PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 2019 | Issue 1 Article 3

5-30-2020

The First Amendment and Data Privacy: Securing Data Privacy Laws That Withstand Constitutional Muster

Kathryn Peyton

The First Amendment and Data Privacy: Securing Data Privacy Laws That Withstand Constitutional Muster

Kathryn Peyton*

Abstract

Given the growing ubiquity of digital technology's presence in people's lives today, it is becoming increasingly more necessary to secure data privacy protections. People interact with technology constantly, ranging from when engaging in business activates, such as corresponding through emails or doing research online, to more innocuous activities like driving, shopping, or talking with friends and family. The advances in technology have made possible the creation of digital trails whenever someone interacts with such technology. Companies aggregate data from data trails and use predictive analytics to create detailed profiles about citizen-consumers. This information is typically used for profit generating purposes. The way Big Data is being used threatens individuals' autonomy because users of Big Data are becoming increasingly more successful in shifting citizen-consumer's behaviors to meet the guider's objectives.

This Article discusses the difficulty in enacting laws that protect individuals' data information, as such laws potentially come into conflict with the First Amendment's right to free speech. This Article proceeds to analyze whether data is speech and concludes that it is likely speech. Thus, regulating data information raises First

* Tax LL.M. candidate at the University of California, Irvine School of Law, Graduate Tax Program. I would like to thank my family and Charles Hitchcock for their unconditional love and support.

Amendment concerns. Regulating data is in essence regulating people's ability to obtain information. By preventing dissemination of information, freedom of speech has very little value because people don't have the information they otherwise would have obtained. Consequently, individuals cannot speak about such information they don't have, and this thus diminishes speech. Despite finding data likely constitutes speech, and thus regulating data poses free speech concerns, this Article argues that securing data privacy is necessary to safeguard the same objectives freedom of speech protects. Data privacy is necessary to protect the creation of new ideas and differing opinions because people may self-censor their behavior if such behavior is completely exposed to the public. To ensure the continuance of a citizenry that critically engages in society, data privacy is necessary, not just freedom of speech.

In striking the balance between securing data privacy, while still affording a level of freedom of speech that promotes democratic ideals, this Article contends data privacy regulations should be analyzed under the commercial speech doctrine, and thus subject to intermediate scrutiny. Next, this Article argues that the Court should uphold data privacy regulations as meeting the requirement of being no more restrictive than necessary so long as they pertain to the protections common in codes of fair information practices. These protections directly safeguard (1) the use of the data, ensuring use is consistent with the purpose of why the data was originally collected; (2) individuals' right to notice and participate in how their data is being used; (3) extra protections for sensitive data pertaining to race, sexual orientation, political views, and religion; and lastly, (4) a system for enforcement, including available remedies for individuals who have been wronged. The Court should uphold data privacy regulations embodying these protects because they advance the government's substantial interest in preserving autonomy amongst individuals in order to protect self-governance. Further, such regulations directly are narrowly tailored because they regulate the concerns of data privacy that threaten individuals' ability for self-determination.

TABLE OF CONTENTS

I. INTRODUCTION

Over a century after Warren and Brandeis emphasized the importance of privacy in their iconic article *The Right to Privacy*—in which they argued that people have a "right to be let alone"—privacy remains a fundamental concern in our society.[1] It is becoming increasingly important to establish protections to safeguard this right, given the ubiquitous and invasive nature of advanced technology.[2] Today, technology is present in all aspects of people's lives, ranging from its use for business-related tasks to more innocuous behaviors such as watching television, talking with friends and family over the phone, online shopping, and even driving.[3] As such, it is increasingly more difficult to avoid using computerized technology when engaging in society. It almost as if people do not have a choice other than to opt into these modes of engagement to be a productive member of our technology-driven world.

Advances in technology have made developments such as Big Data[4] possible. Every time an individual interacts with technology, a data trail is being generated.[5] This occurs, for example, when using an application on one's phone or wearing a health-monitoring watch.[6] Each digital trail of information generated is combined with other data sources to produce Big Data.[7] Businesses and organizations analyze Big Data in order to discover patterns about individuals, thus resulting in predictive analytics[8] used to create detailed individual profiles.[9] These results are then used by businesses to make

1. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

2. This article uses the word "technology" to refer to digital technology, which is defined as "electronic equipment and applications that use information in the form of numeric code. This information is usually in binary code." Jayden Harmon, *What are Digital Technologies?*, QUORA (Apr. 27, 2018), https://www.quora.com/What-are-digital-technologies.

