"You Have the Data" . . . The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?

SARAH L. LODE*

INTRODUCTION

Amidst a global trend of protecting individuals from unnecessary invasions of privacy and in a world culture where nations are finding more innate rights of privacy than ever before,[1] is the United States trailing in the protection of its citizens' personal data? When looking at changing legislation and constitutions across the globe, it is hard not to conclude that the United States could learn a thing or two in the way of personal data protection: specifically, how to better protect personal medical records, treatment data, and other health-related information.

American citizens are given seemingly little or no control over the use, dissemination, and storage of their personal data—this is especially apparent when United States' legal footwork is compared with several other parts of the world.[2] Although the United States enacted the Health Insurance Portability and Accountability Act (HIPAA) (which was passed in 1996 and is rarely updated) to provide some protection of medical data,[3] along with several other topical data protection statutes and acts, the United States' ad hoc approach does little to protect citizens' personal data, which is becoming the norm in other parts of the world.[4] Internationally, citizens are provided, and sometimes constitutionally guaranteed, avenues to challenge the use, collection, and storage of their personal data by governmental and private agencies alike.[5] Other world citizens have access to a

---

* J.D. Candidate 2019, Indiana University Maurer School of Law; B.S., Business Administration, and A.A.S., Legal Studies, 2015, Ferris State University. I would like to express my sincere appreciation to Professor Joseph Hoffmann for his feedback, guidance, and advice during the seminar for which this Note was originally drafted. Additionally, I would like to thank Executive Online Editor Alexis Daniel and all the Indiana Law Journal Online Editors for their hard and thoughtful work during the publication process.

1. *See generally* Hillary B. Farber & Marvin J. Nodiff, *Protecting Homeowners' Privacy Rights in the Age of Drones: The Role of Community Associations*, 44 FORDHAM URB. L.J. 623 (2017); Yvonne Lindgren, *The Doctor Requirement:* Griswold*, Privacy, and At-Home Reproductive Care*, 32 CONST. COMMENT. 341 (2017); Margaret Byrne Sedgewick, Note, *Transborder Data Privacy as Trade*, 105 CAL. L. REV. 1513 (2017).

2. *See, e.g.*, Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.); Jordan D. Brougher, Note, *The Right to Be Forgotten: Applying European Privacy Law to American Electronic Health Records*, 13 IND. HEALTH L. REV. 510, 532 (2016).

3. *See* Pub. L. No. 104-191, 110 Stat. 1936. HIPAA provides downstream protections for medical information, allowing the Secretary of the U.S. Department of Health and Human Services to sue medical providers for inappropriately disseminating personal medical data. Federal HIPAA does not provide private citizens the right to challenge the collection or dissemination of their own data. HHS HIPAA Enforcement Rule, 45 C.F.R. §§ 160, 164 (2006).

4. GETTING THE DEAL THROUGH, DATA PROTECTION & PRIVACY 2015, 208 (Rosemary P. Jay & Hunton & Williams, eds., Law Business Research 3d ed. 2014).

5. *See, e.g.*, Andrés Guadamuz, *Habeas Data: The Latin-American Response to Data*

variety of rights and writs that allow an individual to control the use, distribution, and storage of his personal information. These rights include the writ of habeas data,[6] the right to be forgotten,[7] the right to erasure, the right to stop processing, and the right to access.[8]

With the goal of further understanding the changing international climate regarding personal data protection, this Note will not only discuss the past and current laws in several countries and regions—specifically Latin American countries and the European Union—but will attempt to harmonize these changing international data protection norms in a way that could allow the United States to build its own comprehensive data protection scheme. While the international trend towards more personal data protection covers a wide variety of personal data, this Note will focus predominately on the protection of personal medical records as a case study and starting point from which to propose a more comprehensive solution for reforming United States legislation.[9]

In Part I of this Note, I will discuss the writ of habeas data that has been developed primarily, but not exclusively, in Latin American countries. I will discuss the intricacies of the writ, how it evolved, and how it is applied today. Using Argentina as an example, I will discuss how the writ would be used by an Argentine citizen to protect her personal data. Part II summarizes the previously employed data protection scheme in the European Union, the Data Protection Directive ("the Directive"), and will also discuss the new EU data protection regulation, the General Data Protection Regulation (GDPR), which became effective in May of 2018. I will discuss how the old Data Protection Directive is different from the GDPR, and how the rights given to EU Member citizens differ under each. I will cover the right to access, the right to stop processing, and the right to erasure, which are all provided within the new regulation (although previously alluded to in the Directive). I will provide an example of an EU Member citizen's use of the rights provided under the GDPR.

The next two Parts of this Note will shift focus to U.S. legislation. Part III of this Note delves into the United States' ad hoc approach to data protection, discussing several piecemeal regulations within the United States, and what type of rights those regulations provide to everyday citizens. The focus of this Part is primarily HIPAA, but other ad hoc regulations are discussed. Finally, Part IV will propose suggestions

---

Protection, J. OF INFO. L. & TECH., June 2000, at 8.

6. *See, e.g.*, Marc-Tizoc González, Habeas Data*: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance*, 90 CHI.-KENT L. REV. 641 (2015); Maxim Gakh, Note, *Argentina's Protection of Personal Data: Initiation and Response*, 2 I/S J.L. & POL'Y 781 (2006).

7. *See, e.g.*, EUROPEAN COMMISSION, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C 131/12).

8. *See, e.g.*, 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 Procession of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulations), arts. 15–18, 2016 O.J. (L 119) 1, 43–45 (EU) [hereinafter, GDPR].

9. *See, e.g.*, Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.); Brougher, *supra* note 2.

for the United States to learn from changing and growing international regulatory norms. In this Part, I will discuss the possible sources of authority for Congress to pass a comprehensive legislative scheme regarding personal data protection, as well as the authority to amend already existing legislation to expand personal rights for data protection. Lastly, I will discuss a possible expansion of the writ of habeas corpus by the judiciary to include personal data.

I. LATIN AMERICA'S TAKE ON DATA PROTECTION: THE WRIT OF HABEAS DATA

The writ of habeas data is a constitutional right available to citizens of certain Latin American countries that provides citizens the right to access personal information collected by the government or a private entity and to challenge or correct the data.[10] The overarching purpose of the writ of habeas data is to protect citizens from the improper use of collected personal data held by the government and private agencies.[11] The writ does not specify what type of data it protects, and in turn, it is used to protect citizens from the procurement and use of all kinds of personal data,[12] such as personal medical records.

The writ of habeas data is one of many constitutionally-based individual complaints throughout the world.[13] In the United States, the writ of mandamus is used to compel a government official to comply with a law or court order,[14] while the writ of habeas corpus is commonly used to require a public official to prove a valid reason for personal physical detention.[15] The writ of habeas corpus in the United States takes on two forms. Its statutory form is used to look behind the face of a criminal conviction to determine if the defendant has been detained in violation of the Constitution.[16] On the other hand, the common law writ of habeas corpus is used whenever someone is detained by the authorities in cases that are not criminal, and the writ is again used to determine whether the detention is valid.[17] The common law writ of habeas corpus can be traced back to the Magna Carta and is still used today in situations where statutory habeas corpus does not apply.[18] These individualized writs and private rights of action are not limited to the United States.[19]

---

10. Gonzalez, *supra* note 6, at 642; *see also* Gakh, *supra* note 6, at 781.

11. *See* Nicola Carah Menaldo, ¿Viva La *Data Protection? Chile As a Touchstone for the Future of Information Privacy*, 18 U. MIAMI INT'L & COMP. L. REV. 137, 156–57 (2011).

