DREXEL LAW REVIEW

THOMAS R. KLINE SCHOOL OF LAW

VOLUME 16 | 2024 | ISSUE 1

NOTE

FREEDOM OF MOVEMENT: PROTECTING THE RIGHT TO TRAVEL FROM LOCATION TRACKING INTERFERENCE

Nicholas J. Lee[*]

ABSTRACT

Americans often take for granted the ability to travel freely throughout the United States. Nonetheless, the ability to travel freely enables Americans to move throughout the United States without government or private interference, including interferences that cause a chilling effect on the ability. Considered a basic right in the United States, the ability to travel freely is a foundational political liberty that serves numerous important purposes. The ability to travel freely allows Americans to participate in everyday, basic activities, facilitates political freedom, and permits the exercise of associated rights, such as the First Amendment right of peaceful assembly. Yet, as one exercises his ability to travel freely, companies are hiding in the shadows, quietly tracking, collecting, and using individuals' location information.

Indeed, it is commonplace for people to have no knowledge of which companies receive their location information or how those companies use it. Technological innovations in location tracking and data analytics have made location tracking ubiquitous. The expansive location

[*] J.D. Candidate, 2024, Drexel University Thomas R. Kline School of Law; B.F.A., 2017, The Pennsylvania State University.

Thank you Professor Robert I. Field for your guidance and feedback as I developed this Note. Additional thanks to my colleagues on the *Drexel Law Review* for their meticulous edits. Finally, thank you to my family and Brynn McGillin for their endless support and encouragement in all that I do.

tracking industry, combined with the lack of comprehensive federal legislation regulating its practices, has led the industry to become the "Wild West" of privacy. Companies use existing technology, such as cell phones and smartphone applications, and emerging technology, such as facial recognition, to create comprehensive data sets on unsuspecting individuals. Companies use the compiled location information to provide services, but also to send targeted advertisements, influence individuals' behaviors, and interfere with individuals' ability to travel freely—the latter being a foundational and fundamental right in the United States.

Accordingly, this Note argues Congress, using its Commerce Clause authority, should enact legislation to protect the right to travel freely from interference caused by companies' location tracking practices. This Note also proposes Congress should draft this comprehensive legislation using the Health Insurance Portability and Accountability Act, specifically its Privacy and Security Rules, as a model framework for regulating companies' collection, use, and disclosure of individuals' location information.

TABLE OF CONTENTS

INTRODUCTION 189
I. LOCATION INFORMATION COLLECTION 194
A. *Connected Devices* 195
1. *Cellular phones* 195
2. *Smartphone applications* 200
B. *Advances in Technology: Facial Recognition* 205
II. THE RIGHT TO TRAVEL IN THE UNITED STATES 207
A. *The Historical Evolution of the Right to Travel in the United States* 208
B. *The Commerce Clause and the Right to Travel* 214
III. THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT 216
A. *The HIPAA Privacy Rule* 217
B. *The HIPAA Security Rule* 220
IV. HIPAA AS A FRAMEWORK TO PROTECT THE RIGHT TO TRAVEL 223
A. *Location Tracking's Impact on the Right to Travel* 224

B. *Location Tracking and HIPAA* 227
1. *Consent to be tracked?* 228
2. *Anonymity and de-identification of location information* 231
3. *Secured storage of location information* 233
C. *Alternative Legislation and Legislative Frameworks* 236
1. *The American Data Privacy and Protection Act* 237
2. *The Geolocation Privacy and Surveillance Act* 241
3. *The General Data Protection Regulation* 242
CONCLUSION 246

INTRODUCTION

Americans often take for granted the ability to travel freely throughout the United States.[1] Nonetheless, the ability to travel freely enables Americans to move throughout the United States without government or private interference,[2] including interferences that cause a "chilling effect" on the ability.[3] Considered a basic right in the United States,[4] the ability to travel freely is "a foundational political liberty" that serves numerous important purposes, alone and in combination with other fundamental rights.[5] The ability to travel freely allows Americans to do basic, everyday activities, such as go to work, school, or doctor appointments, run mundane errands, and visit friends and family around the country.[6] The ability to travel freely also facilitates political freedom in the form of internal migration.[7] Moreover,

1. *See* Kathryn E. Wilhelm, Note, *Freedom of Movement at a Standstill? Toward the Establishment of a Fundamental Right to Intrastate Travel*, 90 B.U. L. REV. 2461, 2461–62 (2010).

2. Richard Sobel, *The Right to Travel and Privacy: Intersecting Fundamental Freedoms*, 30 J. MARSHALL J. INFO. TECH. & PRIV. L. 639, 640 (2014); United States v. Guest, 383 U.S. 745, 759 (1966).

3. *See* Shapiro v. Thompson, 394 U.S. 618, 623, 631 (1969) (holding interferences that cause "a chilling effect on the right to travel" are "patently unconstitutional").

4. *See Guest*, 383 U.S. at 758.

5. *See* Sobel, *supra* note 2, at 639–40; Aptheker v. Sec'y of State, 378 U.S. 500, 520 (1964) (Douglas, J., concurring). The ability to travel freely "is the very essence of our free society, setting us apart. Like the right of assembly and the right of association, it often makes all other rights meaningful—knowing, studying, arguing, exploring, conversing, observing and even thinking. Once the right to travel is curtailed, all other rights suffer . . . ." *Id.*

6. *See* Wilhelm, *supra* note 1.

7. *See, e.g.*, ILYA SOMIN, FREE TO MOVE: FOOT VOTING, MIGRATION, AND POLITICAL FREEDOM *passim* (2020). Internal migration allows you to "vote with your feet by deciding to move to a different city or state because you prefer its government policies to those in force where you currently reside."

the ability to travel freely permits Americans to exercise other fundamental rights, including access to the courts and public offices[8] and First Amendment rights, like the right to peaceful assembly.[9] Yet, as one exercises his ability to travel freely, or any of its associated rights and freedoms, companies are hiding in the shadows, quietly tracking and collecting individuals' location to use however they deem fit.[10]

It is commonplace for people to lack knowledge about which companies receive their location or how those companies use that information.[11] Technological innovations in location tracking and data analytics have made location tracking "ubiquitous."[12] Moreover, the collection of location information is largely unregulated in the United States.[13] Without regulation, not only can companies legally access individuals' location information, but they can also buy or sell that information in perpetuity.[14] Indeed, the lack of regulation has led to endless business opportunities in the location data industry.[15] Thus, as technological innovation in location tracking and data analytics continues to develop rapidly, the location data tracking industry has become a "Wild West" of sorts, as privacy legislation has struggled to keep up with the rapid developments.[16]

Id. at 1. Throughout United States history, internal migration has facilitated and enhanced Americans' political freedom. *Id.* at 46–48 (providing examples).

8. *See* Crandall v. Nevada, 73 U.S. 35, 48–49 (1868).

9. *See* Zemel v. Rusk, 381 U.S. 1, 23–24, 26 (1965) (Douglas, J., dissenting) ("[T]he right to travel is at the periphery of the First Amendment, rather than at its core, largely because travel is, of course, more than speech: it is speech brigaded with conduct."); U.S. CONST. amend. I.

10. *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/BP5Y-8PST] [hereinafter Thompson & Warzel, *Twelve Million Phones*].

11. Stuart A. Thompson & Charlie Warzel, Opinion, *Smartphones Are Spies. Here's Whom They Report To.*, N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html [https://perma.cc/M4FH-JP3M] [hereinafter Thompson & Warzel, *Smartphones Are Spies*].

12. Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, BUS. L. TODAY (March 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/ [https://perma.cc/2SHZ-29XD].

13. Thompson & Warzel, *Smartphones Are Spies*, *supra* note 11.

14. *Id.*

15. *Id.*

16. *Id.*; *see* Boshell, *supra* note 12.

The fact location tracking is such a "Wild West" may have profound effects on individuals' ability to travel freely. For example, in 2019, the *New York Times* Privacy Project compiled a comprehensive report on the privacy implications of the location data industry, titled *One Nation, Tracked*.[17] The report notes that "[e]very minute of every day, everywhere on the planet, dozens of companies — largely unregulated, little scrutinized — are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files."[18] The Privacy Project obtained one of the gigantic data files, which contained in excess of fifty billion location pings from the cell phones of more than twelve million Americans.[19] Every single point of information in the fifty billion pings represented the exact location of the individual's cell phone over the course of several months.[20]

The Privacy Project used the obtained location information to track a wide variety of individuals.[21] The Privacy Project tracked the movements of millions of individuals visiting Lower Manhattan in New York City, the Los Angeles beachfront neighborhoods, and even the Pentagon and White House in Washington, D.C.[22] The data set used by the Privacy Project included individuals—adults and minors alike—going about their normal, daily lives.[23] The data set also included location information from individuals who attended public assemblies, such as the 2017 Presidential Inauguration protests and Women's March in Washington, D.C.[24] Moreover, the data set included the precise movements of a Secret Service agent

17. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

22. *Id.*

23. *See* Stuart A. Thompson & Charlie Warzel, Opinion, *Where Even the Children Are Being Tracked*, N.Y. TIMES (Dec. 21, 2019), https://www.nytimes.com/interactive/2019/12/21/opinion/pasadena-smartphone-spying.html [https://perma.cc/YST9-XG9W].

24. Charlie Warzel & Stuart A. Thompson, Opinion, *How Your Phone Betrays Democracy*, N.Y. TIMES (Dec. 21, 2019), https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-democracy-protests.html [https://perma.cc/BQV6-X837].

accompanying the President of the United States over the course of a day full of meetings with another world leader.[25] Indeed, the Privacy Project could "see the places you go every moment of the day, whom you meet with or spend the night with, where you pray, whether you visit a methadone clinic, a psychiatrist's office or a massage parlor."[26] As the Privacy Project details, if a sweeping location data set like this ended up in the wrong hands, the disclosed location information could be used to target, influence, harass, stalk, or perpetually surveil individuals—interfering with one's ability to travel freely.[27]

The Privacy Project exposed the pervasiveness of the small handful of companies who quietly collect individuals' location information.[28] These companies justify their business practices in three ways: "[p]eople consent to be tracked, the data is anonymous and the data is secure."[29] However, numerous problems arise with these justifications.[30] First, consent to location tracking can be deceptive as companies "rarely make clear how the data is being packaged and sold."[31] Second, although location data contains no identifiable information, such as an individual's name, "it's child's play to connect real names to the dots that appear on the maps."[32] Finally, the location data securely stored by companies today can be easily hacked, stolen, or leaked tomorrow.[33]

To protect individuals' privacy, and thus protect their ability to travel freely without interference, individuals' location data

25. Stuart A. Thompson & Charlie Warzel, Opinion, *How to Track President Trump*, N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html [https://perma.cc/Q74C-WGSP] [hereinafter Thompson & Warzel, *How to Track President Trump*]. Through the acquired data set and other publicly available information, the *New York Times* deanonymized the geolocation information of a Secret Service agent to track President Trump's whereabouts—"down to a few feet"—as the President conducted a full day of meetings with Prime Minister Shinzo Abe of Japan. *Id.*

26. Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

27. *See id.*

28. *See id.*

29. *Id.*

30. *See* Boshell, *supra* note 12.

31. Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

32. *Id.*

33. *Id.*

should be regarded as "sensitive information," similar to an individuals' health information.[34] Individuals should know exactly what type of information tracking they are consenting to, steps should be taken to ensure location information is anonymized, or at least de-identified, and companies that store location information should be required to comply with stringent security rules. Therefore, this Note proposes Congress use the Health Insurance Portability and Accountability Act as a model framework for regulating the collection, use, and disclosure of individuals' location information because of the profound effects location tracking has on Americans' fundamental ability to freely travel.

Part I of this Note examines the ways in which companies collect, use, and disclose individuals' location information. Part II examines the origins of the right to travel in the United States and shows the fundamentality of the ability to travel freely. Further, Part II uses examples of when Congress has regulated, under the Commerce Clause, the activities of private companies and actors who created a negative impact or chilling effect on Americans' ability to travel freely. Part III details the Health Insurance Portability and Accountability Act and its Privacy and Security Rules. Part IV shows why, from a policy standpoint, Congress should regulate the collection, use, and disclosure of individuals' location information because of the impact on Americans' ability to freely travel. Additionally, Part IV shows how the Health Insurance Portability and Accountability Act can be used as a framework to protect the privacy of individuals' location information. Finally, Part IV examines alternative legislation and legislative frameworks and why the Health Insurance Portability and Accountability Act serves as a better model to use for protecting individuals' location information and the ability to travel freely.

34. *See* Boshell, *supra* note 12.

I. LOCATION INFORMATION COLLECTION

Individuals' location information can reveal much about them, including where they live, work, shop, or even more generally, where they travel.[35] As the Supreme Court of the United States has noted, location information can provide "an intimate window into a person's life, revealing not only [one's] particular movements, but through them [their] 'familial, political, professional, religious, and sexual associations.'"[36] Thus, location information provides an all-encompassing look into the movements and lives of millions of individuals.[37] By using location information, companies can provide beneficial services, such as directions, ridesharing, or fitness tracking.[38] However, companies can also use the same collected location information to make conclusions or predictions about individuals or monetize the information by selling it to third parties.[39] Therefore, an individual's location is a powerful piece of information, and "[i]t should be no surprise . . . that there is a big demand for [one's] location data."[40]

Advances in technology allow companies to track location information in increasingly easy and accurate ways.[41] Location tracking technology is widely available, and companies use multiple location tracking systems simultaneously to collect individuals' location information.[42] Further, companies combine the collected location information with other personal information from individuals, such as addresses, to compile precise

35. *Location Tracking*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/data-protection/location-tracking/ [https://perma.cc/XXE7-E6Y8].

36. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 440, 415 (2012) (Sotomayor, J., concurring)).

37. Jennifer Valentino-DeVries, *How Your Phone Is Used to Track You, and What You Can Do About It*, N.Y. TIMES (Aug. 19, 2020), https://www.nytimes.com/2020/08/19/technology/smartphone-location-tracking-opt-out.html [https://perma.cc/PZ7B-X4VF].

38. Boshell, *supra* note 12.

39. *Id.*

40. *Location Tracking*, *supra* note 35.

41. *See, e.g.*, Valentino-DeVries, *supra* note 37 (discussing the privacy implications of location tracking).

42. Boshell, *supra* note 12.

and all-encompassing profiles of the individuals.[43] Such location tracking practices, without some form of regulation, may have profound impacts on individuals, particularly on individuals' ability to travel freely.

A. *Connected Devices*

A prominent way companies collect location information is through individuals' use of connected devices—primarily cellular phones.[44] Today, Americans increasingly have the world at their fingertips through the ubiquitous use of smartphones.[45] As of 2021, 97% of Americans owned a cell phone, with the vast majority owning smartphones.[46] For Americans under the age of fifty but over eighteen, 100% own a cell phone, with approximately 95% of those cell phones being smartphones.[47] Moreover, Americans who own cell phones tend to take their cell phones almost everywhere they go.[48] As more and more individuals continue to own and use cell phones to call, text, email, or play games, companies will increasingly collect those individuals' location information to provide useful services, but also to make conclusions or predictions about the individual and make financial gains by selling the information to third parties.[49]

1. *Cellular phones*

Cell phones are one of the "easiest means to gather the most comprehensive data about a person's public—and *private*—

43. *Id.*

44. *See* RACHEL LEVINSON-WALDMAN, CELLPHONES, LAW ENFORCEMENT, AND THE RIGHT TO PRIVACY: HOW THE GOVERNMENT IS COLLECTING AND USING YOUR LOCATION DATA 1 (2018), https://www.brennancenter.org/sites/default/files/2019-08/Report_Cell_Surveillance_Privacy.pdf [https://perma.cc/78SS-C7MZ].

45. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/XKY9-SUL6].

46. *Id.* (noting 85% of Americans own a smartphone).

47. *Id.*

48. LEVINSON-WALDMAN, *supra* note 44; *see also* Riley v. California, 573 U.S. 373, 395 (2014) (noting smartphone users even use their phones while in the shower).

49. *See* Boshell, *supra* note 12.

movements available."[50] When an individual uses his cell phone, the device regularly pings and connects to cell towers.[51] The cell phone connections, in turn, create an all-inclusive record of the user's whereabouts.[52] As a cell phone user goes about his daily life, his cell phone continuously searches for, and connects to, the strongest cell tower signal in the service's network.[53] Every time the user's cell phone connects to one of the service provider's cell towers, the user's identifying information is transmitted to the service provider.[54] The individual's identifying information collected by the service provider is "information that can be used to distinguish or trace an individual's identity," including information such as the individual's name, birthday, or location information.[55] An individual's identifying information allows the service provider to "track the phone, discontinue service, or blacklist it from a network."[56]

Today, cell towers are rapidly expanding in density and proliferation.[57] With the rapid expansion of cell towers, cell phone service providers can collect and store what is known as "cell site location information" with increasing ease and accuracy.[58] Cell site location information ("CSLI") is the "combination of information identifying a particular subscriber and the cell

50. United States v. Powell, 943 F. Supp. 2d 759, 780 (E.D. Mich. 2013) (emphasis in original).

51. Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FED. TRADE COMM'N (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/2GDD-SM3Q].

52. *Id.*

53. LEVINSON-WALDMAN, *supra* note 44.

54. *Id.* (noting identifying information is transmitted regardless of whether a call is underway).

55. *Rules and Policies—Protecting PII—Privacy Act*, U.S. GEN. SERVS. ADMIN., https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act [https://perma.cc/KYC5-JQ3Z] (Aug. 11, 2023); *see What Is Personally Identifiable Information (PII)?*, CAP. ONE (Aug. 18, 2022), https://www.capitalone.com/learn-grow/privacy-security/what-is-pii/ [https://perma.cc/S4JG-CRRG].

56. LEVINSON-WALDMAN, *supra* note 44.

57. *Id.*; *see also* David Shepardson, *Verizon Plans to Turn on About 2,000 5G Towers in February -Sources*, REUTERS (Feb. 1, 2022, 5:28 PM), https://www.reuters.com/business/media-telecom/verizon-plans-turnaround-2000-5g-towers-february-sources-2022-02-01/ [https://perma.cc/H5L7-SHVR] (describing Verizon's recently constructed infrastructure for its 5G network).

58. LEVINSON-WALDMAN, *supra* note 44, at 1–2.

providing connectivity at a certain point in time."[59] Cell phone service providers collect CSLI at various times and for various purposes.[60] CSLI may be generated for routine business purposes, such as network updates, but it may also be collected when the cell phone user places a call or sends a text message.[61] However, the service provider is also collecting the user's location information every seven to nine minutes.[62] Such precise location information may then be sold or disclosed to third parties in perpetuity, including to other companies and the government.[63]

Carpenter v. United States illustrates one service provider's disclosure of CSLI to a third party.[64] In *Carpenter*, law enforcement officers obtained CSLI from the defendant's cell phone service provider for a period of 127 days in connection with a series of armed robberies.[65] The Supreme Court held the disclosure of the CSLI invaded the defendant's Fourth Amendment right to a "reasonable expectation of privacy in the whole of his physical movements."[66] The Court noted individuals compulsively carry their cell phones almost everywhere, as if cell phones are a "feature of human anatomy."[67] Accordingly, the Court determined the CSLI "achieve[d] near perfect surveillance" of the defendant's whereabouts, akin to if the government "attached an ankle monitor to the phone's user."[68]

---

59. Justin Hill, *Digital Technology and Analog Law: Cellular Location Data, The Third-Party Doctrine, and the Law's Need to Evolve*, 51 U. RICH. L. REV. 773, 785 (2017).

60. *Id.*

61. *Id.* at 786.

62. *Id.*

63. *See id.* at 787; Thompson & Warzel, *Smartphones Are Spies*, *supra* note 11.

64. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018).

65. *Id.* at 2212.

66. *Id.* at 2219.

67. *Id.* at 2218.

68. *Id.* Further, the Court noted:

> the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.
>
> *Id.* at 2219.

Similar to CSLI, companies track individuals' location information through their cell phone's connection to Wi-Fi, Bluetooth, and GPS.[69] For instance, companies can use a cell phone's Wi-Fi, Bluetooth, and GPS connections to "define a virtual geographical boundary" to track individuals' locations.[70] Companies typically use this geographical boundary, known as a geofence, "to direct advertisements to users through browsers and applications on their devices when those users are located in a designated territory."[71] When an individual with a cell phone travels into the designated territory, the cell phone triggers the geofence and advertisements are targeted at the individual.[72] Additionally, the geofence may also send the individual's location information to the company so the company can continue to send targeted advertisements after the cell phone leaves the designated area.[73] Typically, the cell phone user is never even aware their location information is being collected.[74]

In 2017, for example, a marketing company erected "secret digital 'fence[s]' . . . near clinic[s] offering abortion services."[75] The company created geofences around reproductive health centers to direct targeted advertisements for abortion

69. *See id.* at 2211–12; *see also Wi-Fi RTLS, Location Tracking & Positioning*, INPIXON, https://www.inpixon.com/technology/standards/wifi [https://perma.cc/2S2J-ECEU] (describing how Wi-Fi "can be leveraged to detect and track the location of people, devices and assets").

70. Rahul Awati, *Geofencing*, TECHTARGET, https://www.techtarget.com/whatis/definition/geofencing [https://perma.cc/PC3U-AU8V] (Dec. 2022); *see also* Saraphin Dhanani, *The D.C. District Court Upholds the Government's Geofence Warrant Used to Identify Jan. 6 Rioters*, LAWFARE (Mar. 10, 2023, 8:16 AM), https://www.lawfareblog.com/dc-district-court-upholds-governments-geofence-warrant-used-identify-jan-6-rioters [https://perma.cc/S6LT-K4HH] (noting the U.S. District Court for the District of Columbia upheld the government's use of a "geofence warrant" to seize Google's location history data for individuals "in and immediately around the Capitol . . . on January 6, 2021"); United States v. Rhine, 652 F. Supp. 3d 38, 90 (D.D.C. 2023) (upholding the government's use of a geofence warrant).

71. Press Release, Commonwealth of Mass., AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities [https://perma.cc/YSS4-WG9E] [hereinafter Press Release, AG Reaches Settlement].

72. Awati, *supra* note 70.

73. Press Release, AG Reaches Settlement, *supra* note 71.

74. *Id.*

75. Cohen, *supra* note 51; *see also* Press Release, AG Reaches Settlement, *supra* note 71.

alternatives to "abortion-minded women."[76] Once an individual "tripped" the geofence, the tailored advertisements appeared in an open application or web browser on the individual's cell phone.[77] Further, the geofence "tagged" the individual's device so more targeted advertisements "can be directly pushed to it whenever the same app or browser page is opened in the future."[78]

All the while, the individuals targeted based on their physical proximity to reproductive health centers likely did not realize that using their cell phone would disclose their location information to a third-party marketing company.[79] In reaching a settlement agreement with the marketing company to cease its geofencing, the Massachusetts Attorney General noted geofencing may provide benefits to individuals, but "it is also a technology that has the potential to digitally harass people and interfere with health privacy."[80]

As discussed above, cell phones are able to collect individuals' location information to an increasingly precise degree.[81] Indeed, cell phones are the "easiest means to gather the most comprehensive data about a person's public—and *private*—movements available."[82] However, cell phones are just one tool in the toolbox of ways a company may track individuals' location information.[83] In fact, smartphone applications may be a more useful, efficient tool to track and collect individuals' location information.[84]

---

76. Press Release, AG Reaches Settlement, *supra* note 71.

77. *Id.*

78. *Id.*

79. *See id.*

80. *Id.*

81. *See supra* notes 57–63 and accompanying text; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (noting "the accuracy of CSLI is rapidly approaching GPS-level precision").

82. United States v. Powell, 943 F. Supp. 2d 759, 780 (E.D. Mich. 2013) (emphasis in original).

83. *See* Boshell, *supra* note 12.

84. *See* Sara Morrison, *The Hidden Trackers in Your Phone, Explained*, VOX (July 8, 2020, 10:30 AM), https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location [https://perma.cc/TWS7-G2LH].

2. *Smartphone applications*

Companies use smartphone applications to collect location information for a variety of reasons.[85] Companies may create targeted advertising, generate maps and monitor traffic, or let people know when stores are busy.[86] To accomplish their objectives, companies use software development kits ("SDKs") to track individuals' movements as their cell phone connects with GPS, Wi-Fi, and cell towers.[87] The use of SDKs allow companies to efficiently capture and track the application user's precise location, including the amount of time the user spends in any given location.[88] Moreover, SDKs can even capture and track the user's location information when the application is running in the background or when the application is completely inactive.[89] The ability to collect location information continuously makes SDKs one of the most useful, efficient methods used to track an individual's location information.[90]

While similar, location tracking via SDKs in smartphone applications differs from location tracking via cell phones in various ways.[91] The main difference is the type of companies collecting users' location information through each medium.[92] Although both cell phones and smartphone applications collect location information in similar ways,[93] the companies that track location information via cell phones are cell service providers,

85. Valentino-DeVries, *supra* note 37.

86. *Id.*

87. Morrison, *supra* note 84; Stacey Gray, *FTC Settles with Major Ad Platform for Deceptive Location Tracking via Wi-Fi*, FUTURE OF PRIV. F. (June 22, 2016), https://fpf.org/blog/ftc-settles-major-ad-platform-deceptive-location-tracking-via-wi-fi/ [https://perma.cc/4H5F-HZQ6].

88. *See* Boshell, *supra* note 12 ("[R]eal-time location tracking compiles a precise and continuous location record of the individual's whereabouts indefinitely.").

89. James Temperton, *Uber Can Now Track Your Location Even When You're Not on a Ride. Here's How to Turn It Off*, WIRED (Feb. 12, 2016, 10:06 AM), https://www.wired.co.uk/article/uber-track-location-data-update-turn-off [https://perma.cc/787X-54K9].

90. *See* Morrison, *supra* note 84.

91. *See id.*

92. *See id.*

93. *Compare* LEVINSON-WALDMAN, *supra* note 44 (discussing the method in which cellphone location data is collected), *with* Gray, *supra* note 87 (discussing the method in which smartphone app location data is collected).

such as Verizon,[94] while the companies that track location information via smartphone applications are the application's owners, such as Google.[95]

In that sense, location tracking via smartphone applications and SDKs is far more expansive in scope than location tracking via cell phones because of the sheer amount of applications and application owners that one user interacts with as compared to cell phone service providers.[96] The opportunity for companies to collect location information via applications is far more expansive than the same ability via cell phones.[97] The substantial level of available applications, in conjunction with SDKs, provides companies the ability to track millions of individuals' location information continuously, irrespective of whether the application is being used, idling in the background, or inactive.[98]

Companies regularly use SDKs in their applications to collect users' location information to provide the application's intended services, such as fitness tracking.[99] However, location tracking, even for purposes of the application's intended services, may pose risks to users when the location information is disseminated to third parties or the public.[100] For example, Strava, a San Francisco-based online fitness company, collects

---

94. *See Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, AM. C.L. UNION, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart [https://perma.cc/C77H-2ELX] (comparing the location data retention policies of major cell service providers).

95. *See* Morrison, *supra* note 84.

96. *See* L. Ceci, *Number of Active Apps from the Apple App Store 2008–2022*, STATISTA (May 15, 2023), https://www.statista.com/statistics/268251/number-of-apps-in-the-itunes-app-store-since-2008/ [https://perma.cc/GLP2-FU4R] (noting Apple's App Store offers more than four million applications and games); *see also* Petroc Taylor, *Wireless Carriers in the U.S. by the Number of Subscribers 2013–2020, by Quarter*, STATISTA (Jan. 18, 2023), https://www.statista.com/statistics/283507/subscribers-to-top-wireless-carriers-in-the-us/ [https://perma.cc/9452-XQY8] (noting the number of subscribers to the top cell phone service providers in the United States).

97. *See* Ceci, *supra* note 96; Taylor, *supra* note 96.

98. *See* Morrison, *supra* note 84; Temperton, *supra* note 89.

99. *See* Ashley Thomas, *No Place to Hide: Privacy Implications of Geolocation Tracking and Geofencing*, AM. BAR ASS'N (Jan. 17, 2020), https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/no-place-hide-privacy-implications-geolocation-tracking-and-geofencing/?login [https://perma.cc/5BAN-UZL7].

100. *See id.*

the location information of over 100 million users in 195 countries around the world.[101] Strava's smartphone application provides its users with the ability to monitor their fitness performances while also comparing their performance with other users.[102] In addition, Strava analyzes the collected location of its users—trillions of location data points—to generate a heatmap that allows Strava's users to "discover new places to be active."[103] The heatmap reflects the aggregated location information of Strava's users who post their workouts publicly on the application to give other users the ability to follow the same routes for their workouts.[104]

The heatmap is a key aspect of Strava's appeal to its users; however, such an extensive collection and dissemination of location information potentially carries grave privacy risks for Strava's users.[105] For instance, in 2018, an Australian university student revealed that Strava's heatmap made it easy to determine the locations of United States military bases and the daily fitness routines of military personnel deployed to those bases.[106] The student's analysis of Strava's heatmap showed how easy it was to determine the military personnel's precise movements and patrolled routes from military bases, including in the then-active combat zones of Afghanistan, Iraq, and Syria.[107] After this headline-grabbing revelation, the United States Department of Defense issued a policy prohibiting military personnel from using GPS functions, such as Strava's application, while in

101. *About Us*, STRAVA, https://www.strava.com/about [https://perma.cc/LUU3-KP95].

102. Thomas, *supra* note 99.

103. *Heatmap Updates*, STRAVA (Mar. 13, 2018), https://blog.strava.com/press/heatmap-updates/ [https://perma.cc/D2TW-6M2V]. The brighter the route on the heatmap, the more that route has been used and tracked by Strava's users. *See* Drew Robb, *Building the Global Heatmap*, MEDIUM (Nov. 1, 2017), https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de [https://perma.cc/E8QM-BDLM]. To examine Strava's heatmap, *see Global Heatmap*, STRAVA, https://www.strava.com/heatmap#2.39/-71.58975/9.34282/hot/all [https://perma.cc/P727-V5SS].

104. *See Heatmap Updates*, *supra* note 103.

105. *See* Thomas, *supra* note 99.

106. *Id.*; *Fitness App Strava Lights Up Staff at Military Bases*, BRIT. BROAD. CORP. (Jan. 29, 2018), https://www.bbc.com/news/technology-42853072 [https://perma.cc/JPD9-CUTK].

