2023

Data for Sale: Navigating the Role of Data Brokers and Reproductive Health Information in a Post-<i>Dobbs</i> World

Heather Chong

*Southern Methodist University, Dedman School of Law*

---

**Recommended Citation**


This Case Note is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in SMU Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit [http://digitalrepository.smu.edu](http://digitalrepository.smu.edu).
Data for Sale: Navigating the Role of Data Brokers and Reproductive Health Information in a Post-Dobbs World

Heather Chong*

ABSTRACT

Data privacy is a growing concern in our fast-paced society, as it has become increasingly necessary to relay and retain information digitally. However, the United States trails behind its counterparts in terms of the strength of existing data protection legislation. Unlike the European Union and its General Data Protection Regulation (“GDPR”) law, the United States has no similar comprehensive data protection act. This lack of legislation has led to the exploitation of people’s private data and allowed companies to utilize loopholes in current laws to access sensitive health information. Data brokers have been collecting and reselling consumers’ personal information, including their health data. To combat the actions of data brokers and other parties that might desire to be privy to sensitive data, the bipartisan American Data Privacy and Protection Act (“ADPPA”) has been proposed and is arguably the nation’s first comprehensive legislation affecting information privacy that has a substantial prospect of passage. This case note looks at the history of data brokers and their relationship to the evolving field of data privacy, specifically concerning reproductive health information. Additionally, an overview and comparison of the GDPR is examined. Recent trends in government action concerning the protection of reproductive health information are discussed, and the possible effects of the passage of the ADPPA are considered, too.

I. INTRODUCTION

Participants in today’s society face the necessity of sharing their personal information online due to an increased dependency on technology in their daily lives.¹ A record-breaking number of data breaches involving personal security information that have occurred in recent years makes this reality increasingly evident.² One way that an individual’s private information can be disseminated to third parties is through a data breach of a company’s


* Heather Chong is a 2024 candidate for Juris Doctor from SMU Dedman School of Law. She received a Bachelor of Science and Arts in Human Development and Family Sciences from The University of Texas in Austin in 2020.


private records. The type of personal information that is collected is targeted and specific, which turns the knowledge of people’s traits and habits into a product to sell. In the past, activity like personal internet search history has been obtained through subpoenas by law enforcement, and search history has even been used to indict people on criminal charges. This kind of invasive surveillance into sensitive personal information may have further implications for the buying and selling of private health information in today’s legal landscape.

Technological advances and the commodification of personal data have rendered data brokering a viable method of distributing collected personal information. However, the legality of the methods that data brokers use is of increased concern. Particularly concerning is the trend of data brokers buying the reproductive health data of women and selling this information to anti-abortion organizations. Currently, there are no Health Insurance Portability and Accountability Act (HIPAA) violations that arise from data brokers collecting and selling health data, simply because data brokers selling individual health information is not a topic covered by the act’s narrow scope. Further, the United States does not have a comprehensive data protection act similar to the European Union’s General Data Protection Regulation (GDPR) law, so it is difficult to say with certainty what level of data brokering activity is legal. Today, the hope is that the bipartisan American Data Privacy and Protection Act (ADPPA) will finally provide comprehen-

6. See id.
7. See Guinness, supra note 4.
8. See id.
10. Id.
sive information privacy protection for Americans, especially for pregnant ones.\textsuperscript{12}

\section*{II. DATA BROKERS DEFINED}

The Federal Trade Commission (FTC) defines data brokers as “companies that collect consumers’ personal information and resell or share that information with others.”\textsuperscript{13} The information that these companies collect is obtained in a multitude of ways.\textsuperscript{14} Those methods include going through third-party companies that consumers directly interact with, searching in public databases, like courthouse records and social media, and tracking consumers’ online activity.\textsuperscript{15} Consumers may affirmatively agree to the release of their data when agreeing to the terms and conditions of, for example, a social media app; Many apps collect user information and sell that data to data brokers.\textsuperscript{16} However, consumers are usually unaware that their information is being collected. Once this information is collected or released from third-party apps, data brokers either sell the data as-is, in the form of factual statistics, or they release consumer profiles based on inferences using actual data.\textsuperscript{17} It is challenging to keep track of the actual size of the data broker market in the United States, because there is no comprehensive list or registry of these types of companies.\textsuperscript{18}