12. *Id.* at 156.

13. Guadamuz, *supra* note 5, at 8.

14. *See Developments in the Law—Remedies Against the United States and Its Officials*, 70 HARV. L. REV. 827 (1957).

15. *See* Note, *The Freedom Writ—The Expanding Use of Federal Habeas Corpus*, 61 HARV. L. REV. 657 (1948).

16. *See* Joseph L. Hoffmann & William J. Stuntz, *Habeas After the Revolution*, 1993 SUP. CT. REV. 65, 69 (1993); *see also* 28 U.S.C. § 2254.

17. *See* Joseph L. Hoffmann, *Retroactivity and the Great Writ: How Congress Should Respond to* Teague v. Lane, 1990 BYU L. REV. 183, 183 (1990).

18. *See id.*; Christopher Ogolla, *Non-Criminal Habeas Corpus for Quarantine and Isolation Detainees: Serving the Private Right or Violating Public Policy?,* 14.1 DEPAUL J. HEALTH CARE L. 135 (2011).

19. Guadamuz, *supra* note 5, at 8.

For example, the writ of amparo exists in the Philippines, a remedy available to any person whose right to life, liberty, and security is violated or threatened with violation by an unlawful act or omission of a public official or employee,[20] and the writ of respondeat superior exists in Taiwan, a remedy that makes a superior liable for the acts of the subordinates.[21]

The writ of habeas data was developed as a means for recovering from the turmoil that was suffered in Latin American countries at the hands of strict military regimes.[22] Habeas data roughly translates to "you have the data," and was originally created to assist family members looking for their missing loved ones (*desaparecidos*).[23] Although the writ of habeas data was originally created to assist those who suffered the effects of forced disappearances and extrajudicial executions, a constitutional writ of habeas data has been enacted in many Latin American countries and is available to any citizen within the countries that have enacted it.[24]

The concept behind the writ of habeas data may have been born from the German constitutional right to information self-determination created by the German Constitutional Tribunal.[25] This historic German right allowed its citizens to "know what type of data is stored on manual and automatic databases about an individual."[26] The alleged direct predecessor to the writ of habeas data, which attempted to provide citizens with a private right to action regarding the misuse of their personal data, was developed during the Council of Europe's 108th Convention on Data Protection of 1981.[27] Whatever the origin of the writ may be, in 1988, Brazil was the first country to include the writ of habeas data in its constitution.[28] Several other countries quickly followed: Columbia in 1991, Paraguay in 1992, Peru in 1993, Argentina in 1994, Bolivia in 1995, Ecuador in 1996, Venezuela in 1999, and the Philippines in 2008.[29]

---

20. *See* Atty.Fred, *Writ of Amparo: Questions and Answers*, JLP-LAW BLOG (Sept. 27, 2007), http://jlp-law.com/blog/writ-of-amparo-questions-and-answers/ [https://perma.cc /7H32-3E8D].

21. *See* Atty.Fred, *The Writ of Habeas Data (By Chief Justice Reynato Puno)*, JLP-LAW BLOG (Feb. 23, 2008), https://jlp-law.com/blog/writ-of-habeas-data-by-chief-justice-reynato-puno/ [https://perma.cc/6ZGD-ZSLA].

22. González, *supra* note 6, at 642.

23. Alvin Claridades, *Writs of Amparo and Habeas Data*, ATTY. ALVIN CLARIDADES (Nov. 10, 2016), https://attyalvinclaridades.wordpress.com/2016/11/10/writs-of-amparo-and-habeas-data/ [https://perma.cc/9JS6-YDCU].

24. INQUIRER RESEARCH, *IN THE KNOW: Writ of Habeas Data*, PHIL. DAILY INQUIRER (Nov. 8, 2016, 1:34 AM), http://newsinfo.inquirer.net/842020/in-the-know-writ-of-habeas-data [https://perma.cc/MD3S-CFD8].

25. Guadamuz, *supra* note 5, at 8.

26. *Id.*

27. Claridades, *supra* note 23.

28. IAPP, *Will the New Year Bring New Privacy Laws to Brazil?* (Jan. 28, 2014), https://iapp.org/news/a/will-the-new-year-bring-new-privacy-laws-to-brazil/# [https://perma.cc/AG5X-RKSM].

29. *See* Andrés Guadamuz, *Habeas Data vs. the European Data Protection Directive*, J. OF INFO. L. & TECH., Nov. 2000; Manuel Martinez-Herrera, *From* Habeas Data *Action to* Omnibus *Data Protection: The Latin American Privacy (R)Evolution*, WHITE & CASE (Sept. 2011), https://www.whitecase.com/publications/article/habeas-data-action-omnibus-data-protection-latin-american-privacy-revolution

A. Filing a Writ of Habeas Data

Although the requirements for filing a writ of habeas data vary depending on which constitution the writ is found, the Argentine constitutional writ (and statutory explanations) will be used in this Note to exemplify how, generally, filing a habeas data petition works in the countries where it is available. The Argentine writ of habeas data can be found in Article 43 of the 1994 Argentine Constitution, which establishes the specifics for bringing a habeas data action.[30] In relevant part, the Argentine Constitution states:

> Any person may commence [a writ of habeas data] action to obtain personal information stored in public as well as private registries and databases and to inquire into the purpose of keeping such files. If there is any falsehood or discrimination, the claimant may demand the suppression, rectification, confidentiality, or updating of the data. There shall be no violation of the secrecy of newspaper sources.[31]

The Supreme Court of Argentina has held that "a writ of habeas data could secure personal data in the possession of the national security forces, even if the disclosures of that information [might] affect security, national defense, foreign relations, or a criminal investigation."[32] The scope and use of habeas data is broad and somewhat ambiguous under both the Argentine Constitution[33] and subsequent judicial interpretations;[34] because of this, the Argentine legislature went on to clarify further what a claim seeking habeas data relief must include.[35]

In 2000, the Argentine legislature passed the Law for the Protection of Personal Data (LPPD), which includes forty-eight total sections, but only the last section discusses habeas data actions.[36] The LPPD does not create a new cause of action for the writ of habeas data—it simply codifies the already existing constitutional right and lays out the necessary procedural requirements.[37] The LPPD defines what it means to be "any person" with the ability to bring an action for the constitutional writ of habeas data, and it clarifies what exactly a person must prove at the outset of the cause of action to be a proper plaintiff with standing.[38] "Any person" as listed in

---

[https://perma.cc/TZ3Z-K62L]; INQUIRER RESEARCH, *supra* note 24.

30. Gakh, *supra* note 6, at 789.

31. Gonzalez, *supra* note 6, at 656 (quoting ÁNGEL R. OQUENDO, LATIN AMERICAN LAW 397 (2d ed. 2011) (translating Art. 43, CONSTITUCIÓN NACIONAL [CONST. NAC.] (Arg.))

32. *Id.* (internal quotations omitted).

33. *See id.* (showing the general and ambiguous language of the writ of habeas data in Argentina).

34. *Id.*

35. Gakh, *supra* note 6, at 789.

36. *Id.*

37. *Id.*

38. *See* Ley No. 25.326, 3 Oct. 2000, Proteccion de los Datos Personales, [Personal Data Protection Act] (Arg.), *translated* in Argentina Personal Data Protection Act (2000), Act 25,326 (U.N. Pub. Admin. Network ed.), http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044147.pdf [https://perma.cc/R5A8-7RY5].