3. *See* Ronald Van Loon, *What is Big Data And How Does It Work?*, DATA SCI. CTR. (Dec. 12, 2017), https://www.datasciencecentral.com/profiles/blogs/what-is-big-data-and-how-does-it-work.

4. "Big Data" is a generalized and imprecise term but can be used to refer to "the use of large data sets in data science and predictive analytics." Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014).

5. *See* Van Loon, *supra* note 3.

6. *Id.*

7. *Id.*

8. "Predictive analytics" is defined as "the practice of extracting information from existing data sets in order to determine patterns and predict future outcomes and trends." Vangi Beal, *Predictive Analytics*, WEBOPEDIA, https://www.webopedia.com/TERM/P/predictive_analytics.html (last visited Jan. 17, 2020).

9. Van Loon, *supra* note 3; Crawford & Schultz, *supra* note 4, at 93.

marketing decisions which can impact individuals' experiences with the world around them.[10] The detailed profiles generated do not always produce optimal results, however, as the profiles can create an inaccurate picture.[11] This can cause businesses utilizing Big Data to make misguided decisions because they rely so heavily on such data, believing it produces results with greater truth, accuracy, and objectivity.[12]

Whether or not predictive analytics produce accurate results, Big Data practices still violate general privacy concerns. The implementation of these practices infringes on what privacy theorists describe as the right of "control over personal information."[13] An example of this type of privacy violation is the infamous incident in which the retail chain Target used Big Data to predict which of its female customers were pregnant by looking at customers' purchase histories.[14] For instance, if a customer bought items such as unscented lotions, scent-free soap, sanitizers, washcloths, or calcium supplements, Target would assign her a high pregnancy prediction score and would thereby increase the amount of advertising directed at her for baby-related goods.[15] In one case, a teenage girl's father found out that his daughter was pregnant before she was able to tell him because Target persistently sent advertisements for baby items to the family's home.[16] Such disclosures are problematic because they rob individuals of their autonomy in controlling information relating to intimate details about their personal lives.

The role that technology plays in almost all aspects of human interactions and the resulting ubiquity of Big Data brings to light a concern for information

10. Van Loon, *supra* note 3.

11. For example, relying on Big Data generated by its search results, Google drastically overestimated peak flu levels compared to the Centers for Disease Control and Prevention's ("CDC") estimate. Declan Butler, *When Google got flu wrong*, NATURE (Feb. 13, 2013), https://www.nature.com/news/when-google-got-flu-wrong-1.12413. The CDC's estimates were based off of doctors reporting patients' complaints, whereas Google relied on predicting who had the flu based off of individuals' flu-related search results. *Id.* Google's overestimation can be attributed to more people searching for flu symptoms that year, despite being sick, because of the widespread media coverage of severe cases. *Id.*

12. *See* Crawford & Schultz, *supra* note 4.

13. Scholar Alan Westin describes privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated." DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 24 (2008).

14. Kashmir Hill, *How Target Figured Out How A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#129f5aff6668.

15. *Id.*

16. *Id.*

privacy. To address privacy concerns and protect the right to be let alone, data privacy laws must be enacted that will withstand constitutional muster by not violating the First Amendment.[17] This Article argues that data information privacy laws should be analyzed under the Commercial Speech Doctrine.[18] Further, in setting the parameters of what regulations withstand intermediate scrutiny, this Article suggests that the Supreme Court should recognize laws which put into place the protections common in codes of fair information practices. The recommended protections would be narrowly tailored, pertaining to safeguarding (1) the use of the data (i.e., ensuring use is consistent with the purpose of why the data was originally collected);[19] (2) individuals' right to notice and participate in how their data is being used;[20] (3) extra protections for sensitive data pertaining to race, sexual orientation, political views, and religion;[21] and lastly, (4) a system for enforcement, including available remedies for individuals who have been wronged.[22] Laws embodying these protections should withstand intermediate scrutiny under the Commercial Speech Doctrine because they directly regulate the federal government's concerns.