\section*{III. HISTORY AND BACKGROUND}

The lack of a comprehensive federal law lends its hand to the pervasiveness of data brokering today.\textsuperscript{19} Historically, the practice of buying and selling consumer data predates even the era of common internet use.\textsuperscript{20} Practices like assigning credit scores were primitive ways of segmenting consumers based

\begin{itemize}
\item \textsuperscript{12} Cameron F. Kerry, \textit{How comprehensive privacy legislation can guard reproductive privacy}, \textit{Brookings} (July 7, 2022), https://www.brookings.edu/blog/techtank/2022/07/07/how-comprehensive-privacy-legislation-can-guard-reproductive-privacy/ [https://perma.cc/A4CJ-5W3F].
\item \textsuperscript{14} Guinness, \textit{supra} note 4.
\item \textsuperscript{15} \textit{Id.}
\item \textsuperscript{16} \textit{Id.}
\item \textsuperscript{17} \textit{See} Rieke et. al, \textit{supra} note 1, at 11.
\item \textsuperscript{18} \textit{Id.} at 13.
\item \textsuperscript{19} Guinness, \textit{supra} note 4.
\item \textsuperscript{20} Rieke et. al, \textit{supra} note 1, at 5.
\end{itemize}
Despite the country’s long history of applying data brokering practices to consumer activity, the United States has yet to enact any form of comprehensive law that governs the buying and selling of private data information.22 This activity is concerning considering the widespread use of smartphones and web browsing, and data brokers now, more than ever, have an unlimited wealth of information at their fingertips.23 Who this information goes to and how it is used varies across markets, but law enforcement is one market whose use of information provided by data brokers could result in potentially significant consequences.24 Even prior to recent landmark cases, police have used personal internet search activity to penalize and criminally indict people suspected of seeking abortions.25

In June of 2022, through its decision in Dobbs v. Jackson Women’s Health Organization, the Supreme Court overturned the constitutional right to abortion granted in Roe v. Wade.26 Dobbs involved an abortion clinic in Mississippi that wanted to challenge the state’s ban on abortions after the fifteenth week of pregnancy.27 Mississippi initially appealed to the United States Supreme Court to ask the for the abortion ban to be upheld, arguing that the ban was compliant with Roe v. Wade.28 The appointment of a new Supreme Court Justice prompted the State to change its strategy and asked the Court to instead overturn Roe, which the Court did.29 This landmark case signaled a shift in federal abortion rights throughout the country and prompted the enactment of more restrictive state laws.30

Proponents of abortion are now concerned with the repercussions of the decision; they are particularly concerned with the surveillance of pregnant bodies by data brokers through apps and communication services and the potential criminalization of people through the acquired information.31 This concern is not based solely on the Supreme Court’s recent landmark decision, but also considers prior cases of data brokers surveilling pregnant peo-

21. Id. at 4–5.
22. Id. at 16.
23. Id. at 6.
24. Id. at 8.
25. Feder, supra note 5.
28. Id.
29. Id.
30. See id.
31. Feder, supra note 5.
In 2017, the Massachusetts attorney general settled a case with data broker Copley Advertising. The firm had been tracking people entering reproductive health facilities and storing their location data to run targeted ads. This location data was used by anti-abortion groups to identify people in the waiting rooms of these clinics to run targeted advertisements consisting of anti-abortion messages.

Abortion rights groups are concerned that this type of information may be used in the future to investigate and prosecute pregnant people who seek out an abortion or whose activities may be interpreted as abortion-seeking behavior. Evidence from digital traces of online activity can be used to draw inferences regarding someone’s status. This information would be available not only to data brokers but possibly to other governmental institutions. Law enforcement agencies have used digital evidence, such as proof of text messages and web browsing activity, to enforce laws prohibiting abortion. Internet search history has even been used to convict a woman of feticide via a self-induced abortion. Data brokers make information used to make inferences about a person’s health status more accessible. The concern is that the lack of regulation would allow law enforcement agencies to use private health data from data brokers to investigate and prosecute possible pregnancies and abortions, especially with a warrant.