Article 43 of the 1994 Argentine Constitution is defined by the LPPD to include the affected person and additionally, "a guardian, curator, or successor of that person."[39] When filing a writ of habeas data, the plaintiff must identify the name and domicile of either the data file or the register, while additionally attempting to identify the appropriate government body when a governmental data bank is involved.[40] A writ of habeas data may be filed against a government agency, official, or private entity.[41] Once the plaintiff meets her burden and initial showing, the burden shifts to the defendant to either provide the plaintiff with the information or "demonstrate why the questioned information was included in the database and the reasons it refrained from providing the plaintiff's requested information."[42]

B. The Writ of Habeas Data and Protection of Personal Medical Records

Imagine a young woman in Argentina went to a government-run health care facility and had a basic metabolic panel run on a blood sample—a simple yearly checkup. When the test came back, it showed that the woman had markers for a rare genetic disorder for which she exhibited no symptoms. The woman, through the process of the yearly checkup, gave a governmental entity consent to test and store her personal medical data (her genetic information and the markers for her genetic disorder). What could she do if she found out, or even merely suspected, that the medical data was being used and shared between the government entity and private medical companies for testing and analysis regarding a possible cure for the genetic disease without her consent?

Because she is an Argentine citizen, she would be afforded the constitutional writ of habeas data. When filing the writ, she would have to identify the name and domicile of either the data file or the register and attempt to identify the appropriate government body and data bank.[43] The requirements of plaintiffs in habeas data actions under the Argentine Constitution are vague and often require unknown facts, figures, and locations of data storage. If the plaintiff in this case could meet her initial burden, the original government health care entity that breached her rights, or is suspected of breaching her rights, would have to either provide the plaintiff access to its records regarding the dissemination and processing of her data, or demonstrate why the questioned information was included in the database and provide the reasons it refrained from providing the plaintiff's requested information.[44]

Once the plaintiff received the information she requested through her writ, "[i]f there is any falsehood or discrimination [within her data records], the claimant may demand the suppression, rectification, confidentiality, or updating of the data."[45] In this case, because the information regarding the plaintiff's genetic markers was

---

39. *See id.*

40. Gakh, *supra* note 6, at 789.

41. *See* Gonzalez, *supra* note 6, at 656 (quoting language from the Argentine Constitution that "personal information [can be] stored in *public* as well as *private* registries and databases.") (emphasis added).

42. Gakh, *supra* note 6, at 781.

43. *Id.* at 789.

44. *Id.* at 789–90.

45. Personal Data Protection Act, *supra* note 38.

unlawfully disseminated, the ability to suppress, correct, update, or mark the information as confidential would provide a remedy for the plaintiff to keep her personal medical records just that, personal.

II. THE EUROPEAN UNION'S TAKE ON DATA PROTECTION: THE DATA PROTECTION DIRECTIVE AND THE GENERAL DATA PROTECTION REGULATION

Up until May of 2018, personal data in the European Union (EU) was protected by the Data Protection Directive.[46] The Directive was passed by the EU in 1995 and until recently has been the driving force for data protection throughout the twenty-seven countries it affects.[47] However, in May of 2018, the EU turned the Directive into a regulation by passing the General Data Protection Regulation.[48] Generally, a directive is implemented to ask, or strongly suggest, that nations bring their own laws in line with other EU Member States (for a cross-border, cohesive set of laws).[49] However, a directive is just a request and a guideline; it does not actually change any currently enacted laws or have any binding authority.[50] On the other hand, a regulation "automatically becomes part of the national legal system of each Member State" and is a mandatory change in law.[51] As such, a regulation, like the GDPR, is the most direct way for the EU to regulate the laws of its Member States.[52]

Although the Directive was one of the early global attempts at personal data protection, it "proved to be very cumbersome due to the significant discrepancies between the interpretations [and] implementations" of each individual Member State.[53] The GDPR is an attempt to resolve these issues by removing them completely; the GDPR does not need to be implemented by individual Member State legislatures at all and has the full force of law upon Member States.[54] This Part will summarize the Directive for its historical value and effects on the protection of personal data, and will discuss the rights that the Directive provided to citizens. Then, this Part will analyze the changes to the EU's laws under the GDPR and what the changes mean for a Member's citizen looking to challenge the use of her personal medical data. The EU has been one of the world leaders in personal data protection,

---

46. *GDPR Portal: Site Overview*, EU GDPR.ORG, http://www.eugdpr.org/ [https://perma.cc/C2TT-NK5N].

47. *See* Christopher Wolf & Timothy P. Tobin, *The European Union ("EU") Data Privacy Directive*, PROSKAUER, http://www.proskauerguide.com/law_ topics /28/III/:pf_printable/Template=print? [https://perma.cc/V783-7XFP]; *see also* Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight—What The Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 824 (2011).

48. Zack Gross, *8 Ways EU GDPR Differs From the EU Data Protection Directive*, CLOUDLOCK (May 12, 2016), https://www.cloudlock.com/blog/eu-gdpr-vs-data-protection-directive/ [https://perma.cc/3NY7-LGXR].

49. Gilbert, *supra* note 47, at 823.

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.* at 824.

54. *Id.* at 825.

and the analysis of the past directive and current regulation are perfect examples of what regulating bodies, like the United States legislature and judiciary, can do to provide their citizens with more rights to protect their own data.

A. The Data Protection Directive

The Directive was intended to create a floor of protections for personal data held within all EU Member States.[55] It was established based on eight basic principles: (1) data processing purpose limitation, (2) data quality, (3) data security, (4) sensitive data protection, (5) processing transparency, (6) data transfer protection, (7) independent data processing oversight, and (8) individual redress for violations.[56] Under the Directive, very basically, "personal data [could] not be processed without the consent of the data subject unless processing is necessary for the performance of a contract with the data subject or some explicit exception applies."[57] This data processing could also be strictly limited to the purpose originally notified to, or agreed upon with, the data subject.[58] The Directive did not apply in two contexts: one, when the activity was outside the scope of community law—for example, national security and criminal law—and two, when the processing of the data was done by a natural person in the course of a purely private and personal activity.[59]

The Directive provided several definitions and, although fairly broad, started to define the scope of the Directive's regulatory application.[60] First, "processing of personal data" was defined as "any operation or set of operations" that included "collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[61] Similarly, "personal data" was defined just as broadly as "any information relating to an identified or identifiable natural person."[62] The Directive imposed liability on the data controller for violations of its terms[63] and defined "data controller" as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[64] The broadness of the Directive's definitions contributed to an overall lack of

---

55. Ryan Moshell, Note, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 368 (2005).

56. *Id.*

57. Christopher Kuner, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, 35 INT'L L. 79, 82 (2001); *see also* Moshell, *supra* note 55, at 368.

58. Kuner, *supra* note 57, at 82.

59. Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 182 (1999).

60. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. 95 (L 281) [hereinafter, Data Protection Directive].