107. Thomas, *supra* note 99; *Fitness App Strava Lights up Staff at Military Bases*, *supra* note 106.

deployed locations.[108] The United States government, at least in the context of its own military personnel, recognized the privacy concerns surrounding companies' unregulated collection and disclosure of individuals' locations and its potential negative impact on the ability to freely move.[109] While this may seem like an extreme example, it is not far-fetched that individuals would use obtained location information to track down another whom they wish to harass or physically harm, thus interfering with the victim's ability to safely, freely travel.[110]

In addition to collecting location information while the application is in use, SDKs can generate and collect users' location information even while the application is not providing its intended service, such as when the application is operating in the background or is inactive.[111] For example, in 2016, Uber began collecting its users' location information at all times, not just when an individual actively used the ridesharing application.[112] In a software update, Uber gave itself permission to continually collect its users' locations so long as the application is still running in the background.[113] Uber claimed it only collected users' location information for up to five minutes after a ride; however, Uber continued to collect the information long after five

108. Thomas, *supra* note 99; Jim Garamone, *New Policy Prohibits GPS Tracking in Deployed Settings*, U.S. DEP'T OF DEF. (Aug. 6, 2018), https://www.defense.gov/News/News-Stories/Article/Article/1594486/new-policy-prohibits-gps-tracking-in-deployed-settings/ [https://perma.cc/8Z6R-SHWY].

109. *See* Garamone, *supra* note 108. Pentagon spokesman Army Col. Robert Manning III told reporters that "[t]he rapidly evolving market of devices, applications and services with geolocation capabilities presents a significant risk to the Department of Defense personnel on and off duty, and to our military operations globally." *Id.* Further, Col. Manning stated the use of these applications "potentially create[s] unintended security consequences and increased risk to the joint force and mission." *Id.*

110. *See, e.g.*, Thompson & Warzel, *Twelve Million Phones*, *supra* note 10 (noting "there are often few protections to stop an individual analyst with access to such data from tracking an ex-lover or victim of abuse"); Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data that Tracked Gay Priests*, WASH. POST (Mar. 9, 2023, 8:52 AM), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/ [https://perma.cc/3R32-AG3G] (noting a group obtained an individual's location information and attempted a "character assassination of a private citizen for some kind of political reason" based on information the individual did not know was being tracked).

111. *See* Temperton, *supra* note 89.

112. *Id.*

113. *Id.*

minutes.[114] Indeed, Uber collected its users' location information even "when the app [was] not being used for a ride and, more interestingly, [was] being used to monitor rides with competing services."[115] Since Uber relies on its users' location to provide ridesharing services, if a user did not want his location to be continuously tracked, the user needed to toggle the location permission button from on to off before and after each ride.[116] Uber users were rightfully concerned over Uber's continuous location tracking given reports of Uber's misuse of its internal tracking technology, which has been dubbed "God View."[117]

As cell phone-based location tracking technologies continue to advance, the American people and Congress should remain vigilant regarding the associated potential abuses and risks, such as the potential for individuals to use location information to influence, stalk, and harass others.[118] Technology will only continue to advance and create more expansive, pervasive tools and methods for companies to track and collect individuals' location information, such as facial recognition,[119] which will continue to have an impact on Americans' ability to travel freely.

---

114. DARREN R. HAYES, CHRISTOPHER SNOW & SALEH ALTUWAYJIRI, GEOLOCATION TRACKING AND PRIVACY ISSUES ASSOCIATED WITH THE UBER MOBILE APPLICATION 6 (2017), http://proc.conisar.org/2017/pdf/4511.pdf [https://perma.cc/ZKC3-XUBG].

115. *Id.*

116. Temperton, *supra* note 89.

117. Sarah Perez, *Uber Explains Why It Looks Like Its App Is Still Tracking Your Location, Long After Drop-Off*, TECHCRUNCH (Dec. 22, 2016, 7:33 PM), https://techcrunch.com/2016/12/22/uber-explains-why-it-looks-like-its-app-is-still-tracking-your-location-long-after-drop-off/ [https://perma.cc/FD3E-QGR4]; *see also* Kashmir Hill,*'God View:' Uber Allegedly Stalked Users for Party-Goers' Viewing Pleasure*, FORBES (Oct. 3, 2014, 11:32 AM), https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/ [https://perma.cc/BK4V-PCNB] ("One of the go-to Uber party tricks for [its] events is to treat the attendees to Uber's 'God View,' which lets them see all of the Ubers in a city and the silhouettes of waiting Uber users who have flagged cars.").

118. *See* discussion *supra* Section I.A; *see also* Emily Baker-White, *Exclusive: TikTok Spied on Forbes Journalists*, FORBES (Dec. 22, 2022, 2:53 PM), https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance [https://perma.cc/5JEC-5674] (discussing how employees of ByteDance, Tik-Tok's parent company, spied on Forbes journalists); Justin Sherman, *Unpacking TikTok, Mobile Apps and National Security Risks*, LAWFARE (Apr. 2, 2020, 10:06 AM), https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks [https://perma.cc/DFS7-4B3L] (discussing the risks associated with Tik-Tok's collection of data on U.S. persons and government employees).

119. *See* Drew Harwell, *FBI, Pentagon Helped Research Facial Recognition for Street Cameras, Drones*, WASH. POST (Mar. 7, 2023, 6:00 AM), https://www.washingtonpost.com/technology/2023/03/07/facial-recognition-fbi-dod-research-aclu/ [https://perma.cc/FN9W-ZSBB].

B. *Advances in Technology: Facial Recognition*

Advances in technology increasingly allow companies to track individuals' locations and use the information to affect individuals' ability to travel freely.[120] Currently, facial recognition technology is becoming increasingly controversial because of its pervasiveness and the potentially negative impacts it can have on an individual's ability to travel freely.[121] Cities increasingly implement camera system networks, typically attached to street lights and intersections, that record images every minute of every day.[122] As citywide camera networks proliferate, so does facial recognition technology.[123] Additionally, the federal government, via the Customs and Border Protection Agency, has used facial recognition technology at United States borders for years.[124] Further, the Transportation Security Administration ("TSA") is currently testing, and implementing, the technology for passenger screening at select major domestic airports with the hope of using it across the United States in the next couple of years.[125] The TSA's use of facial recognition technology is primarily aimed at "improving security" and

120. *See, e.g.*, Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES, https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html [https://perma.cc/F3VG-75VP] (Jan. 3, 2023) (describing how guards at Radio City Music Hall used facial recognition to identify and then remove an attorney from the Christmas Spectacular show).

121. *See* Harwell, *supra* note 119. The Federal Bureau of Investigation and the United States Department of Defense have researched and developed facial recognition software they "hope[] could be used to identify people from footage captured by street cameras and flying drones . . . ." *Id.* However, civil liberties advocates are concerned over the government's development and use of facial recognition technology because it "give[s] the government the ability to pervasively track as many people as they want for as long as they want"—a "nightmare scenario." *Id.*

122. *See* Drew Harwell & Danny Freedman, *Memphis's SkyCop Cameras Couldn't Prevent Tyre Nichols's Beating Death*, WASH. POST, https://www.washingtonpost.com/technology/2023/02/02/skycop-nichols-memphis-crime/ [https://perma.cc/W8HA-JA69] (Feb. 2, 2023, 9:24 AM).

123. *Id.*

124. *See* Elaine Glusac, *What You Need to Know About Facial Recognition at Airports*, N.Y. TIMES (Feb. 26, 2022), https://www.nytimes.com/2022/02/26/travel/facial-recognition-airports-customs.html [https://perma.cc/5FY3-UR9B].

125. Geoffrey A. Fowler, *TSA Now Wants to Scan Your Face at Security. Here Are Your Rights.*, WASH. POST (Dec. 2, 2022, 7:00 AM), https://www.washingtonpost.com/technology/2022/12/02/tsa-security-face-recognition/ [https://perma.cc/YY2Y-XL7L].

"efficiency."[126] Airline companies, such as Delta Air Lines, are also looking to use facial recognition technology in various processes, such as bag checking and flight boarding.[127] Airlines generally have the same goals as the federal government: to improve security and, most importantly for the airlines, to increase efficiency.[128]

However, the use of facial recognition can have the opposite effect, negatively interfering with an individual's ability to freely travel instead of facilitating secure and efficient travel.[129] Indeed, instead of improving efficiency, facial recognition at airports has been encumbering travel.[130] For instance, while the use of the technology at airports is voluntary, TSA agents are reportedly operating "as if they are mandatory, providing no signs that indicate passengers have a right to opt out."[131] This leaves passengers with the option to either catch their flight or potentially face "significant delay."[132]

While potential delays during travel is more of an inconvenience than interference, facial recognition has also been used to prevent individuals from attending events with their families.[133] For example, in 2022, Madison Square Garden Entertainment ("MSG Entertainment") in New York used facial recognition to keep "enemies" out of its venues.[134] Specifically, when a lawyer attempted to attend the Rockette's Christmas Spectacular at Radio City Music Hall with her daughter, guards used facial recognition to identify her and prevented her from entering the

126. *Id.*

127. *See* Elaine Glusac, *Your Face Is, or Will Be, Your Boarding Pass*, N.Y. TIMES, https://www.nytimes.com/2021/12/07/travel/biometrics-airports-security.html [https://perma.cc/5FY3-UR9B] (Jan. 11, 2022).

128. *Id.*

129. *See, e.g.*, Hill & Kilgannon, *supra* note 120; Shira Ovide, *You Can Say No to a TSA Face Scan. But Even a Senator Had Trouble*, WASH. POST, https://www.washingtonpost.com/technology/2023/07/11/tsa-airport-security-facial-recognition/ [https://perma.cc/9H2G-LB2D] (July 11, 2023, 5:12 PM) ("When [Senator] Merkley said no to the face scan at Washington's Reagan National Airport, he was told it would cause significant delay.").

130. *See* Ovide, *supra* note 129.

131. *Id.*

132. *Id.*

133. *See* Hill & Kilgannon, *supra* note 120.

134. *Id.*

concert.[135] MSG Entertainment's security flagged the lawyer whose name was on an "attorney exclusion list," which had been created to prevent any lawyer from any law firm suing MSG Entertainment from patronizing its venues.[136] MSG Entertainment's use of facial recognition to ban individuals from its venues has sparked criticism from the banned individuals, civil liberties advocates, and New York's Attorney General, as it negatively interferes with individuals' freedoms.[137]

Advances in technology, including cell phones and facial recognition, can be used to benefit or repress society.[138] As these technologies continue to proliferate, the American people and Congress should remain cognizant of the impact new technologies have on the ability to freely travel throughout the United States. The following Part of this Note examines the fundamentality of the right to travel in the United States to illustrate why it should be protected from abuses of advances in location tracking technology.

II. THE RIGHT TO TRAVEL IN THE UNITED STATES

Many Americans travel from state to state without giving a second thought to their intrinsic, albeit unenumerated, right to interstate travel provided by the United States Constitution.[139] Nonetheless, the Supreme Court of the United States has recognized the fundamental importance of the right to travel in American life, calling it "a basic right under the

135. *Id.*

136. *Id.* ("[MSG Entertainment] says 'litigation creates an inherently adversarial environment' and so it is enforcing the list with the help of computer software that can identify hundreds of lawyers via profile photos on their firms' own websites . . . .").

137. *Id.*; Noah Sheidlower, *NY AG Letitia James Presses MSG Over the Use of Facial Recognition Technology*, CNBC, https://www.cnbc.com/2023/01/25/letitia-james-presses-msg-facial-recognition-tech.html [https://perma.cc/3JX9-JC6U] (Jan. 26, 2023, 3:54 PM) (quoting Letitia James, stating: "Anyone with a ticket to an event should not be concerned that they may be wrongfully denied entry based on their appearance, and we're urging MSG Entertainment to reverse this policy").

138. *See* Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES: WIRECUTTER (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ [https://perma.cc/G9G8-GNV3].

139. Wilhelm, *supra* note 1.

Constitution."[140] But how is the basic right of freedom to travel relevant to the privacy of an individual's location information? The answer must start with the evolution of the right to travel in the United States.

Accordingly, Section A first examines the historical trajectory of the right to travel and how the Supreme Court concluded the freedom of travel is a basic right protected against government and private interference. Then, Section B examines the Commerce Clause,[141] and its importance regarding regulation of private interference with the right to travel. As one of the most powerful Constitutional sources of Congress's regulatory authority, the Commerce Clause grants Congress the power to regulate: "the use of the channels of interstate commerce," "the instrumentalities of interstate commerce, or persons or things in interstate commerce, even though the threat may come only from intrastate activities," and "those activities having a substantial relation to interstate commerce."[142] From this broad authority, not only does Congress possess the power to regulate the movement of individuals, it also has the power to protect individuals from interference on their free movement.[143]

A. *The Historical Evolution of the Right to Travel in the United States*

The right to travel in American jurisprudence is as old as the United States.[144] After the United States declared independence from Great Britain in 1776,[145] the newly formed Continental Congress drafted the Articles of Confederation to create a union

140. United States v. Guest, 383 U.S. 745, 758 (1966).

141. U.S. CONST. art. I, § 8, cl. 3 ("The Congress shall have Power . . . To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes.").

142. United States v. Lopez, 514 U.S. 549, 558–59 (1995) (citations omitted).

143. *Guest*, 383 U.S. at 759 ("[T]he federal commerce power authorizes Congress to legislate for the protection of individuals from violations . . . that impinge on their free movement . . . .").

144. *See* Leonard B. Boudin, *The Constitutional Right to Travel*, 56 COLUM. L. REV. 47, 47–48 (1956); ARTICLES OF CONFEDERATION of 1781, art. IV, para. 1.

145. THE DECLARATION OF INDEPENDENCE (U.S. 1776).

of sovereign states from the original thirteen British Colonies.[146] The Continental Congress recognized the importance of travel between the new sovereign states and solidified the right to travel in the Articles of the Confederation.[147] Specifically, "[t]he better to secure and perpetuate mutual friendship and intercourse among the people of the different states," the Articles of Confederation affirmed that the American people "shall be entitled to all privileges and immunities of free citizens in the several states, and the people of each state shall have free ingress and regress to and from any other state, and shall enjoy therein all the privileges of trade and commerce."[148] However, the Articles of Confederation's deficiencies led the Founders to replace the Articles of Confederation with the newly drafted United States Constitution.[149] Although the new Constitution kept the first clause of Article IV of the Articles of Confederation regarding privileges and immunities, it did not incorporate the second clause granting the right to travel between the states.[150]

The exact reason the drafters of the Constitution decided not to enumerate the right to travel into the Constitution is a subject of debate.[151] One argument is the Framers did not regard the right to travel as a fundamental right.[152] Proponents of this

146. *Policies and Problems of the Confederation Government*, LIBR. OF CONG., https://www.loc.gov/classroom-materials/united-states-history-primary-source-timeline/new-nation-1783-1815/policies-and-problems-of-the-confederation-government/ [https://perma.cc/R3A8-KHGD].

147. *See* ARTICLES OF CONFEDERATION of 1781, art. IV, para. 1; *see also* Zobel v. Williams, 457 U.S. 55, 79 (1982) (O'Connor, J., concurring) (stating the right to travel is "expressly recognized" by Article IV of the Articles of Confederation).

