culture around privacy in this country," said Eli Wade-Scott, a partner and leader of the class action practice group at plaintiffs firm Edelson PC.

While data privacy has become a hot-button issue in recent years in large part because of an explosion of data breaches and major revelations about how tech giants such as Google and Meta Platforms Inc. are using and sharing consumers' information, the Dobbs ruling raised immediate tangible data misuse concerns that have spurred both legislatures and the courts "to start seeing privacy through a much clearer lens" and be "more willing to hold corporations accountable," Wade-Scott said.

"People are caring more and more about these data privacy issues post-Dobbs," he added.

This increased scrutiny has prompted companies to "take a fresh look" at their privacy practices to ensure that their policies are consistent with how they're actually using and disclosing consumer data, noted Scott Weinstein, a partner at McDermott Will & Emery LLP.

Businesses are also taking a hard look at ways to minimize the reproductive health information they're collecting in the first place since they can't disclose information they don't have to out-of-state officials seeking to enforce subpoenas for access to reproductive health information in states where abortion remains legal, Weinstein added.

However, as was the case even before the Dobbs decision, these privacy-enhancing efforts tend to be

"at odds" with the business model widely embraced by big tech companies, which typically rely on vast data sets to generate revenue and keep their users engaged, noted Wade-Scott.

This "fundamental tension between privacy rights and Big Tech's data model is only going to be exacerbated by" the rapid rise of products and services that run on artificial intelligence, which needs to be trained on vast and diverse data sets in order to be most effective, Wade-Scott said.

"Companies are paying lip service to data minimization, but where the rubber hits the road, that's at odds with what so many companies are focused on, especially when it comes to the heaviest hitters in tech," he said.

Still, regulators and legislatures have been clamoring over the past year to stave off some of these concerns by tightening existing protections for reproductive health and other sensitive data. While some of these developments may have happened eventually, the increased attention that Dobbs brought to the use and disclosure of sensitive health information has likely "made these changes happen more quickly," said Andrew Crawford, senior counsel with the Center for Democracy and Technology's data and privacy project.

Over the past 12 months, the bulk of the action on this front has come from a pair of federal regulators: the U.S. Department of Health and Human Services' Office for Civil Rights and the Federal Trade Commission.

"What we're seeing is these agencies are moving to use their existing authority to ensure that health data has strong privacy protections to address the novel issues that Dobbs has created," the CDT's Crawford said.

In the immediate aftermath of Dobbs, the OCR issued guidance that laid out the limitations on federal protections for medical information under the Health Insurance Portability and Accountability Act, which applies only to health care providers, insurers and their businesses associates, and provided tips for safeguarding privacy when using mobile devices and apps that may fall outside the law's reach.

"The OCR guidance contains numerous examples of ways in which the [HIPAA] privacy rule continues to protect the privacy of individuals in the wake of Dobbs," said Linda Malek, chair of the health care and privacy and cybersecurity practices at Moses & Singer LLP.

Still, confusion continued to abound over HIPAA's reach, particularly when it came to the rules for responding to demands for data about an out-of-state resident seeking legal abortion services.

The agency has since moved to clarify these protections with the issuance of a proposed rule **in April** that would strengthen the HIPAA privacy rule by prohibiting the use or sharing of protected health information to investigate or prosecute patients or providers who have obtained or provided legal reproductive health care, including an abortion.

The proposed rule is designed to alleviate concerns about law enforcement in states where abortion has been outlawed seeking patient information from health care providers in states where the procedure remains legal by clarifying that this sharing of information is prohibited under HIPAA.

While there's been no indication that prosecutors have been moving to subpoena out-of-state providers on a large scale, "that doesn't mean it couldn't happen in the future," making the OCR's move at this

juncture to tighten the rules around how reproductive health data is shared with law enforcement agencies a critical one, noted McDermott's Weinstein.

The public had until June 16 to weigh in on the proposal, and the OCR is currently wading through the responses. According to the docket for the proposed rule, the agency has received more than 25,000 comments, including feedback from a coalition of attorneys general in California, New York, North Carolina, Washington, D.C., and 20 other states expressing their "strong" support for the proposed changes and calling on the agency "to move expeditiously" to finalize them.

"The department's proposed modifications would help to ensure that private health information is not used against people for seeking, obtaining, providing, or facilitating lawful reproductive health care, and would give individuals confidence that their protected health information will be kept private," said the attorneys general, many of whom have also been ramping up their scrutiny of companies' data-handling and security practices in recent years.

"The department's swift action in implementing these necessary protections is a vital step in defending sensitive reproductive health information against disclosure to the maximum extent possible in today's rapidly-shifting and increasingly hostile climate," they added.