This Article proceeds in three Parts. Part II discusses whether data is speech, and if so, whether laws regulating information privacy would be subject to free speech concerns. Part III discusses the role of the First Amendment in the protection of data information and privacy, concluding that there must be a balance between protecting free speech and privacy, because both are necessary for traditional American ideals of the Founding Fathers to exist. Part IV poses a possible solution to securing information privacy laws that withstand constitutional muster by maintaining First Amendment protections while honoring the Commercial Speech Doctrine. Part IV concludes the Article by proposing a plan for the solution's implementation.

17. U.S. Const. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").

18. *See generally* James B. Franks, *The Commercial Speech Doctrine and the First Amendment*, 12 TULSA L. J. 699, 699–700 (2013) (explaining that commercial speech, in other words, speech that includes commercial information, such as advertisements, is protectable by the First Amendment).

19. Joel R. Reidenberg, *Setting Standard for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 514 (1995).

20. *Id.* at 515.

21. *Id.*

22. *Id.* at 515–16.

II. WHETHER DATA IS SPEECH

When addressing whether a law violates the First Amendment's guarantee of the right to free speech, one of the first questions that must be asked is whether the law in question is targeting speech. If the law is merely addressing conduct, then there is no First Amendment issue. To this end, there is considerable debate among privacy scholars as to whether data constitutes speech.

A. Arguments That Data is Speech

Some legal scholars, such as Eugene Volokh, take the firm view that data is speech.[23] Volokh argues that the right to control data information translates into "my right to control your communication of personally identifiable information about me."[24] This, in effect, creates "a right to have the government stop you from speaking about me."[25] Analyzing data privacy laws from this perspective makes clear that such regulations effectively are inhibiting speech. Volokh rebuts other scholars' arguments for a code of fair information practices (discussed below) by arguing the First Amendment already provides fair parameters delineating how data may be disclosed.[26] These parameters favor speech because most of the rules regulating data information collection run afoul of the First Amendment.[27] Thus, according to Volokh, these laws are not defensible.[28]

Specifically, Volokh believes that search engine results constitute speech and therefore are protected.[29] The modes of communication used by our society have changed considerably since First Amendment jurisprudence first began to develop. Volokh notes that while people once turned to newspapers, guidebooks, and encyclopedias, today, individuals go to search engines like Google for news and other sought-after information.[30] In delivering its

23. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000).
24. *Id.* at 1050.
25. *Id.* at 1051.
26. *Id.*
27. *Id.*
28. *Id.*
29. Eugene Volokh & Donald M. Falk, *Google: First Amendment Protection for Search Engine Results*, 8 J. L. ECON. & POL'Y 883, 884 (2012).
30. *Id.*

consumers news and search query results, Google selects and sorts results in a way that each individual user will find the most helpful and useful.[31] To do this, Google implements a computerized algorithm that prioritizes search results based off of metrics such as the frequency and location of keywords, how long a webpage has existed (giving greater value to pages that have a longer established history of being on the web), and the number of webpages that link to the page in question.[32] Although the traditional newspaper or print-encyclopedia did not automatically sort its information this way, Google is still similar to these predecessor information sources as individuals now turn to Google as they once did to newspapers and encyclopedias to gain information.

Agreeing with the two federal cases which held Google's search engine results are protected speech, *Search King, Inc. v. Google Technology, Inc.*[33] and *Langdon v. Google, Inc*,[34] Volokh argues that automation does not render speech unprotected.[35] He explains that algorithms are created by people, and in the context of search engines, ranking algorithms can be likened to editorial judgments.[36] Thus, the search engine speech belongs to the corporation, just as the speech of what employees of a corporate newspaper create or select belongs to the newspaper corporation.[37] Secondly, Volokh explains that First Amendment protection not only focuses on a speaker's rights, but also protects the rights of listeners and readers.[38] Automation is necessary in providing users with "free, convenient, quick, and comprehensive access" and consequently only increases the value of speech to the user.[39]

Volokh's search engine analysis can also apply to Big Data and data information generally. Similar to search engine rankings, Big Data can likewise

31. *Id.*

32. *Id.*; Jonathan Strickland, *How Google Works*, HOWSTUFFWORKS (Dec. 20, 2006), https://computer.howstuffworks.com/internet/basics/google1.htm.