61. *Id.*

62. *Id.*

63. Kuner, *supra* note 57, at 82.

64. Data Protection Directive, *supra* note 60.

clarity within the regulation, and one of the main problems it suffered since its enactment—varying interpretations and implementations between Member States—must stem from the ambiguity within the text itself. However ambiguous, the Directive paved the way for the creation of a new right: the right to be forgotten.[65]

1. The Data Protection Directive and the Implied Right to Be Forgotten

The right to be forgotten can be found in European law as early as 1965 when it was mentioned in a French court case through the use of the French term *le droit a l'oubli* (translated as "right to be forgotten" or "right to oblivion").[66] However, this right to be forgotten dealt less with the digital age (as the original *le droit a l'oubli* was mentioned before the rapid rise of computer technology) and more with wanting to make personal information disappear, such as record of a criminal conviction after a certain time period had elapsed.[67] The more current right to be forgotten, however, applies to personal data in the age of new information and communication technologies.[68] However, the right to be forgotten is somewhat of a misnomer: it does not actually require that information be forgotten (simply because memory is what is forgotten) but instead is a right to deletion and censorship.[69] An appropriate definition of the right to be forgotten is "the right for natural persons to have information about them deleted after a certain period of time."[70] In 2016, the Court of Justice for the European Union addressed the right to be forgotten in the *Google Spain* case.[71]

In *Google Spain*, referenced to the Court of Justice of the European Union by the Spanish Court that had proceeded over the issue, several issues were decided regarding the scope of the Directive; the relevant question to the analysis in this Note is "whether an individual has the right to request that his or her personal data be removed from accessibility through a search engine (the 'right to be forgotten')."[72] The final decision by the Court of Justice was that individuals do have the right—when certain conditions are met—to ask search engines to remove personal information from links that can be found in search results.[73] This right applies when the information requested to be deleted is inaccurate, inadequate, irrelevant, or excessive.[74] The court, however, indicated that the right to be forgotten is not

---

65. W. Gregory Voss & Céline Castets-Renard, *Proposal for an International Taxonomy on the Various Forms of the "Right To Be Forgotten": A Study on the Convergence of Norms*, 14 COLO. TECH. L.J. 281, 284 (2016).

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.* at 285.

70. *Id.*

71. EUROPEAN COMMISSION, *supra* note 7, at 1 (stating the holding of the *Google Spain* case and how it effects the EU's enforcement of the Directive); *see* Voss & Castets-Renard, *supra* note 65 at 285.

72. EUROPEAN COMMISSION, *supra* note 7, at 1.

73. *Id.*

74. *Id.*

absolute and will be considered on a case-by-case basis, balancing the right to be forgotten against the freedoms of expression, speech, and the media.[75]

The procedure associated with the right to be forgotten (as established in *Google Spain*) is rather malleable but is generally as follows: One, the individual requests the removal of data that is inaccurate, inadequate, irrelevant, or excessive.[76] Two, the court determines, on a case-by-case basis, whether the individual's right to privacy, the individual's role in the public, the nature of the information, and the public interest against censorship should result in the information being "forgotten."[77] If the court determines that the information should be deleted, the data controller has the obligation to notify any third party "to whom the data [has] been disclosed" that the data is subject to deletion or censorship.[78]

B. The General Data Protection Regulation

On April 14, 2016, the European Union passed the regulation currently in effect, which has now replaced the Directive.[79] The GDPR was first created, and subsequently passed, in response to the lack of uniformity among the Member States' data protection guidelines (a process that started in 2012).[80] Although passed for many reasons, the initial concerns that sparked the GDPR's proposal were Members' "fragmented legal environment[s] which ha[d] created legal uncertainty and uneven protection for individuals and also unnecessary costs and administrative burdens for businesses" to comply with multiple interpretations of the Directive.[81] The GDPR went into full effect on May 25, 2018, and all businesses and entities within the Member States, or who deal with citizens of the Member States, are now expected to be in compliance with the regulation.[82]

The GDPR's aim is the same as the Directive's in that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right."[83] However, the GDPR attempts to achieve that purpose with more accuracy and less ambiguity, as it is a binding regulation and no longer simply a directive (or suggestion) to the EU's Member States.[84]

Aside from its binding, regulatory nature, the GDPR actually proves to be substantively very different from the Directive in several ways. A few prominent changes are as follows: One, the territorial scope has increased so more countries, other than EU Member States, have to comply because even companies that are not based within Member States are required to follow the GDPR when interacting with

---

75. *Id.*
76. *Id.* at 5.
77. *Id.* at 4–5.
78. Data Protection Directive, *supra* note 60, at art. 12.
79. *GDPR Portal: Site Overview*, *supra* note 46.
80. David Erdos, *European Union Data Protection Law and Media Expression: Fundamentally Off Balance*, 65 INT'L. & COMP. L.Q. 139, 143 (2016).
81. *Id.* (internal quotations removed).
82. *GDPR Portal: Site Overview*, *supra* note 46.
83. GDPR, *supra* note 8.
84. *See* Gilbert, *supra* note 47, at 823.

citizens of the EU.[85] Two, penalties for noncompliance have increased and can be as high as four percent of a company's annual global turnover.[86] Three, requirements for consent have been strengthened, and the means by which a company can obtain consent have been narrowed.[87] Four, a right to access has been included within the GDPR, allowing data subjects to request access to a data controller's information (whether or not they have proof that the data controller has their personal information or is misusing that personal information) to determine whether data concerning them is being processed, where, and for what purpose.[88] Five, and rather importantly, a right to erasure (similar to the right to be forgotten) has been directly included within Article 17 of the GDPR.[89]

1. Challenging the Use of Personal Data through the GDPR Using the Right to Access, the Right to Restrict Processing, and the Right to Erasure

Can I see the data you have on me? Can you cease processing the data that is accessible to you? Can you delete the data you have stored on me? These are all requests a data subject can now make under the GDPR. The GDPR gives rights to data subjects for access, restriction of processing, and removal of certain types of personal data held by data controllers.[90] The GDPR defines its terms in a similar manner to those defined terms in the Directive.[91] "Personal data" under the GDPR "means any information relating to an identified or identifiable natural person"[92] (this is the same definition employed by the Directive).[93] "Data subject" is defined as a natural person "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."[94] Lastly, "data controller" under the GDPR is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[95] The right to access, the right to restriction of processing, and the right to erasure may have been alluded to through the EU's past court decisions (*Google Spain*) and implied within the Directive,[96] but with the GDPR, they are explicitly stated front and center.

---

85. *GDPR Key Changes*, EU GDPR.ORG, http://www.eugdpr.org/key-changes.html [https://perma.cc/VT82-FN3J].

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.*

91. GDPR, *supra* note 8; *see supra* notes 60–65 and accompanying text.

92. *Id.*

93. Data Protection Directive, *supra* note 60.

94. GDPR, *supra* note 8.

95. *Id.*

96. *See, e.g.*, Data Protection Directive, *supra* note 60, at art. 12; EUROPEAN COMMISSION, *supra* note 7, at 1.

The right to access seems to be an add-on protection to the *Google Spain*'s version of the right to be forgotten. The right to access specifically allows the data subject the "right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data."[97] In other words, the data subject does not need to have any knowledge that the controller is actually storing or processing personal data of the data subject. The purpose is to allow "individuals to access their personal data . . . so that they are aware of and can verify the lawfulness of the processing."[98] Data subjects can access (1) the purpose of their personal data processing, (2) the categories of personal data concerned, (3) the recipients to whom the personal data has been (or will be) disclosed, (4) the estimated period of time the data will be stored if possible, (5) the right to rectify or erase the data, (6) the right to file a complaint with a supervisor, (7) the source of the data, and (8) the existence of an automated decision-making process.[99] The data controller must provide this information without charge to the data subject requesting it.[100]

The right to restriction of processing allows a data subject to obtain from the controller restriction of processing where certain circumstances are met.[101] A restriction of processing is available when one of the following occurs: (1) the accuracy of the data is contested, (2) the processing of the data is unlawful and the data subject opposes the erasure of the data, (3) the controller no longer needs the data but is required to store it for some other reason, or (4) the data subject has properly objected to the data's processing.[102] If one of the above circumstances is met, the data subject can request that the data controller immediately cease processing her data, and the data controller must comply.[103]