148. ARTICLES OF CONFEDERATION of 1781, art. IV, para. 1.

149. *See* NCC STAFF, *On This Day, the Articles of Confederation Are Approved*, NAT'L CONST. CTR. (Mar. 1, 2023), https://constitutioncenter.org/blog/on-this-day-our-first-flawed-constitution-went-into-effect/ [https://perma.cc/RLB7-XEU2] (providing a list of issues that led the Founders to replace the Articles of Confederation with the Constitution).

150. Nicole I. Hyland, Note, *On the Road Again: How Much Mileage Is Left on the Privileges or Immunities Clause and How Far Will It Travel?*, 70 FORDHAM L. REV. 187, 203 (2001); U.S. CONST. art. IV, § 2 ("The Citizens of each State shall be entitled to all Privileges and Immunities of Citizens in the several States . . . .").

151. *See* Gregory B. Hartch, Comment, *Wrong Turns: A Critique of the Supreme Court's Right to Travel Cases*, 21 WM. MITCHELL L. REV. 457, 476 (1995); Sobel, *supra* note 2, at 644–45.

152. Hartch, *supra* note 151, at 476 ("[O]riginalist evidence points to jettisoning the right [to travel] altogether.").

argument suggest the omission of the right to travel, combined with Congress' power to regulate interstate travel under the Commerce Clause, "strongly suggests that the Framers did not view the right to travel as vital to the new nation."[153] However, the opposing argument is that "[t]he right to travel pervades U.S. history."[154] Indeed, as the argument goes, Thomas Jefferson believed "freedom of movement is a personal liberty by birth."[155] The Supreme Court, for its part in the debate, regards the right to travel as "elementary" and "conceived from the beginning to be a necessary concomitant of the stronger Union the Constitution created."[156] In any event, United States jurisprudence has long recognized the right to travel "as a basic right under the Constitution."[157]

The United States Judiciary has inferred the existence of a right to interstate travel from numerous provisions and concepts embedded in the Constitution.[158] As early as 1823, in *Corfield v. Coryell*, Justice Bushrod Washington, writing for the Circuit Court for the Eastern District of Pennsylvania, acknowledged the right to interstate travel as a component of the privileges and immunities of citizens under Article IV of the Constitution.[159] Justice Washington held a citizen's right to travel through, or reside in, another state is a privilege "deemed to be fundamental" by the Constitution.[160] Echoing the Articles of Confederation, Justice Washington regarded the right to travel as essential to better "secure and perpetuate mutual

153. *Id.*

154. Sobel, *supra* note 2, at 641.

155. *Id.* (citing THOMAS JEFFERSON, ARGUMENT IN THE CASE OF HOWELL V. NETHERLAND, THE WRITINGS OF THOMAS JEFFERSON 474 (1892)); Kent v. Dulles, 357 U.S. 116, 127 (1958) ("Freedom to travel is, indeed, an important aspect of the citizen's 'liberty.'").

156. United States v. Guest, 383 U.S. 745, 758 (1966).

157. *Id.*

158. *See* Wilhelm, *supra* note 1, at 2466.

159. Corfield v. Coryell, 6 F. Cas. 546, 552 (C.C.E.D. Pa. 1823) (No. 3,230); *see also* THE FEDERALIST NO. 80 (Alexander Hamilton) (regarding the Privileges and Immunities Clause as "the basis of the Union").

160. *Corfield*, 6 F. Cas. at 552.

friendship and intercourse among the people of the different states."[161]

A couple decades later, Supreme Court Chief Justice Roger Taney, in his dissent in *The Passenger Cases*, recognized the right to interstate travel as embedded in various provisions of the Constitution and national citizenship.[162] Similar to Justice Washington in *Corfield*, the Chief Justice believed the Privileges and Immunities Clause intended to secure citizens the "freest intercourse" between the States.[163] Further, the Chief Justice held: "We are all citizens of the United States; and, as members of the same community, must have the right to pass and repass through every part of it without interruption, as freely as in our own States."[164] The Chief Justice's reliance on national citizenship—a concept not defined in the Constitution at the time[165]—as the source of the right to travel reveals much about the right to travel's fundamentality, and pervasiveness, in United States history.[166]

In 1868, the Supreme Court confirmed the right to interstate travel for the first time in *Crandall v. Nevada*.[167] The Court, concerned restrictions on travel may prevent or burden the movement of citizens throughout the United States, recognized the right to travel as important to other fundamental rights, such as free access to the courts and public offices in every state.[168] In doing so, the Court officially endorsed the dissent's view in *The Passenger Cases* by basing the right to travel in part on the

161. *Id.* (quoting ARTICLES OF CONFEDERATION of 1781, art. IV); *see also* Sobel, *supra* note 2, at 642.

162. Smith v. Turner (The Passenger Cases), 48 U.S. (7 How.) 283, 492 (1849) (Taney, J., dissenting).

163. *Id.*; *see Corfield*, 6 F. Cas. at 552.

164. *The Passenger Cases*, 48 U.S. at 492.

165. Before the United States ratified the Fourteenth Amendment, the Constitution did not define citizenship. *See* Alexander M. Bickel, *Citizenship in the American Constitution*, 15 ARIZ. L. REV. 369, 369 (1973). After the Fourteenth Amendment's ratification, the Constitution defined national citizens as "[a]ll persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside." U.S. CONST. amend. XIV, § 1, cl. 1.

166. *See The Passenger Cases*, 48 U.S. at 492; Sobel, *supra* note 2, at 643.

167. Crandall v. Nevada, 73 U.S. (6 Wall.) 35, 49 (1868).

168. *Id.* at 46, 48.

Privileges and Immunities Clause and national citizenship.[169] The Court reasoned: "For all the great purposes for which the Federal government was formed we are one people, with one common country . . . [who] must have the right to pass and repass through every part of it without interruption."[170]

For roughly the next seventy-five years, the Supreme Court's right to travel doctrine remained essentially dormant.[171] Not until 1941, in *Edwards v. California*,[172] did the Supreme Court resurrect the right to travel doctrine, "marking the advent of the modern travel doctrine."[173] In *Edwards*, the Court unanimously upheld the right to travel under the Constitution, but it disagreed as to which Constitutional provision, or provisions, provided the right.[174] The majority relied on the Commerce Clause and held California could not "isolate itself from difficulties common to all [the States] by restraining the transportation of persons and property across its borders."[175] In his concurrence, Justice William Douglas argued the right to travel "occupies a more protected position in our constitutional system" than the Commerce Clause can provide.[176] Instead, Justice Douglas determined the right to travel derived from national citizenship protected by the Fourteenth Amendment's Privileges or Immunities Clause.[177] Justice Douglas reiterated the reasoning

169. *Id.* at 49 (citing *Passenger Cases*, 48 U.S. at 492).

170. *Id.* at 48–49 (quoting *Passenger Cases*, 48 U.S. at 492).

171. Andrew C. Porter, Comment, *Toward a Constitutional Analysis of the Right to Intrastate Travel*, 86 NW. U. L. REV. 820, 823–24 (1992).

172. Edwards v. California, 314 U.S. 160, 172–73 (1941).

173. Porter, *supra* note 171, at 824.

174. *Edwards*, 314 U.S. at 172–73, 177–78, 183; *see also* Porter, *supra* note 171, at 824.

175. *Edwards*, 314 U.S. at 172–73.

176. *See id.* at 177 (Douglas, J., concurring).

177. *Id.* at 178; *see also* U.S. CONST. amend. XIV, § 1, cl. 2 ("No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States . . . ."). The Fourteenth Amendment's Privileges or Immunities Clause, however, is essentially meaningless thanks to Justice Samuel Miller's holding in the *Slaughter-House Cases*. John Harrison, *Reconstructing the Privileges or Immunities Clause*, 101 YALE L. J. 1385, 1414 (1992); *see* Slaughter-House Cases, 83 U.S. (16 Wall.) 36, 78–79 (1873). In the *Slaughter-House Cases*, Justice Miller narrowly interpreted the Privileges or Immunities Clause to protect only those rights "which owe their existence to the Federal Government, its National character, its Constitution, or its laws." *Slaughter-House Cases*, 83 U.S. at 79. In dissent, Justice Field argued that Justice Miller incorrectly interpreted the Privileges or Immunities Clause because the narrow interpretation made the Clause "a vain and idle enactment, which accomplished

from *Corfield*, *The Passenger Cases*, and *Crandall* when he concluded that the right to travel, as integral to national citizenship, "stands on firm historical ground."[178]

From this firm historical ground, the Supreme Court, in 1966, considered for the first time whether the Constitution protects the right to travel from *private* interference.[179] In *United States v. Guest*, the Court held the defendants' conspiracy to interfere with African-American citizens' ability to travel freely violated their constitutional right to travel.[180] The Court's decision in *Guest*, like the Court's previous decisions, did not rely solely on one provision of the Constitution in affirming the right to travel.[181] Instead, the Court asserted the right to travel is a "basic right under the Constitution."[182] Nonetheless, the Court did recognize the Commerce Clause "authorizes Congress to legislate for the protection of individuals from violations . . . that impinge on their free movement . . . ."[183] Moreover, the Court held Congress can protect individuals' right to travel from violations by private actors, in addition to State actors.[184]

Over the next sixty years, the Supreme Court continually protected the right to travel from interference.[185] Although the

---

nothing . . . ." *Id.* at 96 (Field, J., dissenting); *see also* McDonald v. City of Chicago, 561 U.S. 742, 754–57 (2010) (discussing the *Slaughter-House Cases* and how "many legal scholars dispute the correctness of the narrow *Slaughter-House* interpretation"). Nonetheless, "it has always been common ground that [the Privileges or Immunities] Clause protects . . . the right to travel." Saenz v. Roe, 526 U.S. 489, 503 (1999).

178. *Edwards*, 314 U.S. at 181; *see also* Corfield v. Coryell, 6 F. Cas. 546, 552 (C.C.E.D. Pa. 1823) (No. 3,230); Smith v. Turner (The Passenger Cases), 48 U.S. (7 How.) 283, 492 (1849) (Taney, J., dissenting); Crandall v. Nevada, 73 U.S. (6 Wall.) 35, 49 (1868).

179. *See* Porter, *supra* note 171, at 826.

180. United States v. Guest, 383 U.S. 745, 757 (1966).

181. *Id.* at 757–59 ("Although there have been recurring differences in emphasis within the Court as to the source of the constitutional right of interstate travel, there is no need here to canvass those differences further. All have agreed that the right exists.").

182. *Id.* at 758.

183. *Id.* at 759.

184. *See id.*; *see also* Shapiro v. Thompson, 394 U.S. 618, 643 (1969) (Stewart, J., concurring) (holding the right to travel "is a right broadly assertable against private interference as well as governmental action").

185. *See, e.g.*, *Shapiro*, 394 U.S. at 638 (holding a state residency requirement violated the "fundamental right of interstate movement"); Saenz v. Roe, 526 U.S. 489, 500 (1999) (holding the right to travel "protects the right of a citizen of one State to enter and to leave another State, the right to be treated as a welcome visitor rather than an unfriendly alien when temporarily present in the second

Court varied on which Constitutional provisions provided the right to travel in its previous decisions, the Court agrees the Constitution protects the right to travel.[186] Indeed, the Court held the right to travel "occupies a position fundamental to the concept of our Federal Union."[187] This fundamental concept of the right to travel should be protected against interference from private and state actors alike—especially from technological interferences.

B. *The Commerce Clause and the Right to Travel*

The Commerce Clause of the Constitution grants Congress the authority to "regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."[188] The Commerce Clause is one of the most important and powerful legislative tools Congress has at its disposal, as it grants Congress "the power to regulate; that is, to prescribe the rule by which commerce is to be governed."[189] The Commerce power, "like all others vested in Congress, is complete in itself, may be exercised to its utmost extent, and acknowledges no limitations, other than are prescribed in the constitution."[190] Thus, from the earliest days of the United States, the Supreme Court has recognized Congress's Commerce Clause powers as a "central basis for the assertion of national regulatory authority."[191]

Using the Commerce Clause as its central basis for regulatory authority, Congress has the power to protect the right to travel from interference by private and state actors alike.[192] For

State, and, for those travelers who elect to become permanent residents, the right to be treated like other citizens of that State").

186. *See* discussion Section II.A.

187. *Guest*, 383 U.S. at 757.

188. U.S. CONST. art. I, § 8, cl. 3.

189. Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1, 196 (1824).

190. *Id.*

191. NOAH R. FELDMAN & KATHLEEN M. SULLIVAN, CONSTITUTIONAL LAW 113 (20th ed. 2019); *see also Gibbons*, 22 U.S. at 196.

192. *See Guest*, 383 U.S. at 759, 759 n.17 ("Although these cases in fact involved governmental interference with the right of free interstate travel, their reasoning fully supports the conclusion that the constitutional right of interstate travel is a right secured against interference from any source whatever, whether governmental or private."). Although the Supreme Court has determined the

example, in *Heart of Atlanta Motel v. United States*, the Supreme Court considered whether the Commerce Clause grants Congress the authority to regulate a private actor's refusal to rent motel rooms to traveling African Americans.[193] The Court determined Congress had the authority under the Commerce Clause to regulate the private actor's actions because the refusal to rent motel rooms impeded African-American citizens' right to travel.[194] The Court noted the right to interstate travel has long been considered commerce; therefore, Congress has long had the power to promote interstate travel by passing legislation under its Commerce Clause authority.[195] Moreover, the Court reaffirmed Congress' power to remove obstructions that impede commerce, such as interferences with the right to travel, whether the obstructions impede interstate commerce or local activities that have a "substantial and harmful effect" on commerce.[196]

In *Katzenbach v. McClung*, a companion case to *Heart of Atlanta Motel*, the Supreme Court likewise determined a private actor's refusal to serve African Americans in his restaurant "had a direct and highly restrictive effect upon interstate travel."[197] The Court reasoned the interference discouraged and obstructed American citizens from exercising their right to travel.[198] Once again, the Court noted that "Congress acted well within its power to protect and foster commerce" by protecting the right to travel.[199] Thus, the Court reaffirmed Congress' "broad and sweeping" Commerce Clause power to legislate travel.[200]

---

right to travel is protected via numerous Constitutional provisions, it is the Commerce Clause that gives Congress the authority to enact legislation to protect the right. *See id.* ("It is also well settled in our decisions that the federal commerce power authorizes Congress to legislate for the protection of individuals from violations . . . that impinge on their free movement . . . .").

193. Heart of Atlanta Motel v. United States, 379 U.S. 241, 249 (1964).

194. *Id.* at 253, 261–62.

195. *Id.* at 255–58.

196. *Id.* at 258, 261–62.

197. Katzenbach v. McClung, 379 U.S. 294, 300 (1964).

198. *Id.*

199. *Id.* at 304.

200. *Id.* at 305.

As right to travel cases suggest, Congress maintains the power to legislate to protect the right to travel against private interferences.[201] Indeed, because the Supreme Court has repeatedly determined the right to travel derives from, for example, the concept of national citizenship, Congress may actually have a "correlative duty" to protect the right to travel against private interference.[202] Therefore, Congress not only has the power, but may also have a duty, to use its Commerce Clause authority to protect citizens from interferences that impinge on their right to travel, including any potential inferences from location tracking.[203] In exercising its Commerce Clause authority, Congress should look to the Health Insurance Portability and Accountability Act for a useful framework to emulate, as it regulates companies' collection, use, and disclosure of individuals' sensitive information.

III. THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

In 1996, Congress used its Commerce Clause authority to enact the Health Insurance Portability and Accountability Act ("HIPAA"), a watershed piece of legislation in the security and privacy of individuals' sensitive medical information.[204] Congress enacted HIPAA for two main reasons: to ensure individuals continue to receive health insurance coverage while between jobs and to secure individuals' health information.[205] Congress intended for HIPAA to protect individuals' health information while maintaining the flow of individuals' health

201. *See* United States v. Guest, 383 U.S. 745, 758–59 (1966); *Heart of Atlanta Motel*, 379 U.S. at 258, 261–62; *Katzenbach*, 379 U.S. at 305.

202. *Membership Has Its Privileges and Immunities: Congressional Power to Define and Enforce the Rights of National Citizenship*, 102 HARV. L. REV. 1925, 1940 (1989).

203. *See id.*; *Guest*, 383 U.S. at 759.

204. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 195(a), 110 Stat. 1936, 1991.

205. Steve Alder, *Why Is HIPAA Important?*, HIPAA J. (Feb. 1, 2023), https://www.hipaajournal.com/why-is-hipaa-important/ [https://perma.cc/MYC7-PV3U].

information when needed.[206] Hence, HIPAA ensures that all Covered Entities,[207] many of which are companies, implement various safeguards to secure individuals' personal and health information.[208] But, HIPAA also permits the flow of individuals' information to third parties under certain circumstances, such as to help buttress clinical research and improve the medical community.[209]

To accomplish Congress's goals and implement HIPAA's requirements, the United States Department of Health and Human Services ("HHS") established the Standards for Privacy of Individual Identifiable Health Information, better known as the Privacy Rule,[210] and the Security Rule, which protects a subset of information covered by the Privacy Rule.[211] Together, the Privacy and Security Rules protect individuals' Protected Health Information by requiring authorization or consent,[212] de-identification,[213] and secure storage of individuals' information.[214]

A. *The HIPAA Privacy Rule*

Under the Privacy Rule, any individually identifiable information relating to an individual's healthcare, in addition to

206. *See HIPAA Privacy Rule*, HIPAA J., https://www.hipaajournal.com/hipaa-privacy-rule/ [https://perma.cc/6HHT-GH5Z].

207. 45 C.F.R. § 160.103 (2023). Covered Entities are health plans, health care clearinghouses, and health care providers. *Id.*

208. Alder, *supra* note 205.

209. Jill McKeon, *De-Identification of PHI According to the HIPAA Privacy Rule*, HEALTHITSECURITY (Oct. 15, 2021), https://healthitsecurity.com/features/de-identification-of-phi-according-to-the-hipaa-privacy-rule [https://perma.cc/Q2RA-2JUN].

210. *See* 45 C.F.R. §§ 160.101–05, 164.102–06, 164.500–34; U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003) [hereinafter SUMMARY OF THE HIPAA PRIVACY RULE], https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/HF7H-7MR5].

211. *See* 45 C.F.R. §§ 164.302–18; *The Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/6KK6-QZNT] (Oct. 20, 2022).

212. 45 C.F.R. § 164.506(b); SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4.

213. 45 C.F.R. §§ 164.502(d), 164.514(a)–(b); *see* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 3–4.

214. *See, e.g.*, 45 C.F.R. §§ 164.308–12 (providing examples of the information storage protections built into HIPAA); *see Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (Oct. 19, 2022) [https://perma.cc/E3AP-QQ7T].

individually identifiable non-health information, is considered Protected Health Information ("PHI") and maintained in designated record sets.[215] An individual's identifiable information (or PHI) may include his medical records, name, address, and birthday.[216] This information must be maintained in designated record sets, which are groups of records that comprise an individual's medical information.[217]

The Privacy Rule regulates access to an individual's PHI, how the PHI may be used, and when the PHI may be disclosed to third parties.[218] Additionally, the Privacy Rule issues "standards for individuals' privacy rights to understand and control how their health information is used."[219] HHS designed the Privacy Rule to be flexible, yet comprehensive, to strike a balance between protecting individuals' PHI and permitting important uses of the information.[220]

Under the Privacy Rule, an individual's PHI maintained in a designated record set is secured from unauthorized uses and disclosures by Covered Entities.[221] Unless otherwise required or permitted by the Privacy Rule,[222] all uses and disclosures by Covered Entities of an individual's PHI are prohibited, subject to the individual's, or a personal representative's, authorization and consent.[223] Such authorizations must be in writing with clear language that explains to the individual what PHI will be used or disclosed, to whom it may be disclosed, and for what purpose.[224] Further, the authorization must state if the Covered Entity is receiving financial compensation for the individual's

215. 45 C.F.R. §§ 160.103, 164.501; *HIPAA Privacy Rule*, *supra* note 206.

216. SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 3–4.

217. *See* 45 C.F.R. § 164.501.

218. S*ee id.* §§ 160.101–.552, 164.102–.106, 164.500–.534; *HIPAA Privacy Rule*, *supra* note 206.

219. SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210.

220. *Id.*

221. *See* 45 C.F.R. §§ 164.501–02. Business associates of Covered Entities are also subject to the HIPAA Privacy Rule. *Id.*; *see also id.* § 160.103 (defining who is considered a "business associate").

222. *See id.* § 164.502 (noting required and permitted uses and disclosures of PHI).

223. SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4; 45 C.F.R. § 164.502.

224. *Id.* at 9 (citing 45 C.F.R. §§ 164.508, 164.532).

PHI and include a warning about potential future disclosures of the information.[225]

The Privacy Rule's general requirement that a Covered Entity receive authorization before using or disclosing PHI gives individuals greater control over their information.[226] Authorization reflects the high value placed on an individual's confidentiality interests in their PHI.[227] Under the Privacy Rule, the individual's confidentiality interests are regarded more highly than the Covered Entity's interest in financial gain from the PHI.[228] However, to balance individuals' and Covered Entities' interests, the Privacy Rule permits Covered Entities to use and disclose de-identified PHI.[229] De-identified PHI "neither identifies nor provides a reasonable basis to identify an individual."[230] As such, de-identified PHI does not impact the individual's confidentiality interests, because the de-identified PHI is unlikely to identify the individual.[231]

To ensure the individual's PHI is de-identified, the Covered Entity must either receive "a formal determination by a qualified statistician" or "remov[e] [] specified identifiers of the individual and of the individual's relatives, household members,

---

225. *HIPAA Privacy Rule*, *supra* note 206. In addition to the HIPAA Privacy Rule, medical research is also governed by the Common Rule, officially known as the Federal Policy for the Protection of Human Subjects. 45 C.F.R. § 46.101(a); *45 CFR 46*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html [https://perma.cc/GUB7-UQEF] (Mar. 10, 2021). After its 2018 revision, the Common Rule requires "informed consent, whether written or oral," from individuals before any research can be conducted. § 46.116. To effectuate informed consent, the Common Rule sets out extensive requirements researchers must satisfy before any identifiable private information may be collected. *Id.*

226. *See* Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 984 (2017).

227. *Id.*

228. *Id.*

229. 45 C.F.R. §§ 164.502(d)(2), 164.514(a)–(b); *see* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4.

230. *See* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4.

231. *See Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale [https://perma.cc/S386-SDN6] (Oct. 25, 2022) [hereinafter *Guidance Regarding Methods for De-identification*]. Even when properly de-identified, a risk remains that the information can be re-identified. *Id.*

and employers."[232] When a Covered Entity chooses the latter, the Covered Entity must not have actual knowledge the de-identified PHI could be used to identify the individual.[233] These steps ensure the de-identification of PHI reduces privacy risks to individuals while also supporting the use of data for important endeavors, such as research or improving health care.[234]

The balance created by authorization and de-identification strikes at the heart of the HIPAA: protecting individuals' health information while maintaining the flow of individuals' health information when necessary to support clinical research and improve the medical community.[235] Indeed, the Privacy Rule's authorization and de-identification requirements "strike[] a balance that permits important uses of information, while protecting the privacy of people who seek care and healing."[236] However, this balance can only be maintained when safeguards are in place to secure PHI.[237] The HIPAA Security Rule provides for such safeguards.[238]

B. *The HIPAA Security Rule*

In addition to the Privacy Rule, HHS established the Security Rule to protect a subset of information covered by the Privacy Rule—electronic protected health information ("ePHI").[239] As the term suggests, ePHI is PHI which is "create[d], receive[d], maintain[ed] or transmit[ed] in electronic form."[240] To ensure a higher level of protection for individuals' ePHI, the Security Rule requires Covered Entities to establish administrative,

232. SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4; 45 C.F.R. § 164.514(b).

233. 45 C.F.R. § 164.514(b)(2)(ii).

234. *See Guidance Regarding Methods for De-identification*, *supra* note 231.

235. *See HIPAA Privacy Rule*, *supra* note 206; McKeon, *supra* note 209.

236. SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 1.

237. *See The Security Rule*, *supra* note 211.

238. 45 C.F.R. §§ 160.101–.552, 164.102–.106, 164.302–.318 (2023); *The Security Rule*, *supra* note 211.

239. *The Security Rule*, *supra* note 211; 45 C.F.R. §§ 160.101–.552, 164.102–.106, 164.302–.318; *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CDC (June 27, 2022), https://www.cdc.gov/phlp/publications/topic/hipaa.html [https://perma.cc/85YY-Y2HJ].

240. *Summary of the HIPAA Security Rule*, *supra* note 214.

physical, and technical safeguards.[241] These three safeguards ensure the confidentiality, integrity, and security of individuals' ePHI.[242]

First, administrative safeguards are policies and procedures that dictate how the Covered Entity will protect individuals' ePHI.[243] Specifically, "[a]dministrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the [C]overed [E]ntity's or business associate's workforce in relation to the protection of that information."[244] The administrative safeguards implement training and procedures for the Covered Entity's employees to secure individuals' ePHI, even if the employee does not have direct access to the protected information.[245] Administrative safeguards include: (1) security management processes; (2) assigned security responsibility; (3) workforce security; (4) information access management; (5) security awareness and training; (6) security incident procedures; (7) contingency plans; (8) evaluation plans; and (9) procedures regarding business associate contracts and other arrangements.[246] These administrative safeguards are the cornerstone for the Covered Entity's security regime designed to protect ePHI.[247]

Second, Covered Entities must implement physical safeguards to ensure the security of individuals' ePHI.[248] Physical

241. *HIPAA Security Rule & Risk Analysis*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis [https://perma.cc/4KZG-BJFD].

242. *Id.*

243. *See* 45 C.F.R. § 164.308; *HIPAA Security Rule & Risk Analysis*, *supra* note 241.

244. 45 C.F.R. § 164.304.

245. *HIPAA Security Rule & Risk Analysis*, *supra* note 241.

246. 45 C.F.R. § 164.308(a)(1)–(8), (b)(1).

247. CTRS. FOR MEDICARE & MEDICAID SERVS., DEP'T OF HEALTH & HUM. SERVS., SECURITY STANDARDS: ADMINISTRATIVE SAFEGUARDS 1 (2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf [https://perma.cc/6KA4-S7YE] [hereinafter SECURITY STANDARDS: ADMINISTRATIVE SAFEGUARDS].

248. 45 C.F.R. § 164.310; *see HIPAA Security Rule & Risk Analysis*, *supra* note 241.

safeguards are measures taken to protect the Covered Entity's physical infrastructure and equipment "from natural and environmental hazards, and unauthorized intrusion."[249] Physical safeguards include: (1) limiting physical access to individuals ePHI and the facilities which house ePHI; (2) specifying proper workstation functions; (3) establishing workstation security to prevent unauthorized users; and (4) establishing device and media controls.[250] These physical safeguards build on the administrative safeguards to protect individuals' ePHI from hazards and unauthorized intrusion.[251]

Finally, technical safeguards cover all technology that protect and control access to individuals' ePHI.[252] Covered Entities must implement technical safeguards that "reasonably and appropriately" preserve the necessary level of security for ePHI.[253] Covered Entities have some flexibility in determining what technical safeguards are "reasonable and appropriate for implementation in its organization."[254] Nonetheless, the Security Rule provides examples of reasonable and appropriate technical safeguards, including: (1) controlling access to ePHI; (2) controlling audits; (3) maintaining the integrity of the ePHI; (4) requiring authentication before access to ePHI is permitted; and (5) establishing transmission security to prevent unauthorized

249. 45 C.F.R. § 164.304 ("Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related building and equipment, from natural and environmental hazards, and unauthorized intrusion.").

250. § 164.310(a)–(d); *see also* CTRS. FOR MEDICARE & MEDICAID SERVS., DEP'T OF HEALTH & HUM. SERVS., SECURITY STANDARDS: PHYSICAL SAFEGUARDS 2–13 (2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf [https://perma.cc/XW2X-L34W] [hereinafter SECURITY STANDARDS: PHYSICAL SAFEGUARDS] (providing guidance for Covered Entities to comply with the physical safeguards required by HIPAA).

251. *See* SECURITY STANDARDS: PHYSICAL SAFEGUARDS, *supra* note 250, at 13.

252. 45 C.F.R. § 164.304 ("Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.").

253. CTRS. FOR MEDICARE & MEDICAID SERVS., DEP'T OF HEALTH & HUM. SERVS., SECURITY STANDARDS: TECHNICAL SAFEGUARDS 2 (2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf [https://perma.cc/W7R7-R27D] [hereinafter SECURITY STANDARDS: TECHNICAL SAFEGUARDS].

254. *Id.*

disclosure of ePHI.[255] As technology continues to advance, technical safeguards will become increasingly more important to buttress the administrative and physical safeguards and protected ePHI.[256]

Together, the three Security Rule safeguards ensure ePHI's confidentiality, integrity, and availability, while also protecting against reasonably anticipated threats, hazards, and unauthorized uses or disclosures of such information.[257] Moreover, the Privacy and Security Rules ensure individuals a minimum level of privacy protections for their PHI.[258] With the Privacy and Security Rules in place, individuals can have confidence and trust that their most sensitive information is protected.[259] Further, the Privacy and Security Rules provide the healthcare industry with the ability to "streamline administrative healthcare functions [and] improve efficiency" while still ensuring individuals' PHI is secure.[260]

The Privacy and Security Rules, and HIPAA in general, play an invaluable role in the efficiency, security, and privacy in the healthcare industry.[261] The HIPAA Privacy and Security Rules also lay a solid framework for other pieces of legislation that aim to protect sensitive information, such as location information.

IV. HIPAA AS A FRAMEWORK TO PROTECT THE RIGHT TO TRAVEL

An individual's location and health information are some of "the most sensitive categories of data collected by connected

255. 45 C.F.R. § 164.312; *see also* SECURITY STANDARDS: TECHNICAL SAFEGUARDS, *supra* note 253, at 3, 7–12 (elaborating further on the examples of reasonable and appropriate technical safeguards set forth in 45 C.F.R. § 164.312).

256. SECURITY STANDARDS: TECHNICAL SAFEGUARDS, *supra* note 253, at 1.

257. *Id.* at 13; *see HIPAA Security Rule & Risk Analysis*, *supra* note 241.

258. *HIPAA Privacy Rule*, *supra* note 206; *HIPAA Security Rule & Risk Analysis*, *supra* note 241 ("[T]he Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and nontechnical safeguards that covered entities must implement to secure ePHI.").

259. *See* Alder, *supra* note 205.