33. The district court held that Google was protected from liability for tortious interference with a contractual relationship for allegedly lowering Search King's ranking on Google's search engine, because Google's search ranking constitutes protected speech. *See* Search King, Inc. v. Google Tech., Inc., No. 02-1457, 2003 WL 21464568, at *4 (W.D. Okla. May 27, 2003).

34. The district court held that Google has the First Amendment right to not post certain website ads, likening Googles decision to an editorial judgment. Langdon v. Google, Inc., 474 F. Supp. 2d 622, 622 (D. Del. 2007).

35. *See* Volokh & Falk, *supra* note 29, at 886, 888.

36. *Id.* at 888–89.

37. *Id.* at 889.

38. *Id.*

39. *Id.* at 888–89.

constitute speech because humans create the algorithms for data-mining software, just as humans created Google's ranking algorithm. Further, the knowledge provided to users of Big Data is as useful as the information the ranked search results provide to users of search engines. Individuals who search on a search engine access an abundance of information that may, in effect, change their perspective and inform their decisions. Big Data also informs the actions of those individuals analyzing it.[40] Big Data gives users access to information detailing patterns about individuals, enabling users to make their decisions based off of such behaviors.

Companies, rather than individuals, are typically the entities that implement algorithms to track and sort data, and they use that data to create reports predicting users' behavior, oftentimes for marketing purposes.[41] This benefits the company because their tailored individualized approach to marketing can increase profits.

The right to create knowledge is another theory that supports the proposition that data information is speech.[42] Professor Jane Bambauer argues that data must be speech because two of the latent prerequisites to free speech are free thought and information flow.[43] Like Volokh, Professor Bambauer points out that the First Amendment has been interpreted to protect the person receiving the message, and not just the speaker.[44] The logic behind this is that if the government could regulate thoughts by restricting access to information, free speech would have very little value.[45]

Professor Bambauer also analyzes the protection of data as speech as being consistent with the marketplace of ideas.[46] The marketplace of ideas is a theory that justifies the protection of free speech through the notion that there should be an open marketplace for the exchange of ideas, where bad ideas eventually lose out to good ones.[47] This "marketplace of ideas" promotes the

40. *See* Jeff Desjardins, *Here's What the Big Tech Companies Know About You*, VISUAL CAPITALIST (Nov. 19, 2018), https://www.visualcapitalist.com/heres-what-the-big-tech-companies-know-about-you/.

41. *See* Richard Wheaton, *Why retailers need to embrace cloud computing for growing sales*, THE DRUM (July 29, 2019, 10:00 AM), https://www.thedrum.com/opinion/2019/07/29/why-retailers-need-embrace-cloud-computing-growing-sales.

42. Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 86–87 (2014).

43. *Id.* at 86.

44. *Id.* at 87.

45. *Id.*

46. *Id.* at 91–96.

47. *Id.* at 92.

free competition of the minds of Americans.[48]

Professor Bambauer argues that data has the power to change minds and thus belongs in the marketplace.[49] For example, she explains that this type of data changed beliefs about the cause of ulcers.[50] Historically, it was believed that stress caused ulcers.[51] Some courts even accepted evidence that a plaintiff suffered from an ulcer as proof of a physical manifestation of stress as required to win damages in intentional infliction of emotional distress claim.[52] However, this belief was dismantled when scientists discovered a type of bacterium common to all who suffered from ulcers that could survive in stomach acid.[53] When patients were treated with antibiotics for their ulcers, rather than simply resting, the patients were cured 900% more often.[54] Ultimately, access to data information in the marketplace of ideas is what led to changing the belief that stress causes ulcers, and access to this information can further lead to other beneficial discoveries.

B. Arguments That Data is Not Speech

Unlike Professor Bambauer, Professor Neil Richards instead argues that distinctions should be drawn between speech and information flows.[55] He suggests that data privacy and the First Amendment can be reconciled because most laws regulating data are regulating *conduct*, not speech.[56] Professor Richards states that regulations for the use, collection, and disclosure of personal data are often introduced as a code of fair information practices.[57] One of the first enacted codes of fair information practices, The Privacy Act of 1974,[58] was passed to regulate federal agencies and has been influential in