The rule change would still leave some uncertainty, including questions over the extent to which patient requests to restrict data sharing should be honored and how having health information exchanges where physicians in various states can view the same information might complicate situations where a patient receives pregnancy ending medication in a state that allows it but seeks treatment for the after-effects in a state where it's not legal, attorneys say.

But while these changes "may not address all of the concerns about privacy of reproductive health data, [they still] are meaningful steps to protect such data," said Jodi Daniel, a partner at Crowell & Moring LLP and former lead policymaker at HHS.

The FTC has also notably dialed up its health privacy enforcement efforts.

In doing so, the commission has leaned heavily on its Health Breach Notification Rule, which requires vendors of personal health records and related entities that aren't covered by HIPAA to notify consumers following a breach involving unsecured information. Triggering events can include not only the loss or theft of consumer data but also the unauthorized disclosure of this information to third parties.

While the rule has been on the books since 2009, the FTC hadn't used it in an enforcement action until the commission in February accused digital health care platform GoodRx Holdings Inc. of "repeatedly" violating its promise to not share personal health information with Facebook, Google and other advertisers.

The commission announced in May that it would be wielding the rule for a second time in an enforcement action against fertility app Premom. The commission claimed that Premom shared users' sensitive personal information with third parties and failed to notify consumers of these unauthorized disclosures in violation of the Health Breach Notification Rule.

Then, the day after the Premom action came to light, the FTC proposed changes to its Health Breach Notification Rule that included clarifying that the rule applies to health apps and other similar

technologies that collect or use consumers' health information. While the commission issued a policy statement in 2021 affirming these services are covered by the rule, the proposed amendments would formalize this stance and give the agency firmer footing to go after a wider universe of companies moving forward.

"Because there isn't a comprehensive federal privacy law in the U.S., the same document that has protection when it's held by a doctor has fewer or no protections when it's held by a non-HIPAA-covered entity, and that's where the FTC's jurisdiction comes in," said the CDT's Crawford.

Several bills have been introduced in Congress to address the health privacy and data disclosure issues raised by Dobbs. These measures include the My Body, My Data Act, which seeks to limit the reproductive health data gathered by apps and websites, and the American Data Privacy and Protection Act, which would set a national standard for how users handle and share personal information, with heightened protections for sensitive information.

"However, because of the divided nature of the current Congress, none have advanced very far," noted Malek of Moses & Singer.

Instead, states have been filling the legislative void.

Earlier this month, Texas became the 10th state to enact a comprehensive privacy law that gives consumers more access to and control over their personal data. Washington took it a step further in April when the state took **the novel step** of approving legislation focused specifically on the protection of health and reproductive information.

The My Health My Data Act requires companies to obtain opt-in consent before processing, selling and sharing any consumer health data, which the law defines broadly to mean any information that identifies the consumer's past, present or future physical or mental health status. The measure is backed by a provision that allows consumers to bring private lawsuits for potential violations.

"The Washington law is part of a wave of state legislatures who are seeing how important these issues are to their constituents and are acting in a concrete way to get concrete legislation through," said Edelson's Wade-Scott.

The plaintiffs' attorney also noted that, in the wake of Dobbs, private attorneys have become more focused on issues such as location tracking and the use of medical data, and both judges and juries have appeared "more willing" to hold companies accountable for these practices.

He particularly pointed to a Chicago federal jury's decision last October to award a class of BNSF Railway employees $228 million in statutory damages for the railroad's collection and use of their fingerprints for identity verification at job sites without providing required notices.

"That verdict shows that juries and courts are going to take privacy violations very seriously," Wade-Scott said, adding that the plaintiffs bar "remains focused" on these issues and is in the midst of "several continuing investigations into cases that will put these issues at the forefront."

While companies have made strides during the past year in shielding reproductive health information from unauthorized access, they can still do more to reduce the likelihood that this data could be used in abortion-related prosecutions and civil lawsuits, Crawford noted.

He pointed to several recommendations that his group made in their May report "Data After Dobbs," including only collecting the information necessary to provide the product or service being offered, deleting data as soon as it becomes unnecessary and removing identifying information from data sets such as the ones used to fuel AI.

"In the past year, we've been seeing the initial reaction to the change in protections around reproductive health," Crawford said. "Dobbs is going to continue to have an impact moving forward, and we're going to continue to see Congress debate these issues and federal agencies take action, so we're going to need to see companies step up and do more to protect consumers' health data."

--Editing by Jay Jackson Jr. and Rich Mills.