260. *Id.*

261. *See id.*

devices."[262] Health information can reveal much about an individual's medical conditions and healthcare generally.[263] But, an individual's location information can provide "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[264] As shown below, because of the profound impact it may have on an individual's ability to travel freely, Congress should regulate the collection and use of location information in the same manner HIPAA regulates health information.

A. *Location Tracking's Impact on the Right to Travel*

When individuals use their connected devices—and even sometimes when they do not—their location may be continually tracked via cell towers, Wi-Fi networks, and GPS signals.[265] Such sustained location tracking creates an expansive record of individuals' whereabouts and can reveal a lot about them.[266] Most of the time, individuals gladly hand over location information in exchange for real-time services, such as directions on the quickest way home from work.[267] However, individuals are not likely to "happily offer their location data" when the information reveals frequent trips to a doctor's office or other sensitive precise daily movements.[268] In reality, when companies collect individuals' location information, they aggregate the information to use however they see fit.[269]

Companies use collected location information for a variety of purposes that may interfere with an individual's ability to freely travel. For instance, as discussed in Part I, companies may

---

262. Cohen, *supra* note 51.

263. SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4.

264. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 440, 415 (2012) (Sotomayor, J., concurring)).

265. *See* discussion *supra* Section I.A.

266. Cohen, *supra* note 51; s*ee, e.g.*, *Carpenter*, 138 S. Ct. at 2217 ("Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts.").

267. Cohen, *supra* note 51.

268. *Id.*

269. *See id.*

track individuals' locations to create geofences for targeted advertisements.[270] Such targeted activities can be used to influence individuals' decision making on serious, personal matters, such as healthcare, and keep them from moving freely to exercise their personal rights.[271] All the while, the individual likely does not know a company is collecting their location information and selling it to third parties who, in turn, are attempting to influence the individual's behavior and movement.[272] This pervasive use of location tracking has the power to "digitally harass people" and interfere with their privacy and ability to move freely without companies attempting to exert influence over the places they travel.[273]

Certainly, a company's disclosure of an individual's location information can interfere with their ability to freely travel.[274] But what if instead of trying to influence the individual's behavior, the third party to whom location information has been disclosed uses the information to physically find an individual?[275] Imagine that a third-party individual gets a hold of one of the location data sets, similar to the *New York Times* Privacy Project, and uses the information to track an ex-girlfriend whom he previously abused.[276] As the Privacy Project noted, "there are often few protections to stop an individual analyst with access to such data from tracking an ex-lover or victim of abuse."[277] With access to the abuse victim's precise location information, the individual can recreate the victim's movements to ascertain their home and work addresses, the exact route the victim takes to

---

270. *See* discussion *supra* Section I.A; Press Release, AG Reaches Settlement, *supra* note 71.

271. *See, e.g.*, Press Release, AG Reaches Settlement, *supra* note 71 (reporting a settlement agreement with companies that created geofences around reproductive health centers to direct targeted anti-abortion advertisements to "abortion-minded women" in an attempt to influence their personal medical decisions).

272. *See id.*

273. *See id.*

274. *See* discussion *supra* Section I.A.

275. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

276. *See id.*; *see also* Kaitlyn Wells & Thorin Klosowski, *Domestic Abusers Can Control Your Devices. Here's How to Fight Back.*, N.Y. TIMES (Apr. 6, 2020), https://www.nytimes.com/2020/04/06/smarterliving/wirecutter/domestic-abusers-can-control-your-devices-heres-how-to-fight-back.html [https://perma.cc/WUV7-M5VT]; Boshell, *supra* note 12.

277. Thompson & Warzel, *Twelve Million Phones*, *supra* note 10; *see also* Boshell, *supra* note 12.

work, and all of the victim's movements more generally.[278] Such information provides the abuser with ample opportunities to reach out and touch the victim, putting the victim in harm's way and interfering with the victim's ability to travel freely without fear.[279]

Although the *New York Times* data set contained past location information, it is also possible to ascertain individuals' real-time location information.[280] In 2019, *Vice* conducted an experiment to see if a bounty hunter could track its reporter's real-time location.[281] He could.[282] *Vice* gave the phone number of one of its reporters to a bounty hunter, who sent the number to a contact of his.[283] The bounty hunter's contact sent back a screen shot of Google Maps with a blue circle showing the phone's current location, approximate to a few hundred meters.[284] The bounty hunter did not hack the device; he purchased the real-time location information that originated from the reporter's phone service provider.[285] For only $300, *Vice* tracked the real-time location information of an individual down to a few city blocks.[286]

For only a few hundred dollars, third-party individuals can create omnipresent surveillance on individuals, even if those individuals take precautions to avoid being tracked.[287] Such omnipresent surveillance may profoundly interfere with

278. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10; *see also* Boshell, *supra* note 12.

279. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10; *see also* Boshell, *supra* note 12.

280. *See* Boshell, *supra* note 12 ("[R]eal-time location data is regularly monetized and sold to third parties for a variety of purposes unrelated to the original transaction that justified the initial location data collection.").

281. Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, VICE (Jan. 8, 2019, 12:08 PM), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile [https://perma.cc/TA58-ETSG].

282. *Id.*

283. *Id.*

284. *Id.*

285. *Id.*

286. *See id.*

287. *Id.*; *see* Boshell, *supra* note 12. The reporter "identif[ied] the exact location of a smartphone using only the phone number and a $300 payment to a bounty hunter in an attenuated process that apparently happens regularly and in violation of the app's posted privacy policies and the parties' written nondisclosure agreements." *Id.*

individuals' ability to freely travel, especially, for instance, when used by private actors to put individuals in harm or to suppress other rights, such as exercising the right to peaceful assembly.[288] Additionally, location tracking will likely continue to become an increasingly common practice.[289] For example, companies may use location tracking to keep tabs on employees.[290] Further, individuals may use location tracking to create weaponized surveillance motivated by politics.[291] Accordingly, the right to travel should be protected from any potential current and future interferences caused by location tracking.

B. *Location Tracking and HIPAA*

Although there are federal laws that regulate some parts of location tracking,[292] there is no federal regulation of location tracking as a whole.[293] Therefore, Congress should use HIPAA as a framework to regulate the collection, use, and disclosure of individuals' location information because of the profound effects location tracking may have on the fundamental right of Americans to travel freely. In doing so, Congress should address concerns over consent and authorization, anonymity and de-identification, and secured storage of location information.

---

288. *See* Boshell, *supra* note 12; MONIKA ZALNIERIUTE, PROTESTS AND PUBLIC SPACE SURVEILLANCE: FROM METADATA TRACKING TO FACIAL RECOGNITION TECHNOLOGIES 2 (2021).

289. *See* Boshell, *supra* note 12.

290. *See, e.g.*, Marc Chase McAllister, *GPS and Cell Phone Tracking of Employees*, 70 FLA. L. REV. 1265, 1293–1310 (2018) (discussing the practice of employers tracking their employees using GPS technology).

291. *See, e.g.*, Boorstein & Kelly, *supra* note 110. In 2023, the Washington Post reported on how a "group of conservative Colorado Catholics . . . spent millions of dollars to buy mobile app tracking data that identified priests who used gay dating and hookup apps and then shared it with bishops around the country." *Id.* Bennet Cyphers, a special adviser to the digital rights organization the Electronic Frontier Foundation, commented to the Washington Post that the group's activities were "a character assassination of a private citizen for some kind of political reason based on information [the citizen] didn't know they were being tracked on." *Id.* (alteration in original).

292. *See, e.g.*, Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06 (1998).

293. *See* Boshell, *supra* note 12.

1. *Consent to be tracked?*

Companies often claim individuals consent to their location information being collected when they use the company's services as a justification for the company's location collection practices.[294] However, it is difficult for individuals to give informed consent to be tracked because companies rarely make clear how the company uses and discloses location information.[295] Indeed, "even where it appears consumers gave valid consent, that agreement might be a product of manipulative dark patterns," which "trick or manipulate users into making choices they would not otherwise have made and that may cause harm."[296] Moreover, it can be even more difficult for an individual to not consent to, or opt out of, being tracked.[297]

Currently, individuals have little ability to give informed consent, or control, how companies collect and use their location information.[298] For example, in 2018, Google came under scrutiny for its location tracking consent practices.[299] By default, Google opts individuals into real-time location tracking when the individual first uses its services.[300] If an individual does not consent for their location to be tracked and wishes to opt out of the default setting, the individual must do two things.[301] First, to delete the location information Google already collected, the individual must turn off and delete "Location History."[302] However, this process does not halt Google's location tracking; it "only halts the user's ability to view his or her location data going forward."[303] To stop Google's location tracking, the

294. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

295. *See id.*; *see also* FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT 15 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf [https://perma.cc/NQP8-7QPV].

296. FED. TRADE COMM'N, *supra* note 295, at 2, 15, 15 n.111 (citations omitted).

297. *See* Boshell, *supra* note 12.

298. *See id.*

299. *Id.*

300. *Id.*

301. *Id.*

302. *Id.*

303. *Id.*

individual must go to "Web & App Activity" and opt out of location tracking.[304] The opt-out process is complicated and confusing, particularly because the two settings are in different places and do not reference each other.[305]

In response, Google argued its location tracking disclosures are transparent and, thus, user consent to its tracking practices are valid.[306] But how can individuals truly consent to location tracking when they are automatically opted in and then face a cumbersome and confusing process to opt out? France agreed, and in 2019, fined Google $57 million for violating the European Union's General Data Protection Regulation's clear disclosure and user consent requirements.[307] More recently, forty states in the United States reached a settlement with Google, requiring the company to make its location tracking practices clearer to users.[308]

It is clear the ability of individuals to consent to location tracking is confusing and complicated. For the most part, individuals may not even be aware their connected devices or applications are tracking their location.[309] Even if individuals are generally aware their location information is collected for a specific

304. *Id.*

305. *See id.*

306. *Id.*; Emily Birnbaum, *Consumer Groups Urge FTC to Investigate Google over Location Tracking*, THE HILL, (Nov. 27, 2018, 9:59 AM), https://thehill.com/policy/technology/418412-consumer-groups-urges-ftc-to-investigate-google-over-location-tracking/ [https://perma.cc/PSP4-NM45].

307. Mathieu Rosemain, *France Fines Google $57 Million for European Privacy Rule Breach*, REUTERS, https://www.reuters.com/article/us-google-privacy-france/france-fines-google-57-million-for-european-privacy-rule-breach-idUSKCN1PF208 [https://perma.cc/ZN8B-RFPU] (Jan. 21, 2019, 1:31 PM); *see also* Boshell, *supra* note 12. *See generally* discussion *infra* Section IV.C.3 (discussing the General Data Protection Regulation and its consent regime).

308. Trisha Sircar, *40 States Reach Historic Settlement with Google Regarding Location-Tracking in the Amount of $391.5m*, JD SUPRA (Nov. 16, 2022), https://www.jdsupra.com/legalnews/40-states-reach-historic-settlement-9961507/ [https://perma.cc/34FZ-5QPW] (naming Google's settlement "the largest multistate privacy settlement in U.S. history"); *see also* Ravie Lakshmanan, *Google to Pay $29.5 Million to Settle Lawsuits over User Location Tracking*,
THE HACKER NEWS (Jan. 2, 2023), https://thehackernews.com/2023/01/google-to-pay-295-million-to-settle.html [https://perma.cc/VQ8X-YU4D] (noting Google's settlement with Indiana and Washington, D.C. in addition to the other forty states).

309. Press Release, AG Reaches Settlement *supra* note 71.

service, such as mapping their workouts, they may not be aware their location information is disclosed to third parties.[310]

The HIPAA Privacy Rule's general authorization requirements for Covered Entities provides an instructive framework for a new piece of legislation to regulate the consent issues surrounding location information collection.[311] Like the Privacy Rule, new legislation should require companies that collect location information to receive the individual's, or a personal representative's, authorization and consent before using or disclosing the information for purposes other than the intended services provided.[312] Such authorization should be in writing with clear language that explains to the individual what location information will be collected, used, or disclosed, to whom it may be disclosed, and for what purpose.[313] Moreover, the authorization should state if the company receives financial compensation for disclosing location information and include a warning about potential future disclosures.[314]

By using the Privacy Rule as a framework, new legislation can likewise give individuals more control over the collection, use, and disclosure of their location information.[315] New legislation, similar to HIPAA, would both protect individuals' confidentiality in their location information and allow companies to use and disclose the information for financial gain.[316] However, to strike the necessary balance, individuals' location information should also be anonymized or de-identified before companies can use or disclose the information for activities outside the intended service.

---

310. *See* Thomas, *supra* note 99; discussion *supra* Section I.A.2.

311. *See* discussion *supra* Section III.A for a description of the privacy rule.

312. *See HIPAA Privacy Rule*, *supra* note 206.

313. *See id.* The proposed American Data Privacy and Protection Act and the European Union's General Data Protection Regulation both require similar consent regimes to be in place before companies can collect, use, and disclose individuals' location information. *See* discussion *infra* Section IV.C.1, .3.

314. *See HIPAA Privacy Rule*, *supra* note 206.

315. *See* Tovino, *supra* note 226.

316. *See id.*

2. *Anonymity and de-identification of location information*

Even if new legislation requires authorization and consent before a company may use or disclose individuals' location information, the information should also be de-identified before companies can use or disclose it.[317] Companies currently justify location information collection by claiming the information is anonymous; however, anonymization of location information presents many issues.[318] Although location information contains no identifiable information, it is not challenging to connect location information to real individuals.[319] Location information is never truly anonymous because such information is "absolutely impossible to anonymize."[320] In an interview with the *New York Times* Privacy Project, Paul Ohm, a Professor of Law at the Georgetown University Law Center, noted that "D.N.A. . . . is probably the only thing that's harder to anonymize than precise geolocation information."[321]

Indeed, third parties regularly combine purportedly anonymized location information with identified personal information to compile comprehensive profiles of individuals, despite the individuals having no direct relationship to the third party.[322] Take, for example, the *New York Times* Privacy Project reconstructing the exact movements of the President of the United States through the location information of a Secret Service agent.[323] Using publicly available information, the Privacy Project de-anonymized the location data of the Secret Service agent to watch the agent travel from exclusive area to exclusive area.[324] The Secret Service agent's movements—"down to a few feet"—were cross-referenced with the President's public schedule to clearly show his precise movements throughout a day full

317. *See* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4.
318. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10; Boshell, *supra* note 12.
319. Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.
320. *Id.*
321. *Id.*
322. *See* Boshell, *supra* note 12.
323. Thompson & Warzel, *How to Track President Trump*, *supra* note 25.
324. *Id.*

of meetings with another world leader.[325] The Privacy Project even discovered where the Secret Service agent lived, exposing details about the agent's family.[326] The ability to de-anonymize location information with ease is not limited to high-profile individuals.[327] Indeed, the Federal Trade Commission has noted one set of researchers showed that by using just four timestamped location points, they could "identify 95% of a dataset of 1.5 million individuals."[328]

Although the Privacy Rule does not place restrictions on de-identified health information's use or disclosure that "neither identifies nor provides a reasonable basis to identify an individual,"[329] location information does provide a reasonable basis to identify an individual by nature.[330] Thus, location information should be considered identifiable information and treated similarly to the way PHI is regulated under the Privacy Rule.[331] To ensure individuals' location information is de-identified, companies should remove any specified identifiers of the individual and his relatives and household members.[332] Further, the company should not have actual knowledge that the de-identified location information can be used to identify the individual.[333] While it may be challenging to prevent the re-identification of individuals based on location information,[334] efforts should still be made to protect this sensitive information.