48. *Id.*
49. *Id.* at 93.
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*
55. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1166 (2005).
56. *Id.*
57. *Id.*
58. The Privacy Act of 1974 prohibits federal agencies from disclosing personal information retrieved from federal systems of records without the written consent of the individual the information pertains to, unless the disclosure is pursuant to one of the twelve statutory exceptions. *See* U.S. DEP'T OF JUSTICE, *Privacy Act of 1974*, https://www.justice.gov/opcl/privacy-act-1974 (last visited Jan. 17,

providing a framework to pass additional state and federal laws regulating the private sector.[59] There is a general consensus among scholars that these codes typically guarantee four protections against the misuse of data.[60]

The first protection that the codes of fair information practices ensure is the implementation of standards for data quality, which requires data to be collected lawfully and used for specific purposes.[61] The data collector must use the data only for purposes compatible with the original intent of collecting the data, which restrains inappropriate secondary uses.[62]

Second, these codes provide standards for the transparency of information processing.[63] The core element of this standard is to have the individual participate in the treatment of their personal information.[64] In sum, information processing must be transparent to all citizens.[65]

Third, the codes create special protections for sensitive data.[66] Such data that warrants extra scrutiny by citizens includes information relating to race, religion, health, or political beliefs.[67]

Finally, these codes also address the enforcement of fair information practices.[68] For the regulations to work, there must first be supervision and oversight of the treatment of individuals' information.[69] Additionally, there must be remedies for those who have been wronged.[70]

Professor Richards adopts Professor Paul Schwartz's view that a majority of regulations in a code of fair information practices actually govern conduct and do not target speech.[71] Professor Schwartz argues that out of the four protections provided by a code of fair information practices, the first, second, and fourth protections do not implicate speech at all.[72] Rather, those

---

2020).

59. Richards, *supra* note 55, at 1166–67.
60. *Id.* at 1167.
61. Reidenberg, *supra* note 19, at 514.
62. *Id.*
63. *Id.* at 515.
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.* at 515–16.
69. *Id.* at 515.
70. *Id.*
71. Richards, *supra* note 55, at 1168; Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1561–62 (2000).
72. *Id.*

provisions merely regulate business practices or conduct.[73]

Professor Schwartz does acknowledge, however, that the third protection—preventing the disclosure of sensitive data—does burden free speech.[74] He admits that this subset does fit into Volokh's view of "information privacy as the right to stop people from talking about you."[75] Consequently, preventing the disclosure of sensitive data likely violates the First Amendment. However, Professor Richards and Professor Schwartz would argue that although regulations of the disclosure of sensitive data may burden speech, most of these regulations address conduct and thus do not pose free speech concerns. Therefore, they would justify most of these regulations in a code of fair information practices.

Presenting an alternative view, Professor Tim Wu argues that data produced by computers is not speech and that the First Amendment is only intended to protect humans.[76] He rejects the court's decision in *Search King, Inc. v. Google Technology, Inc.*, as he disagrees that Google's rankings of search results, which are derived from algorithms, constitute speech.[77] He refutes the analogy posed by Volokh, likening Google's algorithms to an editor of a newspaper, by stating: "Socrates was a man who died for his views; computer programs are utilitarian instruments meant to serve us."[78]

Professor Wu urges that the First Amendment's intended purpose was to protect *humans* against the evils of state censorship, not to protect commercial automation from regulation.[79] Again, Professor Wu uses an analogy in refuting the notion that algorithms are speech because they were programmed by people with First Amendment rights.[80] He equates giving algorithms constitutional rights to Dr. Frankenstein's monster having the right to vote, just because he is able to walk and talk.[81] Professor Wu therefore urges against computers being able to inherit constitutional rights.[82]

---

73. *Id.*
74. *Id.*
75. *Id.* at 1562.
76. Tim Wu, *Free Speech for Computers?*, N.Y. TIMES (June 19, 2012), https://www.nytimes.com/2012/06/20/opinion/free-speech-for-computers.html.
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*

C. Data is Likely Speech

Scholars on both sides of the issue have posed convincing arguments as to why data is or is not speech. Volokh and Bambauer argue that the First Amendment protects not only the speaker's rights, but also the rights of the person receiving the information.[83] If there are laws curtailing the gathering of information, this harms the would-be user of the information because it prevents him or her from ever gaining that knowledge.