In fact, data brokers have become more brazen with their data collecting after the court’s overturning of Roe v. Wade in the June Dobbs ruling. Prior to the Dobbs decision, data brokers offered more than thirty listings for information on expecting parents and were selling the opportunity to third-parties to access these individuals through mass email blasts. After the ruling, data

---

32. Id.
33. Sherman, supra note 9.
34. Id.
35. Id.
37. See Rieke et al., supra note 1, at 8.
38. Id.
39. Ng, supra note 36.
40. Id.
41. Id.
42. See id.
43. Id.
44. Id.
brokers updated twenty-five of those listings. When this type of information is distributed, the individuals whose information is being sold are often unaware that their personal data is in the hands of various third-parties. Even if they are aware, that does not stop companies or government agencies from using that data to perpetuate harmful targeted advertising or investigate suspicious online activity.

IV. THE ADPPA AND ITS IMPLICATIONS ON THE PRIVACY OF REPRODUCTIVE HEALTH INFORMATION

The American Data Privacy and Protection Act (ADPPA) is the nation’s first comprehensive legislation affecting information privacy that has a substantial prospect of passage. The Act is significant due to its proposed regulations on collecting, using, and sharing data, and for providing material boundaries on the types of covered data. Health information, like potential pregnancy and abortion related search activity, is considered covered sensitive data under the Act. Sensitive data is given additional protection in excess of what is provided under standard covered data. One type of data covered under the “sensitive data” classification is “[a]ny information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual.” Traditionally under HIPAA regulations, this type of coverage would only apply when such information was held by a covered healthcare provider. Under the ADPPA, any information defined as sensitive data would be covered regardless of its source, including from health tracking apps, like period-tracking applications, and internet search activity. The ADPPA also protects “derived data” which is personal information created through inferences based on information sourced from an individual or their device.

Under the Act, data brokers would be required to show that their collection and distribution of personal information be “limited to what is reasona-

45. Ng, supra note 36.
46. Sherman, supra note 9.
47. See id.
48. Kerry, supra note 12.
49. Id.
50. Id.
51. Id.
53. Kerry, supra note 12.
54. Id.
bly necessary and proportionate” to fulfill services requested by an individual for specific purposes like shipping and billing. Sensitive data has further restrictions and prohibits the sharing of personal information with third parties unless the individual whose data is being shared affirmatively consents to the transfer. This allows individuals to control the extent to which their data is shared, and ensure that it is not used for any purpose besides what was consented to. The ADPPA would also provide means for individuals to obtain and delete any data that is linked to them, a way for individuals to withdraw previously given consent, and opt out of targeted advertising arising from data purchased by third parties. Control over the chain of custody regarding their personal information would give individuals some control over potentially revealing tracking and aggregation of their online activities.

In the case of legal obligations, the ADPPA provides that the transfer of an individual’s sensitive data to third parties is prohibited unless “the transfer is necessary to comply with a legal obligation imposed by Federal, State, or local law, or to establish, exercise, or defend legal claims.” This establishes that sensitive data is not immune from procurement by law enforcement agencies. However, the protections afforded by the ADPPA would still reduce the amount of private information held by data brokers and third parties that is currently available to law enforcement through commercial sources and online activity. Further, the Act would restrict the freedom of prosecutors and law enforcement to simply request information from covered entities, who would have a legal basis for declining to provide the requested data.

One other issue that lawmakers are facing while trying to pass the ADPPA is preemption. California has notably already passed very robust

58. Kerry, supra note 12.
59. Id.
60. Id.
62. Kerry, supra note 12.
63. Id.
64. Id.
data privacy laws and takes issue with the Act’s ability to preempt state law.66 The California Consumer Privacy Act of 2018 (CCPA):

> [A]llows consumers the right to request a business to disclose the categories and specific pieces of personal information that the business has collected about the consumers as well as the source of that information and business purpose for collecting the information. Provides that consumers may request that a business delete personal information that the business collected from the consumers. Provides that consumers have the right to opt-out of a business’s sale of their personal information, and a business may not discriminate against consumers who opt-out.67