Lastly, the right to erasure, which is also listed as the right to be forgotten, is the right of a data subject to request that her information be removed or erased when certain circumstances are present.[104] The right to erasure is available, according to the GDPR, when (1) the data is no longer necessary for the purposes it was collected, (2) the data subject withdrew proper consent (and there is no other legal grounds for processing), (3) the data subject properly objects to the data processing, (4) the data is unlawfully processed, (5) the data must be erased for compliance with a legal obligation, or (6) the data was collected in relation to the offer of information society services.[105] If one of these conditions is met, the data controller is required to promptly delete the data, and if the data was made public by the controller, the controller must also take reasonable steps to inform other controllers that are processing the data that it is subject to erasure and such controllers should erase any links, copies, or replications of that data.[106]

---

97. GDPR, *supra* note 8.
98. *Id.*
99. *Id.* at art. 15.
100. *Id.*
101. *Id.* at art. 17.
102. *Id.*
103. *Id.*
104. *Id.* at art. 16.
105. *Id.*
106. *Id.*

These three rights provided by the GDPR allow data subjects an incredible amount of control for managing the use of their personal data. Data subjects can merely request information regarding their personal data (the right to access),[107] or can go a step further and request that the data controller restrict processing of their data (the right to restriction of processing),[108] or, even further, request the data be deleted all together (the right to erasure).[109]

Although not inherently clear from the language of the GDPR, the regulation seems to indicate that government entities would be considered a "data controller" and that the GDPR would allow data subjects to use their private rights of action against government and private entities alike. Because a data controller is defined, in part, as a "public authority [or] agency,"[110] the regulation seems to allow for challenges against the government for personal data that is stored or processed by a government agency. If this is the case, the right to access, the right to restriction of processing, and the right to erasure, when used against the government, is a huge and distinct step toward private citizen control and knowledge of how their personal data is being used.

2. The General Data Protection Regulation and the Protection of Personal Medical Records

Take our sample plaintiff from Part I.B of this Note—the woman with a rare genetic disorder and results from a routine blood test—but now, she is a citizen of Ireland (a Member State of the EU) and has attended a government run clinic. How could she challenge the improper dissemination of her medical information? She has three relevant rights available to her: the right to access, the right to restrict processing, and the right to erasure.[111]

Our plaintiff is able to use her right to access to obtain a free copy of information regarding the purpose of her personal data and the recipients to whom the personal data has been (or will be) disclosed.[112] With this information, the plaintiff is better equipped to defend her rights to restriction of processing and erasure because she has been informed of exactly why her data is being processed and to whom exactly it is being shared. Unlike the Argentine plaintiff utilizing the writ of habeas data, our Irish plaintiff need not know the location, name, or government or private entity database storing, processing, or receiving her personal medical data.

Following the retrieval of her information by way of the right to access, the plaintiff can either choose to exercise her right to restriction of processing or her right to erasure. Although our plaintiff could absolutely request the deletion of her personal medical data because it was unlawfully processed by being disseminated, without our plaintiff's consent, to other medical testing facilities, and therefore, falls

---

107. *Id.* at art. 15.
108. *Id.* at art. 17.
109. *Id.* at art. 16.
110. *Id.* at art. 1.
111. *See, e.g.*, Data Protection Directive, *supra* note 60, at art. 12; EUROPEAN COMMISSION, *supra* note 7, at 1.
112. GDPR, *supra* note 8, at art. 15.

under one of the required circumstances to invoke the right to erasure,[113] the right to restriction of processing would be a better option. A restriction of processing is available when the processing of the data is unlawful, and the data subject opposes the erasure of the data.[114] Our plaintiff may wish to keep her medical data within the database of her health care provider (for obvious reasons of accurate medical treatment), but she wants to stop the processing that is being done without her consent. Our plaintiff could request not only that the original government clinic cease processing her data, but that all other entities to whom the data was shared (which she found out when she vindicated her right to access) also cease their processing, whether those entities are public or private. As used in our plaintiff's case, the rights to access, restrict processing, and erasure explicitly stated within the GDPR would provide a remedy for our plaintiff to keep her personal medical records just that, personal.

III. IS THE UNITED STATES FOLLOWING THE GLOBAL PATH ON PERSONAL DATA PROTECTION?

Times are changing in the way of personal data protection, as exemplified by the European Union's comprehensive past-directive and current regulation and the Latin American writ of habeas data.[115] The EU's past-directive and current regulation are pioneers in the way of personal data protection. The right to be forgotten and subsequently, the right to access, erasure, etc., are incredibly citizen-focused and give the power to regulate personal data back to the citizens themselves, which is really where such enforcement power should lie. The writ of habeas data is a pioneer in its own way—it is a constitutionally enacted right to the people of the countries where it is utilized. A constitutional right—more so than a regulation, directive, or law—ingrains into the society the importance of the protections the right provides. Specifically in the case of the writ of habeas data, it shows that the nation and the people of the nation are making it a constitutional priority to protect personal data. Although other countries have passed regulations that protect personal data, they are not the pioneers or the forward-thinkers. Many nations have followed the example set by the EU through the Directive, and countries providing for a writ of habeas data have taken those measures one step farther by enshrining those protections into the constitution. Although the EU and Latin American Countries are great examples of government bodies attempting to rectify the lack of personal data protection in a quickly changing technological era, they are not lone wolves in this field.[116]

These are a few additional examples of government agencies taking steps to protect personal data: Mexico governs the storage and use of personal data by way of the comprehensive Federal Law for Protection of Personal Data in Possession of Third Parties, which was passed in 2010, and was followed by specific regulations, privacy notice rules, and binding self-regulation parameters, which further explained

---

113. *Id.* at art. 16.

114. *Id.* at art. 17.

115. *See generally* GDPR, *supra* note 8; Data Protection Directive, *supra* note 60; Gakh, *supra* note 6; Gonzalez, *supra* note 6.

116. *See* GETTING THE DEAL THROUGH, *supra* note 4.

the federal law.[117] The law provides individuals with ARCO rights: the rights to *A*ccess, *R*ectify, *C*ancel (stop processing), or *O*ppose data processing.[118] Similar to Mexico, in 2012, Singapore passed a comprehensive law governing the protection of personal data: the Personal Data Protection Act (PDPA).[119] This act is working alongside a patchwork set of individual laws (including common law) that were in effect prior to the PDPA's passage[120] (the type of patchwork system that is currently available in the United States).[121] Under the PDPA, an individual has the right to withdraw her consent in respect to the collection, use, or disclosure of her data.[122] Lastly, Switzerland has a federal law—the Federal Data Protection Act—that regulates the relationship between individuals with corporations and the federal authorities.[123] At the same time, Switzerland allows its states to comprehensively regulate the relationship between individuals and state authorities.[124]

What does this all mean for the global path in personal data protection? Countries, regions, and entities alike are moving to a more comprehensive scheme of data protection for individuals.[125] It is no surprise either. We live in a digital age, where personal information is disseminated, reproduced, and published all the time.[126] Logically, the protection of personal information is growing in an attempt to align with the ever-constant need for privacy. There is one other common global theme: the right of individuals to, in some way, challenge the use, processing, production, or dissemination of their personal data.[127] Whether it be the writ of habeas data,[128]

---

117. GETTING THE DEAL THROUGH, DATA PROTECTION & PRIVACY IN 26 JURISDICTIONS WORLDWIDE 2014, 108 (Rosemary P. Jay & Hunton & Williams, eds., Law and Business Research 2d ed. 2013).

118. *Id.*

119. *Id.* at 124.