However, Richards, pointing to other scholars' work, argues data information laws regulate conduct and not the dissemination of speech.[84] Further, Wu argues the First Amendment is meant to protect people, not commercial automation.[85] The key in finding which of these principles should be adopted is to discern how far before the actual utterance of speech should be protected in order to safeguard free speech rights.

As Bambauer points out, allowing the free flow of information is consistent with most of the theories behind why the First Amendment exists.[86] From a marketplace of ideas perspective, not restricting data information collection is in line with the search for truth.[87] Individuals must be able to receive information in order to engage with others in search of the best ideas. Further, the right to receive data information corresponds with the notion that free speech serves to protect democratic participation, particularly dissident opinions.[88] Having the right to access information protects the critical thinking necessary for self-governance.

The Court has also recognized protection must be afforded to not just speech, but what comes before speech. Justice Brandeis, an advocate for privacy, even supported the notion that knowledge is essential to free speech, stating, "[t]hose who won our independence believed . . . that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth."[89] In sum, being able to receive information presupposes knowledge and being knowledgeable is a prerequisite to speech.

In *Branzburg v. Hayes*, although the Court did not grant the press

83. *See* Volokh & Falk, *supra* note 29, at 889; Bambauer, *supra* note 42, at 87.
84. Richards, *supra* note 55.
85. Wu, *supra* note 76.
86. Bambauer, *supra* note 42, at 91–106.
87. *See* Frederick Schauer, *Must Speech be Special?*, 78 NW. U. L. REV. 1284, 1285 (1983).
88. Bambauer, *supra* note 42, at 97.
89. *Id.* at 97-98; Whitney v. California, 274 U.S. 357, 375 (1927).

immunity from being compelled to testify and reveal confidential news sources, the Court still acknowledged journalists are afforded extra protections in order to safeguard the free flow of information.[90] In pertinent part, the Court stated, "[w]e do not . . . [suggest] that news gathering does not qualify for First Amendment protection; without some protection for seeking out the news, freedom of the press could be eviscerated."[91] This statement can be analogized to the idea that without the right to receive information, freedom of speech could be eviscerated.

Given the Court's history with securing rights necessary for speech, it is likely that data information constitutes speech. The Court affirmed this belief in *Sorrell v. IMS Health Inc.*, by rejecting the argument that a law prohibiting the sale of medical information, revealing the prescriptions doctors have prescribed patients, did not regulate speech but simply access to information.[92] The Court reasoned, based on a long history of precedent, that "[a]n individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way in which the information might be used' or disseminated."[93]

Going forward, the Court will likely follow its precedent and treat data information as speech. However, like in *Branzburg* where the Court did not afford the press unlimited privileges in the name of preserving free speech, the Court should strike a balance and not allow the unfettered disclosure of data information. Such unregulated information disclosures can certainly curtail democratic objectives.

III. INFORMATION PRIVACY IS CENTRAL TO DEMOCRATIC IDEALS

Looking at the history behind why the Founding Fathers secured the right to free speech is illuminating on the topic of information privacy. Free speech was, and still is, meant to protect the democratic process of self-governance. However, some level of privacy is necessary to preserve a self-governing society. Although finding the balance can be difficult, it is necessary.

90. Bambauer, *supra* note 42 at 85; Branzburg v. Hayes, 408 U.S. 665, 681 (1972).
91. *Id.*
92. 564 U.S. 552, 557, 567 (2011).
93. *Id.* at 568.

A. Historical Purpose of the First Amendment

The First Amendment was adopted to protect the individual liberty of citizens and create a democracy where such individuals directly participate in governmental affairs by directly voting on issues and electing representative officials.[94] On December 19, 1791, only four days after the Bill of Rights was ratified,[95] James Madison stated in the *National Gazette*[96] that, "[p]ublic opinion sets bounds to every government, and is the real sovereign in every free one."[97] Madison's ultimate view was that a free country ultimately depends on open public opinion.[98] He believed that those who tried to suppress opinions through restrictions on speech were opponents of democracy.[99]

The notion that a democratic society should guard free speech in order to allow differing opinions for the purpose of protecting liberty stems back to the Enlightenment period.[100] Since antiquity, laws have existed that prohibited expressing or even believing in differing views or opinions.[101] For example, many conflicting social and political opinions were outlawed because either the church or the state viewed them as dangerous or false.[102]

By 1275, legislation prohibiting the freedom of speech existed in England.[103] Laws against seditious libel were also enacted, which prohibited criticism of the government.[104] Further, there existed laws against blasphemous

94. *See* Robert A. Sedler, *The "Law of the First Amendment" Revisited*, 58 WAYNE L. REV. 1003, 1022–28 (2013).