These steps will help strike the balance between individuals' confidentiality interests in their location information and

325. *Id.*

326. *Id.*

327. *See id.*

328. Cohen, *supra* note 51.

329. HIPAA PRIVACY RULE, *supra* note 206, at 4; 45 C.F.R. § 164.514(a). Although the Privacy Rule places no restrictions on de-identified health information, it is actually "never possible to guarantee that de-identified data can't or won't be re-identified. That's because de-identification is not anonymization." Katharine Miller, *De-Identifying Medical Patient Data Doesn't Protect Our Privacy*, STAN. U. HUM.-CTRED. A.I. (July 19, 2021), https://hai.stanford.edu/news/de-identifying-medical-patient-data-doesnt-protect-our-privacy [https://perma.cc/HQ4V-C2MK].

330. *See* discussion *supra* Section IV.A.

331. *See* discussion *supra* Section III.A.

332. *See* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4; 45 C.F.R. § 164.514(b)(2)(i).

333. *See* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 4; 45 C.F.R. § 164.514(b)(2)(ii).

334. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

companies' interests in the financial value of the information.[335] Nonetheless, to solidify the necessary balance, authorization and de-identification requirements must be buttressed by the secured storage of location information.

3. *Secured storage of location information*

Information securely stored by companies today can be easily hacked, stolen, or leaked tomorrow.[336] In the healthcare industry for instance, data breaches have given rise to the loss, theft, exposure, or impermissible disclosure of more than 382 million healthcare records between 2009 and 2022.[337] In 2022 alone, approximately two healthcare data breaches of more than 500 healthcare records were reported every day.[338] Between 2015 and 2022, healthcare data breaches accounted for nearly one third of recorded data breaches across all sectors.[339] The location data industry is no different—by its nature, it involves electronic information subject to similar unauthorized access.[340]

To secure location information, and support authorization and de-identification requirements, new legislation that regulates the use and disclosure of location information should require safeguards to ensure the secured storage of information. The HIPAA Security Rule provides an instructive framework from which those safeguards can be formed.[341] Specifically, the Security Rule's administrative, physical, and technical safeguards would ensure the confidentiality, integrity, and security of all location information.[342]

---

335. *See* SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 210, at 1.

336. *See* Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

337. *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics [https://perma.cc/TD4W-CN6V].

338. *Id.*

339. *Id.*

340. *See* Brian Barret, *A Location-Sharing Disaster Shows How Exposed You Really Are*, WIRED (May 19, 2018, 7:00 AM), https://www.wired.com/story/locationsmart-securus-location-data-privacy/ [https://perma.cc/S352-X4PB]; *see also* Jane Wakefield, *Location Data Collection Firm Admits Privacy Breach*, BRIT. BROAD. CORP. (Oct. 29, 2021), https://www.bbc.com/news/technology-59063766 [https://perma.cc/KY5M-VR9P].

341. *See generally* 45 C.F.R. §§ 160.101–.552, 164.102–.106, 164.302–.318.

342. *See HIPAA Security Rule & Risk Analysis*, *supra* note 241.

First, companies that collect individuals' location information should establish administrative safeguards.[343] These administrative safeguards are the policies and procedures that provide for how the company will protect individuals' location information.[344] The administrative safeguards should establish training and procedures for the company's employees to secure individuals' location information, even if the employee does not have direct access to the information.[345] Additionally, companies should establish security management processes, assign security responsibility, establish workforce security, install information access management, implement security awareness and training, create security incident procedures, form contingency and evaluation plans, and set procedures regarding business associate contracts and other arrangements.[346] These requirements could take the form of (1) risk management processes, (2) workforce clearance, termination, and access authorization procedures, (3) log-in and password management, and (4) emergency, disaster recovery, and data backup plans.[347] When implemented, these administrative safeguards will create the foundation from which companies can create comprehensive security programs.[348]

Second, companies should implement physical safeguards to protect the company's physical infrastructure and equipment "from natural and environmental hazards, and unauthorized intrusion."[349] In accordance with the administrative policies and procedures, the company should limit physical access to individuals' location information and the facilities that house the information, specify proper workstation functions for employees, establish workstation security to prevent unauthorized

343. *See* 45 C.F.R. § 164.308; *HIPAA Security Rule & Risk Analysis*, *supra* note 241.

344. *See* 45 C.F.R. § 164.304; *see also* SECURITY STANDARDS: ADMINISTRATIVE SAFEGUARDS, *supra* note 247, at 1–2, 6.

345. *See HIPAA Security Rule & Risk Analysis*, *supra* note 241.

346. *See* 45 C.F.R. § 164.308(a)(1)–(8), (b)(1).

347. *See* SECURITY STANDARDS: ADMINISTRATIVE SAFEGUARDS, *supra* note 247, at 27.

348. *See id.* at 1.

349. *See* 45 C.F.R. § 164.310(a)–(d); SECURITY STANDARDS: PHYSICAL SAFEGUARDS, *supra* note 250, at 2, 7–10.

users, and establish device and media controls over the information.[350] Additionally, such physical safeguards could take the form of access control and validation procedures, contingency operations, facility security plans, and secure data backup and storage.[351] These physical safeguards build on the administrative safeguards to ensure the security of individuals location information.[352]

Finally, companies should install technical safeguards that further protect and control access to individuals' location information.[353] The technical safeguards must "reasonably and appropriately" preserve the necessary level of security for individuals' location information.[354] Companies should have flexibility to implement technical safeguards and organizational best practices as they evolve over time.[355] Nonetheless, controlling access to individuals' location information, conducting audits, maintaining the integrity of the location information, requiring person or entity authentication before access to the information is permitted, and establishing transmission security to prevent unauthorized disclosures of the information should all be highly considered.[356] To facilitate these technical safeguards, companies should consider unique user identifications, emergency access procedures, mechanisms to authenticate the information, and encryption of the information.[357] As location tracking technology continues to advance, technical safeguards become increasingly important to effectively secure location information.[358]

---

350. *See* 45 C.F.R. § 164.310(a)–(d); SECURITY STANDARDS: PHYSICAL SAFEGUARDS, *supra* note 250, at 2, 7–10.

351. *See* SECURITY STANDARDS: PHYSICAL SAFEGUARDS, *supra* note 250, at 16.

352. *See id.* at 13.

353. *See* 45 C.F.R. § 164.304; SECURITY STANDARDS: TECHNICAL SAFEGUARDS, *supra* note 253, at 1–2.

354. *See* SECURITY STANDARDS: TECHNICAL SAFEGUARDS, *supra* note 253, at 2.

355. *See id.*

356. *See* 45 C.F.R. § 164.312(a)–(e); SECURITY STANDARDS: TECHNICAL SAFEGUARDS, *supra* note 253, at 3–10.

357. *See* SECURITY STANDARDS: TECHNICAL SAFEGUARDS, *supra* note 253, at 16.

358. *See id.* at 1, 13; discussion *supra* Section I.B.

In combination, the three Security Rule safeguards will ensure the confidentiality, integrity, and availability of all location information, while also protecting against reasonably anticipated threats, hazards, or unauthorized uses or disclosures of such information.[359] If implemented properly, the safeguards would guarantee individuals a minimum level of privacy protections for their location information.[360] With the Privacy and Security Rules in place, individuals can have more confidence and trust that their most sensitive location information is protected.[361] Using the Privacy and Security Rules as a model, legislation regulating companies' use and disclosure of individuals' location information will play an invaluable role in the efficiency, security, and privacy in the location collection industry.[362]

C. *Alternative Legislation and Legislative Frameworks*

Privacy legislation in the United States is a "hot topic" at the federal and state levels.[363] Despite continued discussion, the United States lacks any comprehensive federal privacy legislation.[364] Instead, privacy legislation is a patchwork made up of various sector-specific federal privacy laws[365] and comprehensive state laws.[366] Naturally, commentators have called for Congress to enact a single, comprehensive piece of federal privacy legislation to alleviate the complications that result from a lack

359. *See HIPAA Security Rule & Risk Analysis*, *supra* note 241; *HIPAA Privacy Rule*, *supra* note 206.

360. *See HIPAA Privacy Rule*, *supra* note 206.

361. *See id.*

362. *See* Alder, *supra* note 205.

363. *Federal Privacy Legislation – An Imminent Reality or Much Ado About Nothing?*, FISHER PHILLIPS (Aug. 4, 2022), https://www.fisherphillips.com/news-insights/federal-privacy-legislation-imminent-reality.html [https://perma.cc/37DU-FY8R].

364. *Id.*

365. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (regulating the healthcare industry); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (regulating data collection of children under thirteen years of age).

366. *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (Deering 2023); Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2023).

of uniformity.[367] Two proposed pieces of federal privacy legislation from the United States, and the European Union's comprehensive privacy legislation offer alternative frameworks.[368]

1. *The American Data Privacy and Protection Act*

Congress's most recent attempt to enact a comprehensive federal privacy law is the American Data Privacy and Protection Act ("ADPPA").[369] In 2022, with bipartisan support, the House of Representative's Energy & Commerce Committee introduced the ADPPA "[t]o provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement."[370] If enacted, the ADPPA would regulate how companies treat a broad range of consumer data.[371]

Regarding location information, the ADPPA would regulate how companies may use "precise geolocation information,"[372]

---

367. *See* Cameron F. Kerry & John B. Morris, *Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation*, BROOKINGS INST. (Dec. 8, 2020), brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/ [https://perma.cc/97YP-VM4W]; Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS INST. (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ [https://perma.cc/C8NX-P2H8].

368. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); Geolocation Privacy and Surveillance Act, S. 395, 115th Cong. (2017); Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive (General Data Protection Regulation) 95/46, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

369. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

370. *Id.*; *see also The American Data Privacy and Protection Act*, AM. BAR ASS'N (Aug. 30, 2022), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washington-letter/august-22-wl/data-privacy-0822wl/?login [https://perma.cc/3Y2F-U5TS] (noting bipartisan support for ADPPA).

371. *See* H.R. 8152 § 2(8)(A). Under the ADPPA, "[t]he term 'covered data' means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers." *Id.*

372. *Id.* § 2(24)(A). Under the ADPPA,

> [t]he term "precise geolocation information" means information that is derived from a device or technology that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, with sufficient precision to identify street level location information of an individual or device or the location of an individual or device within a range of 1,850 feet or less.
>
> *Id.*

which the ADPPA considers "sensitive covered data."[373] Specifically, "Covered Entities" may not collect or process precise geolocation information, except when necessary to provide intended services.[374] Moreover, Covered Entities may not transfer an individual's precise geolocation information to a third party unless certain factors are met, such as "the transfer [being] made pursuant to the affirmative express consent of the individual."[375] Additionally, similar to the HIPAA Security Rule, the ADPPA would require Covered Entities to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition."[376] However, the ADPPA places no restrictions on Covered Entities' use of de-identified precise geolocation information, nor does it impose requirements on the security of de-identified information, as the ADPPA does not consider de-identified information to be covered data.[377]

The ADPPA is a great opportunity for Congress to enact a much needed comprehensive piece of federal privacy legislation.[378] Indeed, the ADPPA aims to solve many of the issues discussed in this Note.[379] For example, the ADPPA aims to solve the issues surrounding individuals' inability to give effective, informed consent before companies collect, use, and disclose their location information by generally requiring Covered Entities to receive "affirmative express consent" before data can be transferred to third parties.[380] Additionally, the ADPPA would

373. *Id.* § 2(28)(A)(vi).

374. *Id.* § 102(2); *see also id.* § 2(9) (defining "Covered Entities").

375. *Id.* § 102(3)(A).

376. *Id.* § 208(a)(1); *see also* 45 C.F.R. §§ 160.101–.552, 164.102–.106, 164.500–.534 (2023).

377. H.R. 8152 § 2(8)(B)(i).

378. *See* Stacey Gray, *The Bipartisan House Privacy Bill Would Surpass State Protections*, LAWFARE (July 21, 2022, 8:54 AM), https://www.lawfaremedia.org/article/bipartisan-house-privacy-bill-would-surpass-state-protections [https://perma.cc/C93K-65B2] (noting the ADPPA represent a federal privacy law which "is long overdue" and "would address very real, current privacy threats caused by gaps in legal protections").

379. *See* discussions *supra* Parts I, IV.

380. *See* H.R. 8152 § 102(3)(A). "The term 'affirmative express consent' means an affirmative act by an individual that clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed . . . ." *Id.* § 2(1)(A).

give individuals the "right to consent and object," including the rights to withdraw consent, opt out of covered data transfers or targeted advertising, and have individual autonomy in consent decisions.[381]

The ADPPA also attempts to strike a balance between protecting individuals' location information and allowing Covered Entities to use de-identified location information.[382] The ADPPA would permit Covered Entities to use and secure de-identified data in any manner it deems fit, subject to certain requirements.[383] Covered Entities must: (1) "take[] reasonable technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual"; (2) "publicly commit[] in a clear and conspicuous manner" to solely use de-identified information and not attempt to re-identify the information; and (3) "contractually obligate[]" anyone who receives the information to comply with the previous requirements.[384] These requirements are steps in the right direction, but they leave it up to Covered Entities to decide what constitutes "reasonable technical measures" instead of promulgating explicit baseline measures.[385] Any legislation that aims to protect individuals' location information should take stronger action to ensure such information remains de-identified, because of how easy it is to re-identify individuals' via location information.[386]

Finally, the ADPPA aims to address issues surrounding the secured storage of individuals' location information by requiring Covered Entities to "establish, implement, and maintain reasonable administrative, technical, and physical data security

381. *Id.* § 204(a)–(d).

382. *See id.* § 2(8)(B)(i).

383. *Id.* § 2(8)(A)–(B)(i). "The term 'de-identified data' means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated . . . ." *Id.* § 2(12).

384. *Id.* § 2(12)(A)–(C).

385. *See id.* § 2(12).

386. *See* discussion *supra* Section IV.B.2; Thompson & Warzel, *Twelve Million Phones*, *supra* note 10.

practices and procedures."[387] However, aside from a handful of generalized "specific requirements,"[388] the ADPPA provides no guidance to Covered Entities on how to create or implement the security requirements.[389] Similar to how HIPAA authorized HHS to develop the Security Rule, the ADPPA would authorize the Federal Trade Commission ("FTC") to promulgate regulations to elaborate on the ADPPA's security requirements.[390] But, until the FTC promulgates a rule similar to the HIPAA Security Rule, companies will be left to determine what constitutes "reasonable administrative, technical, and physical [safeguards]," leaving individuals' location information vulnerable to unauthorized access and disclosure.[391]

The ADPPA is, without a doubt, a step in the right direction toward protecting individuals' location information.[392] Nonetheless, the ADPPA faces many hurdles on its path to enactment, especially on the state preemption front.[393] Thus, it remains to be seen if Congress can rally around the ADPPA and finally pass comprehensive federal privacy legislation.[394] Even

387. *See* H.R. 8152 § 208(a)(1).

388. The covered company's data security practices "shall include, for each respective entity's own system or systems at a minimum, the following practices:" "(1) assess vulnerabilities"; "(2) preventive and corrective action"; "(3) evaluation of preventative and corrective action"; "(4) information retention and disposal"; "(5) training"; "(6) designation"; and "(7) incident response." *Id.* § 208(b)(1)–(7).