120. *Id.*

121. GETTING THE DEAL THROUGH, *supra* note 4, at 208.

122. GETTING THE DEAL THROUGH, *supra* note 117, at 128.

123. GETTING THE DEAL THROUGH, DATA PROTECTION & PRIVACY IN 21 JURISDICTIONS WORLDWIDE 2013, 122 (Rosemary P. Jay & Hunton & Williams, eds., Law and Business Research 2012).

124. *Id*.

125. *See* GDPR, *supra* note 8; Data Protection Directive, *supra* note 60; GETTING THE DEAL THROUGH, *supra* note 117, at 108, 124, 128; Gakh, *supra* note 6; Gonzalez, *supra* note 6.

126. Andrew Liptak, *Hackers Accessed More Personal Data from Equifax than Previously Disclosed*, VERGE (Feb. 11, 2018, 10:55 AM), https://www.theverge.com/2018/2/11/17001046/equifax-hack-personal-data-tax-identification-numbers-email-addresses-drivers-licenses-cybersecurity [https://perma.cc/3SUU-WXTM] (discussing the disclosure and danger of the dissemination of personal information from the credit rating agency Equifax); David Reid, *EU Says Facebook's Apology 'Not Enough' as It Announces Personal Data Investigation*, CNBC (Apr. 12, 2018, 9:30 AM), https://www.cnbc.com/2018/04/12/eu-says-facebooks-apology-not-enough-as-it-announces-personal-data-investigation.html [https://perma.cc/767E-5DWR] (discussing the international concerns results from an "inadvertent" and major personal data leak from social media site, Facebook).

127. *See* GDPR, *supra* note 8; Data Protection Directive, *supra* note 60; Gakh, *supra* note 6; Gonzalez, *supra* note 6.

128. *See, e.g.*, Gakh, *supra* note 6; Gonzalez, *supra* note 6.

the right to be forgotten,[129] the right to access, the right to erasure,[130] or the right to withdraw consent,[131] government bodies are taking notice that citizens should be in the driver's seat when it comes to the control of their own personal data.

A. The Current U.S. Approach to Data Protection: The Ad Hoc Approach and the Protection of Personal Health Care Data

The United States employs a "patchwork quilt" of personal data protections. Unlike the EU or Latin American countries, among others, the United States does not have any laws or regulations dedicated to data protection in a general sense. Instead, it creates and regulates data protection on an industry-by-industry basis.[132] To make matters more confusing, these data protection laws are developed both at the federal and state levels.[133] Unfortunately, since 1973 the United States has stalled in its conversations regarding personal data protection and data privacy. The United States provided a backbone for privacy laws worldwide when "the U.S. Department of Health, Education, and Welfare (HEW) published the Fair Information Practice Principles (FIPPs)." Since the passage of this report, however, the United States progression in data privacy has become stagnant.[134]

The approach the United States has taken to data protection seems to be one of fixing specific problems in topical areas as they arise.[135] For example, the Cable Television Consumer Protection and Competition Act, which amended the Communications Act of 1934, deals with data problems and consumer information protections related to the influx of cable television in the 1990s,[136] and the Fair Credit Reporting Act provides privacy protection of consumer information contained in the files of consumer reporting agencies.[137] These are not the only examples where Congress saw a problem in a certain area of law that dealt with information privacy, and then chose to pass a law addressing only that topical area of data protection.[138]

---

129. *See, e.g.*, EUROPEAN COMMISSION, *supra* note 7.

130. *See, e.g.*, GDPR, *supra* note 8

131. GETTING THE DEAL THROUGH, *supra* note 117, at 124.

132. GETTING THE DEAL THROUGH, *supra* note 4, at 208 ("The US legislative framework for the protection of [personal data] resembles a patch-work quilt. Unlike other jurisdictions, the US does not have a dedicated data protection law, but instead regulates primarily by industry, on a sector-by-sector basis.")

133. *Id.*

134. Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 LEWIS & CLARK L. REV. 595, 596 (2016).

135. *See, e.g.*, Right to Financial Privacy Act, 12 U.S.C. §§ 3402–3403, 3412 (2012); United States v. Miller, 425 U.S. 435, 442–444 (1976).

136. Pub. L. No. 102-385, 106 Stat. 1460 (1992).

137. 15 U.S.C. § 1681 (2012).

138. Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2012); Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2012); Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 (2012); Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), Pub. L. No. 109-187, 117 Stat. 2699 (codified in scattered sections of 15 & 18 U.S.C.); Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.).

This ad hoc, and solely topical (either by type of data or means of transmitting that data), approach to data regulation is a piecemeal compilation of the rights found in the First, Fourth, Fifth, and Fourteenth Amendments,[139] accompanied by various federal and state laws, and common law.[140]

Examples of topically-based federal data protection acts in the United States include the Federal Trade Commission Act,[141] the Children's Online Privacy Protection Act,[142] the Electronic Communications Privacy Act,[143] the Controlling the Assault of Non-Solicited Pornography and Marketing Act,[144] and HIPAA.[145] This type of approach may stem from the lack of explicit constitutional requirements and authority for the protection of personal data and privacy or, alternatively, from citizens' distrust in the government producing a comprehensive legislative scheme.[146] This collage of statutory law "results from the sectoral approach having been created backwards"—that is, "[r]ather than coming up with an overall picture and then breaking it up into smaller pieces that mesh together, Congress has been sporadically creating individual pieces of ad hoc legislation."[147]

When it comes to health care data regulations, HIPAA is the forerunner in the United States. HIPAA regulates personal health information, which is defined as:

> any information, whether oral or recorded in any form or medium, that . . . is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and . . . relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[148]

---

139. *Id.*

140. *See, e.g.*, 15 U.S.C. §§ 41–58; 15 U.S.C. § 1681; 15 U.S.C. §§ 6501–6506; 18 U.S.C. § 2510.

141. 15 U.S.C. §§ 41–58.

142. 15 U.S.C. §§ 6501–6506.

143. 18 U.S.C. § 2510.

144. 15 U.S.C. §§ 7701–7713; 18 U.S.C. §1037.

145. Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.).

146. Moshell, *supra* note 55, at 368.

147. U.S. DEP'T OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK, 60 (2010), http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policyframework [https://perma.cc/K9KM-WT5L].

148. 42 U.S.C. § 1171(4).

Although HIPAA provides a generally robust set of protections and regulations of health care data,[149] it suffers from several problems.[150] HIPAA is limited because it does not include all custodians of health information.[151] Similarly, it uses a downstream protection model meaning that it does not regulate the collection of health data but regulates only the dissemination of that data.[152]

However, there is one specific right—or more appropriately, lack of a right—that warrants discussion here. The federal HIPAA provides *no* private right of action to individuals whose health data is improperly handled, processed, or stored.[153] The only person or entity that is able to bring a suit under HIPAA is the Secretary of the U.S. Department of Health and Human Services.[154] The Secretary can assess penalties for violations, which can include civil and criminal penalties, but the Secretary is the only individual who has standing to enforce HIPAA rights.[155] Some states have provided private right of actions to its citizens for breaches of state equivalents to the federal HIPAA,[156] but this does nothing to remedy the lack, within the statute itself, of a federal private right of action and does more to create a disjunctive personal data protection legal atmosphere.

IV. WHAT CAN THE UNITED STATES LEARN FROM THE EXPANDING INTERNATIONAL PERSONAL DATA PROTECTION RIGHTS?

The increasing importance of international data transfer in the global economy, when combined with a global trend toward comprehensive data protection,

---

149. *See* 42 U.S.C. § 1320d-6 (delineating criminal penalties for misuse of private medical data) ("A person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person" can be charged criminally under the Act.); *see also* Austin Rutherford, Byrne*: Closing the Gap Between HIPAA and Patient Privacy*, 53 SAN DIEGO L. REV. 201, 206 (2016) ("To safeguard [private healthcare information] PHI, a covered entity or business associate must implement reasonable administrative, technical, and physical safeguards. Examples of these safeguards include, respectively, training employees, encrypting information, and limiting access to buildings where PHI is stored. HIPAA and the Privacy Rule create a floor, not a ceiling, from which states can enact more stringent laws to protect patient privacy.").

150. Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143, 161 (2017).

151. *Id.*

152. *Id.* While HIPAA also covers authorized and nonauthorized transmissions of data, breach notification requirements, and permissive and required disclosures, those regulations do not deal specifically with protections for individuals for personal healthcare data, and therefore will not be discussed further in this Note. *See* Brougher, *supra* note 2, at 532; *see also* Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.).

153. Brougher, *supra* note 2, at 532. *See also* Pub. L. No. 104-191, 110 Stat. 1936.

154. Brougher, *supra* note 2, at 532. *See also* Pub. L. No. 104-191, 110 Stat. 1936.

155. Brougher, *supra* note 2, at 532. *See also* Pub. L. No. 104-191, 110 Stat. 1936.

156. For example, the California HIPAA-type statutes regulate the disclosure of medical information by providers and actions that can be brought by unlawful disclosure of patient information. CAL. CIV. CODE § 56.10–16 (West 2007).

highlights the necessity of a United States data-protection position that contributes to, rather than detracts from, global stability.[157]

As demonstrated from Parts I–III, from one end of the globe to the other, countries have passed or are passing comprehensive personal data protection regulations and providing their citizens with a right to do something about entities that misappropriate their personal data.[158] The current state of U.S. data protection laws is haphazard at best. As explained in Part III, the U.S. has approached data protection on an ad hoc basis, facing problems with personal data protection as they arise, and failing to pass one comprehensive data protection law.[159] Could a comprehensive data protection regulation passed by the United States federal government do its citizens good? Absolutely; from a citizen's point of view, there is no contesting that more personal data protection is a good thing in this growing technological era, but a comprehensive regulation would face an uphill battle within the United States. The GDPR and the rights it confers onto its citizens, if imported into U.S. law, would raise First Amendment freedom of speech and freedom of expression concerns. The right to be forgotten (or the right to erasure) is especially problematic because of its censoring nature.[160] Similarly, the United States government lacks the constitutionally-exclusive right to regulate and protect personal data—the right to privacy isn't even explicitly stated in the Constitution.[161]

So what authority would Congress have to enact and enforce such a broad and comprehensive act or regulation? The Commerce Clause is one possible avenue. The Commerce Clause, found in Article I, Section 8, Clause 3 of the U.S. Constitution, allows Congress to regulate commerce "among the several States," commonly referred to as interstate commerce.[162] By using the power given to Congress by the Commerce Clause, Congress could regulate the movement of data across state lines as commerce in data. The Commerce Clause would provide Congress, as it has in the past, the necessary authority to pass a comprehensive legislative scheme broadly regulating the movement of data.[163] The problem? This type of regulation could not, necessarily, regulate the storage of data in libraries or archives because such data may be considered purely local commerce or not within the stream of commerce at

---

157. Moshell, *supra* note 55, at 359.

158. *See, e.g.,* GDPR, *supra* note 8; Data Protection Directive, *supra* note 60; GETTING THE DEAL THROUGH, *supra* note 117, at 108, 124, 128; Gahk, *supra* note 6; Gonzalez, *supra* note 6.

159. *See supra* Part III.

160. *See, e.g.*, Robert Kirk Walker, Note, *The Right To Be Forgotten*, 64 HASTINGS L.J. 257, 274–78 (2012).

161. Moshell, *supra* note 55, at 373.

162. U.S. CONST. art. I, § 8, cl. 3. A regulation passed by Congress that allowed ordinary citizens to challenge, and possibly require, that a search engine, news station, or database remove, delete, or alter their information would raise serious freedom of press concerns, much like strict defamation law limitations. "In the United States, however, the government is constitutionally prohibited under the First Amendment from interfering with the flow of information, except in the most compelling circumstances." Cate, *supra* note 59, at 179–80.

163. *See, e.g.*, 18 U.S.C. § 2510 (regulating the interception of electronic communications).

all.[164] Although the Commerce Clause could be used to allow Congress to pass a more comprehensive data protection scheme than is currently being employed, a statute enacted under the authority of the Commerce Clause would still fail to reach a large sector of personal data by failing to reach data that is purely local. Nevertheless, a comprehensive data protection scheme regulating the movement and commerce of data would certainly be a place to start.

In addition to the Commerce Clause, Congress, with the help of the President, may be able to enter into a treaty with another country, set of countries, or already formed union (for example, the European Union), which would allow Congress to enact legislation according to such a treaty comprehensively regulating private personal data. The President could, with the consent of the Senate, enter into this treaty under his constitutionally-enumerated power.[165] However, as briefly discussed in *Bond v. United States*,[166] the scope of the treaty power in this circumstance is open to challenge. In *Bond*, the Court stated that it need not consider the scope of the treaty power because the defendant was criminally charged under a federally enacted statute (pursuant to a treaty), and he was not charged under a self-executing treaty.[167] If Congress were to sign a treaty with the EU, applying the GDPR to the United States, this would be a self-executing treaty because the GDPR is a regulation, not a set of guidelines like the "Convention on the Prohibition of the Development, Production, Stockpiling, and Use of Chemical Weapons and on Their Destruction" analyzed in the *Bond* case.[168] However, if Congress were to enter into a non-self-executing treaty[169] to regulate the transfer, use, storage, and processing of personal

---

164. Congress is able to regulate interstate commerce by way of people, things, or instrumentalities in the stream of commerce. This was developed through a line of cases in the Supreme Court. Gonzales v. Raich, 545 U.S. 1 (2005) (holding that a comprehensive regulation prohibiting the home-growth of marijuana was within the stream of commerce because if she did not grow it, she would have to partake in the interstate market); Heart of Atlanta Motel v. United States, 379 U.S. 241 (1964) (holding that Congress could regulate a hotel because it impedes travel and has a substantial effect on interstate commerce); Wickard v. Filburn, 317 U.S. 111 (1942) (holding that a local farm who chose to make his own wheat and abstain from the interstate market was sufficiently under the control of Congress because aggregation of abstainers would affect interstate commerce); NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1 (1937) (holding that a strike that stops product of steel at one facility, affects the whole stream of commerce and can be regulated by Congress).

165. "[The President] shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur." U.S. CONST. art. II, § 2, cl. 2.

166. 134 S. Ct. 2077 (2014).

167. *Id.* at 2087–94.

168. *Id.* at 2084–86.

169. "A self-executing treaty is a treaty that becomes judicially enforceable upon ratification. As opposed to a [non-self-executing] treaty, which becomes judicially enforceable through the implementation of legislation. A treaty could be identified as either self executing or non-self executing by looking to various indicators, including statements that are made by Congress or the Executive regarding the treaty, indeterminate language of the treaty, or if the treaty deals with a matter within the exclusive law-making power of Congress, indicating that Congress must create implementing legislation." LEGAL INFO. INST., *Self Executing Treaty*, CORNELL L. SCH.,

data, Congress could enact federal legislation to meet the requirements of the treaty, and the statutes may be subject to the same standards as used in the *Bond* case. The Court in *Bond* stated that, absent clear intention by Congress, federal legislation should be interpreted to uphold the federalism balance between the nation and the states (although it should be noted that this was the standard applied to a criminal statute, not a civil regulation).[170] Under a standard that provides deference to Congress's intentions to uphold a balance of federalism, a comprehensive act regulating personal data may pass judicial muster as aiming at regulating interstate communications, which is within the enumerated powers of Congress under the Commerce Clause, as discussed previously,[171] and may be interpreted to be regulating activity within the stream of commerce and therefore, be constitutional.[172] Although such a treaty and accompanying regulation may not reach purely-local activity, it may be a more practical way to regulate data because it would require an act of the President and Senate, instead of requiring that both houses of Congress pass the regulation.