95. *Today in History – December 15: The Bill of Rights*, LIBR. OF CONG., https://www.loc.gov/item/today-in-history/december-15/ (last visited Jan. 17, 2020).

96. The National Gazette, based in Philadelphia, was one of the most influential newspapers in the early years of the United States. *About National Gazette*, LIBR. OF CONG., https://chroniclingamerica.loc.gov/lccn/sn83025887/ (last visited Jan. 17, 2020).

97. *For the National Gazette*, FOUNDERS ONLINE, https://founders.archives.gov/documents/Madison/01-14-02-0145 (last visited Jan. 17, 2020).

98. Jay Cost, *James Madison's Lesson on Free Speech*, NAT'L REV. (Sept. 4, 2017), https://www.nationalreview.com/2017/09/james-madison-free-speech-rights-must-be-absolute-nearly/.

99. *Id.*

100. *See* Steven D. Smith, *Recovering (From) Enlightenment?*, 41 SAN DIEGO L. REV. 1263, 1273–74 (2004).

101. Jeremy J. Ofseyer, *Taking Liberties with John Stuart Mill*, 1999 ANN. SURV. AM. L. 395, 397–98 (1999).

102. *Id.*

103. John Simkin, *The History of Freedom Speech in the UK*, SPARTACUS EDUC. (Sept. 25, 2018), https://spartacus-educational.com/spartacus-blogURL116.htm.

104. *Id.*

libel, prohibiting criticism of religion.[105] Less than a century later, the 1351 Treason Act was codified, making it a crime to "compass or imagine" the death of the king.[106] All these laws aimed to suppress opinions that differed from the political or religious entity in power.

Political philosophers who sparked the Enlightenment, including John Locke, opposed the suppression and intolerance of differing opinions.[107] Locke and the Enlightenment teachings influenced the Founding Fathers to establish the Declaration of Independence and the Bill of Rights.[108] In addition to the Founding Fathers, John Stuart Mill was also heavily influenced by the teachings of Enlightenment-era philosophers. Mill was inspired by John Milton's theory of the "marketplace of ideas" published in *Areopagitica* in 1644.[109] In his book *On Liberty*, Mill expanded on Milton's idea, explaining that every individual has the ability to critically evaluate opinions, and having disfavored opinions helps in the search of the truth because they encourage the introduction of newer perspectives to into society.[110]

Mill's own theoretical philosophies would ultimately influence Supreme Court's First Amendment jurisprudence.[111] Justice Holmes' famous dissent in *Abrams v. United States* introduced the marketplace of ideas theory into the Court's analytic framework, emphasizing the Constitution's protections of the free trade of ideas.[112] Holmes stated, "the best test of truth is the power of the thought to get itself accepted in the competition of the market."[113]

The marketplace of ideas has become an influential theory of the rationale behind the First Amendment. It is clear that the Enlightenment teachings advocating the dissemination of differing opinions influenced the Constitution, namely the Bill of Rights, and the Supreme Court's approach to analyzing free speech issues.

105. *Id.*

106. Aisha Gani, *Treason Act: the facts*, THE GUARDIAN (Oct. 17, 2014), https://www.theguardian.com/law/2014/oct/17/treason-act-facts-british-extremists-iraq-syria-isis.

107. Ofseyer, *supra* note 101, at 398.

108. Robb A. McDaniel, *John Locke*, FIRST AMEND. ENCYCLOPEDIA, https://www.mtsu.edu/first-amendment/article/1257/john-locke (last visited Jan. 17, 2020).

109. Daniel E. Ho & Frederick Schauer, *Testing the Marketplace of Ideas*, 90 N.Y.U. L. Rev. 1160, 1168 (2015).

110. *Id.*

111. Ofseyer, *supra* note 101, at 395.

112. Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

113. *Id.* (Holmes, J., dissenting).