The comprehensive protections in the CCPA are similar in nature to those provided in the ADPPA: consumers are free to request disclosures regarding how their data is being used and shared,68 and they can request that personal information be deleted or opt-out of a business’s sale of their data.69 However, there is concern that the passage of the ADPPA will stop states from exercising their right to step in when the federal government fails to act to prevent future problems and react to current harm.70 Additionally, there is pushback from lawmakers like Senator Maria Cantwell who argue that the ADPPA places constraints on private lawsuits that would make litigation difficult for women to sue for violations against their right to protect their reproductive information.71 Senator Cantwell heads the Senate Commerce committee, and her opposition to the ADPPA leaves proponents of the act concerned for its passage.72

68. Compare id., with Kerry, supra note 12 (“For sensitive data, [the ADPPA] also prohibits sharing personal information with third parties such as advertisers and data brokers without affirmative express consent from individuals. And if such data is shared, it may not be processed beyond the purposes for which consent was given.”).
69. Compare State Laws Related to Digital Privacy, supra note 64, with Kerry, supra note 12 (“[The ADPPA] also requires a means for individuals to withdraw consent previously provided and to opt out of targeted advertising and transfers of data to third parties, providing some control over online tracking or data aggregation that could be revealing. . . .”).
70. Peterson, supra note 65.
71. Kerry, supra note 12.
72. Ng, supra note 36.
V. EUROPE AND THE GDPR

Europe’s General Data Protection Regulation (GDPR) is the world’s most stringent privacy and security law\(^{73}\) that applies not only to European companies, but any organizations that target citizens of the European Union for data collection.\(^{74}\) The law imposes specific requirements that must be adhered to when processing data, including minimizing the data being collected and processing only what is “absolutely necessary,”\(^{75}\) processing data for a legitimate purpose,\(^{76}\) and imposes hefty fines on anyone found to be in violation of these requirements.\(^{77}\) This imposition of heightened accountability is Europe’s standard for compliance: if you say you are compliant with the GDPR but have no way to prove your claim, then you will be found non-compliant.\(^{78}\) Additionally, there are only a few situations in which the GDPR allows for the processing of personal data.\(^{79}\) Even when one of these situations occurs, there must be clear and transparent documentation for the data processing, and continuous updates of the legal basis for the decision to process that data.\(^{80}\) There is a strong focus on respecting the rights of people being treated as data subjects and obtaining and documenting their clear consent.\(^{81}\)

How does the radical shift in abortion rights in the United States affect the European Union? In general, Europe has leaned in favor of legalizing abortion, with only two of the European Union member nations, Malta and Poland, maintaining restrictive laws.\(^{82}\) After the United States Supreme Court overturned *Roe*, the European Parliament responded by codifying the right to abortion in the Union’s Code of Fundamental Rights.\(^{83}\) Now, the concern is whether the United States will be able to submit warrants for sensitive data, such as location data, to European companies and how that will infringe on

\(^{73}\) Ben Wolford, *What is GDPR, the EU’s new data protection law?*, GDPR.EU (last visited Oct. 31, 2022), https://gdpr.eu/what-is-gdpr/ [https://perma.cc/RW8M-59UP].

\(^{74}\) Id.

\(^{75}\) Id.

\(^{76}\) Id.

\(^{77}\) Id.

\(^{78}\) Id.

\(^{79}\) Wolford, supra note 73.

\(^{80}\) Id.

\(^{81}\) Id.


\(^{83}\) Id.
the protections provided by the GDPR.84 There appeared to be a mutual understanding between the United States and the European Union regarding the importance of data privacy, and the potential difficulties both parties would face should the United States ever demand the collection of private health information.85 Prior to the Supreme Court’s decision to overturn Roe, the United States appeared to be moving in the direction of the European Union in regards to implementing comprehensive data privacy law, but Dobbs threatens to undo the progress made towards a mutual agreement for the right to privacy.86 A split Congress makes it even more difficult to pass a comprehensive data privacy law that would closely adhere to the GDPR and help allay concerns European companies in the United States may have.87