Another effective alternative would be for the United States common law writ of habeas corpus to be judicially interpreted and expanded to not only cover a physical detention, but a virtual detention as well (detention and use of personal data), essentially creating a common law writ of habeas data. The common law writ of habeas corpus in the United States is already used to force government officials to provide valid reasons for noncriminal detentions.[173] Such detentions include pretrial detention, pre-conviction detentions,[174] indeterminate detention (such as detainees in Guantanamo Bay who have not been charged with a crime),[175] and isolation and quarantine detention.[176] In this current era of vast technological growth and transmission of personal data, in some respect, it may not seem a far deviation from the purpose of common law habeas corpus for a court to find the seizure and misuse of personal data akin to the seizure of a person's physical body. Although it is unlikely that the judiciary would stray from the historical roots of the writ of habeas corpus, which dates back to the Magna Carta,[177] and expand it to cover virtual seizures, judicial interpretation would be the most appropriate method for incorporating a writ of habeas data into American jurisprudence.

Notwithstanding all the legal and social resistance, a comprehensive act or judicially created writ might face before it would even get out of the starting gate,[178]

---

https://www.law.cornell.edu/wex/self_executing_treaty [https://perma.cc/RZ7C-73WR].

170. *Bond*, 134 S. Ct. at 2083.

171. *See, e.g.*, 18 U.S.C. § 2510 (regulating the interception of interstate electronic communications).

172. *See supra* notes 168–70 and accompanying text.

173. *See The Freedom Writ*, *supra* note 15.

174. *See, e.g.*, Schall v. Martin, 467 U.S. 253 (1984).

175. *See, e.g.*, Rasul v. Bush, 542 U.S. 466 (2004).

176. *See, e.g.*, Hickox v. Christie, 205 F. Supp. 3d 579 (D.N.J. 2016).

177. *See* Hoffmann, *supra* note 17, at 183; Ogolla, *supra* note 18.

178. The Supreme Court might expect public or legal backlash if it steps too far out of its "case and controversy" stronghold. *See* Chris Schmidt, *The Forgotten Backlash Against the Warren Court*, ISCOTUSNOW BLOG (Dec. 30, 2014), http://blogs.kentlaw.iit.edu/iscotus/forgotten-backlash-warren-court/ [https://perma.cc/PS9X-PGUE] (discussing backlash that

Congress could take less drastic steps to fall in line with the data protections being offered internationally. These changes could be implemented and incorporated within the United States' sectoral, topical, and ad hoc legislation on personal data protection. The right to access, erasure, and restriction of processing of personal data could be highly advantageous to work into certain, or all, topical data protection regulations, like HIPAA. Amending federal HIPAA to include the right to access, as found in the GDPR, and allowing citizens to file actions to retrieve personal health information, along with information on how it is being used or shared would allow citizens to feel more safe, informed, and in control of their personal data.[179] This type of amendment to the Act could be modeled after the current Freedom of Information Act legislation because it would follow similar guidelines and requirements for requesting government information.[180]

Similarly, Congress could amend certain legislative acts, specifically HIPAA, to include a right to erasure—on a smaller and less intrusive scale than is currently employed by the EU—when the personal health care information is subject to a contract between the data subject and the data controller, allowing for the deletion of voluntarily submitted data according to the contract.[181] Contracts are not subject to the same stringent freedom of expression and freedom of speech rules, and this would put less onus on courts to weigh the competing interests of privacy and First Amendment freedoms, among other factors.[182] However, the social resistance would be greater under this type of amendment because it is unlikely that a corporation, or even a large government entity, will want to enter into contracts that may require them, at a later date, to voluntarily give up collected data.

Another way Congress could include the right to erasure in data protection regulation like HIPAA would be to amend the current act to include a private right of erasure only on the occasions when the personal data has been used or processed unlawfully. This would not run afoul of the First Amendment because unlawful actions—in these cases, the unlawful processing of health care data (based on a

---

the Supreme Court has faced for "judicial law making" in the past from the public); Alison Siegler, *Rebellion: The Courts of Appeals' Latest Anti*-Booker *Backlash*, 82 THE UNIV. OF CHI. L. REV. 201 (2015), https://lawreview.uchicago.edu/publication/rebellion-courts-appeals%E2%80%99-latest-anti-booker-backlash-0 [https://perma.cc/58JB-KLPE] (discussing the backlash the Supreme Court suffered from the federal courts of appeals after deeming the federal sentencing guidelines "mandatory.").

179. This would not bring about certain First Amendment concern because such an amendment would simply allows access, not censorship in any way.

180. The Freedom of Information Act (FOIA) allows private citizens to request information from the government. *See* 5 U.S.C. § 552. A FOIA request can be made for any agency report, with some exception. The only requirement is that the request must be in writing and reasonably describe the records you seek. U.S. Dep't of Justice, *How Do I Make a FOIA Request?*, FOIA.GOV, https://www.foia.gov/how-to.html [https://perma.cc/2FHS-KSZE]. FOIA requests can be agency specific and should be drafted according to each agency's requirements. There is no need, or requirement, to include in a FOIA request why the information is being sought. There is often a fee that accompanies FOIA requests. PUB. CITIZEN, *How to File a FOIA Request: A Guide*, https://www.citizen.org/our-work/litigation/litigation-how-file-foia-request [https://perma.cc/WQA3-FE2P].

181. Walker, *supra* note 160, at 278–84.

182. *Id.*

statute or regulation)—are not protected by constitutional rights.[183] The unlawful sharing of our plaintiff's health information could not be considered a form of freedom of expression or speech, just like defamatory statements.[184] Although this type of amendment would be shallower than the right to erasure that is offered under the GDPR, it would be an initial step for Congress to introduce private rights of action without enacting a comprehensive legislative scheme.

CONCLUSION

Although a truly comprehensive data protection scheme or a judicially enacted writ of habeas data for the United States may be just a glimmer of hope for the future, that does not mean that the United States must remain stagnant in the evolution of personal data protection. Small changes can be made over time to bring the United States' ad hoc approach to data protection in line with the global trend of allowing citizens' private rights of action for misuse of their personal data, while in turn holding entities responsible for their use, storage, and dissemination of data. While these changes do not seem likely to occur very rapidly, they may need to. With the enforcement date of the GDPR in the rearview mirror, the United States and its entities and corporations could face hefty penalties for not meeting the minimum protections standards with regards to personal data obtained from citizens of the EU's Member States.[185] In light of the global climate calling for more protection, a fundamental question remains: do you know what is being done with your personal data?

---

183. *See, e.g.*, United States v. Alvarez, 132 S. Ct. 709, 720–22 (2012) (discussing why criminal perjury is not protected by the First Amendment); Posner v. Lewis, 965 N.E.2d 949, 953 (N.Y. 2012) (discussing why blackmail is not constitutionally protected speech).

184. *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) (discussing the appropriate constitutional protection for defamation claims).

185. *See* Steven C. Bennet, *Is America Ready for the Right To Be Forgotten*?, 88 N.Y. ST. B. ASS'N J. 11 (2016).