389. *See id.* § 208.

390. *See* JOHNATHAN M. GAFFNEY, CHRIS D. LINEBAUGH & ERIC N. HOLMES, CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 2 (2022).

391. *See* H.R. 8152 § 208(a)(1).

392. *See* Peter Swire, *The Bipartisan, Bicameral Privacy Proposal Is a Big Deal*, LAWFARE (June 9, 2022, 2:12 PM), https://www.lawfareblog.com/bipartisan-bicameral-privacy-proposal-big-deal [https://perma.cc/UH4R-YMXA] (noting the ADPPA provides privacy protections that are "long overdue").

393. *See* Cameron F. Kerry, *Will California be the Death of National Privacy Legislation?*, BROOKINGS INST. (Nov. 18, 2022), https://www.brookings.edu/blog/techtank/2022/11/18/will-california-be-the-death-of-national-privacy-legislation/ [https://perma.cc/T4F9-YRJR] (noting California has "mounted a full court lobbying press against [the] preemption of provisions in state laws that are 'covered by' provisions in the federal law"). The preemption doctrine states that "[w]hen state law and federal law conflict, federal law displaces, or preempts, state law, due to the Supremacy Clause of the Constitution." *Preemption*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/preemption [https://perma.cc/P36K-VGNG] (citing U.S. CONST. art. VI, § 2, cl. 2).

394. *See* Editorial Board, *Democrats and Republicans Agree on this Tech Privacy Bill. But Can It Pass?*, WASH. POST (Dec. 8, 2022, 2:38 PM), https://www.washingtonpost.com/opinions/2022/12/08/tech-privacy-bill-bipartisan-congress/ [https://perma.cc/ELM7-L6HZ].

if Congress does enact the ADPPA, it should still look to the HIPAA framework, with its Privacy and Security Rules established by HHS, as an instructive model to protect individuals' location information.[395]

2. *The Geolocation Privacy and Surveillance Act*

In 2017, five years before the House Energy & Commerce Committee introduced the ADPPA to Congress, a bipartisan group of Congress members introduced the Geolocation Privacy and Surveillance Act ("GPS Act") "to specify the circumstances in which a person may acquire geolocation information."[396] Modeled after federal wiretapping laws, the GPS Act would "create[] a legal framework designed to give government agencies, commercial entities and private citizens clear guidelines for when and how geolocation information can be accessed and used."[397] Specifically, the GPS Act would prohibit the interception of geolocation information and its use and disclosure,[398] except for certain delineated circumstances, including "information acquired in the normal course of business" by a "covered service" and where consent is given.[399]

The GPS Act's primary purpose is to create a clear and conspicuous standard for the government to access geolocation information.[400] Instead of protecting individuals' location information from companies, the GPS Act would give companies clarity about how to respond to and comply with government requests for location information.[401] Therefore, the GPS Act differs from this Note's proposed privacy legislative framework.[402] The GPS Act would not require clear, informed consent or de-identification before location information can be collected,

395. *See* discussion *supra* Section IV.B.

396. Geolocation Privacy and Surveillance Act, S. 395, 115th Cong. (2017).

397. *GPS Act*, RON WYDEN U.S. SEN. FOR OR., https://www.wyden.senate.gov/priorities/gps-act [https://perma.cc/9M3W-HREW].

398. S. 395 § 2602(a)(1).

399. *Id.* § 2602(b)–(h).

400. *See GPS Act*, *supra* note 397.

401. *See id.*

402. *See id.*; discussion *supra* Section IV.B.

used, or disclosed.[403] Nor would the GPS Act require covered companies to establish any safeguards to secure individuals' location information once it is collected.[404] The GPS Act's sole purpose is aimed specifically at government—not private—collection of individuals' location information.[405] Accordingly, Congress should still look to HIPAA as a model framework for regulating the collection, use, and disclosure of individuals' location information.[406]

3. *The General Data Protection Regulation*

The European Union's General Data Protection Regulation ("GDPR")[407] is often considered the "gold standard" for privacy legislation.[408] The GDPR is "the toughest privacy and security law in the world . . . [which] imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the [European Union]."[409] At the heart of the GDPR lies the protection of individuals' "personal data," which includes location information.[410] The GDPR protects data using a set of principles outlined in Article 5: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and

403. *See* discussion *supra* Section IV.B; S. 395.

404. *Compare* discussion *supra* Section IV.B, *with* S. 395.

405. *See* S. 395; *GPS Act*, *supra* note 397.

406. *See* discussion *supra* Sections III, IV.B. In any event, the GPS Act has not made it out of the introduction stage in either the United States House of Representatives or the Senate. *See* S. 395.

407. GDPR, *supra* note 368.

408. *See, e.g.*, Giovanni Buttarelli, *The EU GDPR as a Clarion Call for a New Global Digital Gold Standard*, 6 INT'L DATA PRIV. L. 77, 78 (2016) (discussing why the European Data Protection Supervisor hopes that the GDPR will become a "digital gold standard").

409. Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/P2FZ-SKMR].

410. *See id.* The GDPR defines "personal data" as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, *location data*, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
>
> GDPR, *supra* note 368, art. 4, ¶1 (emphasis added).

accountability.[411] The GDPR's delineated principles require companies that process individuals' personal data do so responsibly.[412]

The GDPR is a potentially useful model for federal privacy legislation in the United States that would protect individuals' location information as it aims to solve many of the issues presented in this Note. First, the GDPR requires "freely given, specific, informed and unambiguous" consent as one of the specific conditions companies must meet before collecting personal data.[413] Accordingly, companies must request consent in "clear and plain language" that is "clearly distinguishable from the other matters."[414] Further, individuals have the right to withdraw consent at any time.[415] The GDPR's robust consent regime solves many of the issues surrounding individuals' inability to control the location information companies collect.[416]

Additionally, the GDPR aims to protect individuals' location information by setting forth stringent rules regarding personal data, even if de-identified.[417] Although companies may use de-identified data more freely through "pseudonymisation," de-identified data is not exempt from the GDPR's requirements.[418]

---

411. Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 112 (2021); GDPR, *supra* note 368, art. 5. In addition to providing foundational principles to ensure data protection, the GDPR grants individuals multiple rights. *Id.* These rights include the rights to be informed, of access, to rectification, to erasure (the right to be forgotten), to restrict processing, to data portability, to object, and to automated decision-making and profiling. *See id.* art. 12–15; Wolford, *supra* note 409.

412. Rich Castagna, *General Data Protection Regulation (GDPR)*, TECHTARGET, https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR [https://perma.cc/CNT5-KU3U].

413. *See* GDPR, *supra* note 368, art. 6, ¶1. The GDPR only permits companies to process personal data when one of six conditions are met. *Id.* These conditions include consent for "the performance of a contract," "compliance with a legal obligation," "protect[ion of] vital interests of the data subject," "the performance of a task carried out in the public interest," and "purposes of the legitimate interests pursued by the controller or by a third party." *Id.*

414. GDPR, *supra* note 368, art. 7, ¶ 2.

415. *Id.* ¶ 3.

416. Wolford, *supra* note 409; *see* discussion *supra* Section IV.B.1.

417. *See* Wolford, *supra* note 409.

418. *See Pseudonymization According to the GDPR [Definitions and Examples]*, DATA PRIV. MANAGER (Feb. 11, 2021), https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/. [https://perma.cc/M4ZM-ECKA]. The GDPR defines "pseudonymisation" as:

To be considered pseudonymous, or de-identified, the personal data cannot be attributable to the individual without additional information, any additional information must be stored separately from the pseudonymous data, and measures must be taken to ensure the data is unattributable to the individual.[419] As discussed in Section IV, location information is easily attributable to individuals because the vast amounts of location data points present an all-encompassing picture of individuals' lives.[420] By its nature, location information provides additional information in the form of physical points on a map, such as an individual's home or work, which companies cannot easily ensure is unattributable.[421] Accordingly, the GDPR's stringent requirements limit the use and disclosure of individuals' location information because of the virtual impossibility to anonymize the information.[422]

Finally, the GDPR requires companies to process data "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures" to "ensure a level of security appropriate to the risk."[423] The GDPR's security requirements—the integrity and confidentiality principle—are intentionally vague to allow companies the flexibility to implement technical and organizational best practices as they

---

> the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

GDPR, *supra* note 368, art. 4, ¶ 5.

419. GDPR, *supra* note 368, art. 4, ¶ 5.

420. *See* discussion *supra* Section IV.B.2.

421. *See* discussion *supra* Section IV.B.2.

422. *See* GDPR, *supra* note 368, art. 4, ¶ 1. Truly anonymized personal data is not subject to any GDPR restrictions as it falls outside its scope. Odia Kagan, *Anonymization Governance: Why It's Important for GDPR and for CPRA*, FOX ROTHSCHILD LLP (Mar. 11, 2022), https://www.foxrothschild.com/publications/anonymization-governance-why-its-important-for-gdpr-and-for-cpra [https://perma.cc/8286-EYXL].

423. GDPR, *supra* note 368, art. 5, ¶ 1(f), art. 32, ¶ 1.

evolve over time.[424] Similar to the HIPAA Security Rule, the GDPR provides examples of appropriate security measures, including the "pseudonymisation" of data and "regular[] testing, assessing and evaluating" of the measures put in place.[425] The GDPR's integrity and confidentiality principle, like the HIPAA Security Rule, helps ensure the confidentiality, integrity, and availability of individuals' location information.[426]

The GDPR provides a robust framework that the United States could use to craft similarly comprehensive privacy legislation.[427] However, a GDPR-type law would face many obstacles on its path to enactment.[428] Congress likely does not have the appetite for a bill of the GDPR's scale, and state preemption is a high likelihood, which would likely cause heavy lobbying against the bill.[429] Even if Congress does enact privacy legislation modeled on the GDPR, it should still look toward HIPAA and its Privacy and Security Rules for a model to implement regulations on companies' collection, use, and disclosure of individuals' location information.[430] HIPAA's framework

---

424. Luke Irwin, *The GDPR: Understanding the 6 Data Protection Principles*, IT GOVERNANCE (Dec. 9, 2021), https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles [https://perma.cc/MQ6Y-Y737]; *see also* Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED UK (Mar. 24, 2020, 4:30 PM), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 [https://perma.cc/RGM7-7TMZ] ("[The] GDPR doesn't say what good security practices look like, as it's different for every organisation. A bank will have to protect information in a more robust way than your local dentist may need to.").

425. *See* GDPR, *supra* note 368, art. 32, ¶ 1(a), (d); *see also* discussion *supra* Section III.B (noting that the HIPAA Security Rule provides examples of possible administrative, physical, and technical safeguards for ePHI).

426. *See* GDPR, *supra* note 368, art. 32, ¶ 1; discussion *supra* Section IV.B.3.

427. *See* Bryan Clark, *GDPR in the USA? New State Legislation Is Making This Closer to Reality*, NAT'L L. REV. (Mar. 18, 2021), https://www.natlawreview.com/article/gdpr-usa-new-state-legislation-making-closer-to-reality [https://perma.cc/Y9Q8-TH9D]; Saryu Nayyar, *Is It Time for a U.S. Version of GDPR?*, FORBES (Feb. 1, 2022, 10:15 AM), https://www.forbes.com/sites/forbestechcouncil/2022/02/01/is-it-time-for-a-us-version-of-gdpr/?sh=229ab7cb637a [https://perma.cc/8DYV-JGFJ].

428. Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018, 8:14 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/ [https://perma.cc/5QRD-NYAW].

429. *See id.*; Jedidiah Bracy, *In Push for US Federal Privacy Law, State Preemption Will Depend on the Details*, INT'L ASS'N OF PRIV. PROS. (Sept. 27, 2018), https://iapp.org/news/a/in-push-for-us-federal-privacy-law-state-preemption-will-depend-on-the-details/ [https://perma.cc/XXM2-FXKL].

430. *See* discussion *supra* Part III, Section IV.B.

provides an instructive model for Congress, and any government agency tasked with enforcing the law, to protect individuals' location information.

CONCLUSION

The ability to travel freely throughout the United States is foundational to American life and serves many important purposes.[431] Significantly, it permits individuals to exercise other fundamental rights, such as accessing courts and public offices[432] and peacefully assembling.[433] It also facilitates political freedom in the form of internal migration or "foot voting."[434] Further, at a basic level, it allows Americans to travel as they wish, including going to work or school, attending anything from doctor appointments to concerts, and visiting family and friends around the country.[435] Indeed, as Justice William Douglas argued:

> This freedom of movement is the very essence of our free society, setting us apart. Like the right of assembly and the right of association, it often makes all other rights meaningful—knowing, studying, arguing, exploring, conversing, observing and even thinking. Once the right to travel is curtailed, all other rights suffer . . . .[436]

Yet, the United States lacks any comprehensive federal privacy legislation to protect the basic right to travel freely from being curtailed by private interference via location tracking.[437]

---

431. *See* discussion *supra* Part II.

432. *See* Crandall v. Nevada, 73 U.S. 35, 41–42, 48 (1868).

433. *See* Aptheker v. Sec'y of State, 378 U.S. 500, 520 (1964) (Douglas, J., concurring) ("Freedom of movement is kin to the right of assembly and to the right of association."); Zemel v. Rusk, 381 U.S. 1, 25–26 (1965) (Douglas, J., dissenting) ("[T]he right to travel is at the periphery of the First Amendment, rather than at its core, largely because travel is, of course, more than speech: it is speech brigaded with conduct.").

434. *See* SOMIN, *supra* note 7, *passim*.

435. *See* Wilhelm, *supra* note 1, at 2461–62.

436. *Aptheker*, 378 U.S. at 520 (Douglas, J., concurring).

437. *See* Boshell, *supra* note 12; *Federal Privacy Legislation – An Imminent Reality or Much Ado About Nothing?*, *supra* note 363.

Without privacy legislation to regulate companies' incessant collection, use, and disclosure of individuals' location information, companies are free to do whatever they please with this sensitive information.[438] These unfettered uses of location information could lead to individuals being unduly influenced, harassed, stalked, or put in physical danger.[439] It also could lead to interferences with individuals' exercise of other fundamental rights, especially the right to association and peaceful assembly.[440] Accordingly, Congress should look to HIPAA's Privacy and Security Rules for an extensive, instructive framework to inspire new regulations of companies' collection, use, and disclosure of individuals' location information. Congress should use its Commerce Clause authority to enact this new comprehensive federal privacy legislation, using HIPAA as a model for crafting a framework to protect individuals' basic right to travel freely without interference from location tracking.

438. *See* discussion *supra* Introduction, Sections I.A, IV.A.

439. *See, e.g.*, Press Release, AG Reaches Settlement, *supra* note 71; Cox, *supra* note 281; Boorstein & Kelly, *supra* note 110.

440. *See, e.g.*, Amna Toor, Note, *"Our Identity Is Often What's Triggering Surveillance": How Government Surveillance of #BLACKLIVESMATTER Violated the First Amendment Freedom of Association*, 44 RUTGERS COMPUT. & TECH. L. J. 286, 299–301 (2018) (discussing how location information was used to interfere with Americans' ability to associate during the Black Lives Matter Movement); ZALNIERIUTE, *supra* note 288, at 2–3 (discussing how location information has been used to suppress the right to peaceful assembly).