VI. RECENT TRENDS IN THE UNITED STATES

Despite the opposition facing the ADPPA, recent trends in lawmaker and government action signal leaning support in favor of the Act’s passage by preventing the dissemination of reproductive health and location data. In 2017, the Massachusetts attorney general found Copley Advertising in violation of Massachusetts General Law Title XV, Chapter 93A § 2.88 The company had been tracking consumers through geofencing technology, which identified internet-enabled devices through means of GPS and Bluetooth technology, and sold this data to its clients.89 One of Copley’s clients was an evangelical Christian organization that purchased advertisement access to devices located within geofenced areas, including locations with abortion clinics.90 The organization ran digital advertisements that, when clicked on, connected people in the abortion clinics to individuals who could potentially manipulate the person to not go through with their abortion.91 Copley and the Massachusetts attorney general agreed to a settlement that prevented them from geofencing areas in the vicinity of Massachusetts medical centers that could be used to infer an individual’s health status, medical condition, or medical treatment.92

In June of 2022, in anticipation of the Dobbs decision, Senators Warren and Wyden introduced the Health and Location Data Protection Act, a bill

84. Id.
85. See id.
86. See id.
87. See id.
88. Sherman, supra note 9.
89. Id.
90. Id.
91. Id.
92. Id.
banning data brokers from selling location and reproductive health data. The bill aims to prevent data brokers from using reproductive health data obtained from health apps like period-trackers and location data to ascertain whether someone is trying to obtain an abortion, particularly in states where abortion is criminalized.

In August of 2022, the FTC sued data broker Kochava for selling consumers’ geolocation data that placed them going to and from sensitive locations, including reproductive health clinics. In the FTC’s complaint, it alleged that consumers identified through the location data sold by Kochava could become vulnerable to injury through “stigma, discrimination, physical violence, emotional distress, or other harms.” The location data that Kochava acquired could be used to identify consumers who visited abortion clinics, and possibly identify any medical professionals involved in performing or assisting in abortion services. Ultimately, the FTC found that Kochava had violated Section 5 of the FTC Act by engaging in an unfair practice that would likely cause injury to the consumer that they could otherwise not prevent.

Post-Doobbs, there have been concerns regarding period-tracking applications and how their policies affect the protection of sensitive user data. Some European companies assure American users that they will adhere to Europe’s more stringent GDPR requirements and will not comply with subpoenas from the United States without certain requirements. American companies like Apple encrypt user data in their Health App to ensure that no one other than the user can have access to their health information. The

94. Id.
97. Id. at 8.
98. Id. at 10.
99. See Feder, supra note 5.
100. Id.
101. Id.
implications of health tracking apps like period trackers are still relatively unknown, and without a comprehensive policy in place to protect personal health data, users should err on the side of caution and limit their digital trail.\textsuperscript{102}

\section*{VII. CONCLUSION}

Data brokering as a practice is likely here to stay, at least for the foreseeable future. However, the use of such technology to police reproductive health and criminalize pregnant people based on inferences drawn from collected user data can be curbed at the very least, and eliminated at best. Lawmakers have shown their general stance on data brokering is that it requires more stringent regulation in today's internet-dependent society. Emulating the European Union's strict GDPR standards of buying and selling data and requiring a legal basis to do so through the ADPPA would provide American consumers with more autonomy over their digital footprint, and a heightened sense of security for sensitive personal health data.

It is apparent that the lax laws surrounding data brokering have led to adverse effects on some Americans who want to utilize technology to adapt to modern standards. A comprehensive information privacy act such as the ADPPA would provide additional safeguards for data privacy, including reproductive health privacy. Pregnant people in particular would be provided with more say in the ways their data is distributed and could decide how, if at all, that data could be linked back to them. The ADPPA's passage would mark a shift in the way the country approaches data privacy in an unpredictable society, where every technological advancement signals a new variable in consumer privacy. Not only would the ADPPA provide data privacy for the general population, but also for those at risk in places where their own bodies can be policed and criminalized.

Although the Act faces challenges concerning its passage, trends have shown that the country is supportive of taking measures to advance protection of private data information. Whether or not the ADPPA can pass in its entirety, its proposal has laid the groundwork for future legislation and can serve as a model for new proposals. The Act's comprehensive nature lends itself to the possibility of new, more robust lawmaking that can be introduced in the coming years. Even in the aftermath of \textit{Dobbs}, pregnant people and those seeking abortions may not need to worry about their health status being publicly available and easily accessed and instead focus on their health if their right to protect their online data is codified.

\textsuperscript{102} \textit{Id.}