B. Granting Some Protection to Data Privacy is Necessary for the Democratic Process

Given the history behind the rationale of free speech—beginning with the philosophers of the Enlightenment, then followed by Founding Fathers and early Supreme Court jurisprudence—it is clear that the First Amendment at its core is supposed to protect differing opinions. By protecting differing opinions and introducing all ideas into the open market, individuals are able to more critically engage in society. Ideas are introduced and fleshed out through rational discussion. Further, having an intelligent and participatory citizenry is necessary for the self-governance that the Founding Fathers envisioned. For a government "by the people for the people" to operate effectively, its populace must be able to engage freely in discussion and express unpopular opinions, prompting the free exchange in ideas, so that eventually the truth or the best idea prevails.

The same rationale that justifies free speech—to allow the citizenry to cultivate thoughts and disseminate differing opinions for the search of good ideas to strengthen their democracy—also justifies a level of privacy that must be afforded to all people. Big Data poses a heightened threat to privacy because almost every action a person engages in is documented through the creation of data trails.[114]

Professor Bambauer, who argues that data is speech, addresses the concerns regarding the inherent tension that on the one hand, data allows individuals to access information and become better informed, but on the other hand, if everything is on display, people may not engage in certain activities.[115] Self-censorship may take place, which can have the same detrimental effect as prohibiting speech. Individuals may not engage in certain activities that they otherwise would have if their data was not being tracked and used. As a result of not engaging in certain ventures, individuals, consequently, will not critically wrestle with the knowledge they would have gained. Thus, individuals will not have the opportunity to contribute their would-be new and enlightened ideas to the marketplace.

To put this idea into more concrete terms, let's say an individual, Abby,

114. *See* Tim Henderson, *States battle big tech over data privacy laws*, GCN (July 31, 2019), https://gcn.com/articles/2019/07/31/state-privacy-laws.aspx.

115. Bambauer, *supra* note 42, at 101.

wants to learn more about terrorism and wants to conduct online research as to how the Islamic State in Iraq and Syria ("ISIS") uses propaganda to recruit members.[116] However, Abby is afraid of how her search data will be used by third parties and is worried she may get flagged by The U.S. Department of Homeland Security for suspicious activity.[117] She does not want to deal with the consequences of investigators searching through all her personal data or a potential police visit to her home.

Consequently, Abby does not want to go to direct sites where ISIS propaganda is disseminated. She instead restricts her inquiry of ISIS's propaganda to secondary sources that she considers safe and not directly connected to ISIS, such as the New York Times and Washington Post websites.

If Abby had visited the sites that ISIS uses directly to disseminate its messages, she would have been able to gain insightful information firsthand on how ISIS tries to connect with those who may be vulnerable, willing recipients to ISIS propaganda.[118] She was not able to receive this illuminating information through the secondary sites because it was dulled down and somewhat censored. If Abby had directly seen ISIS's propaganda, it may have enabled her to grapple with what she saw and read. She then could have possibly come up with counter-content to gain the attention of those visiting propaganda sites and perhaps saved lives. In this hypothetical, Abby would not have been able to come up with her meaningful counter-message if she had not seen the content first-hand.

Abby's fear of being flagged as a threat by searching suspicious content is not irrational. The U.S. government has, in recent years, engaged in "flagging" individuals as security threats for simply inquiring into certain information online.[119] In 2013, the Guardian released a story about how the Unites States National Security Agency ("NSA") used a system called XKeyscore, to search for suspicious activity through vast databases containing emails,

116. *See* Henderson, *supra* note 114.

117. *See* Ryan Browne, *ISIS may be quashed on the ground, but it's still a 'problem' online, EU security official says*, CNBC (Nov. 6, 2018, 10:30 AM), https://www.cnbc.com/2018/11/06/isis-is-still-a-problem-online-eu-security-official-julian-king.html.

118. *See* Evan Perez, *How ISIS is luring so many Americans to join its ranks*, CNN (Apr. 23, 2015), http://www.cnn.com/2015/04/22/politics/isis-recruits-american-arrests/index.html (explaining that, whereas al Qaeda relied on radicalizing those who wished to "join the fight to protect Islamic holy lands[,]" the approach of ISIS is "more secular . . . 'portraying how much better life purportedly is in the caliphate as compared to the corrupt West."').

119. *See, e.g.*, Lily Hay Newman, *Feds Monitoring Social Media Does More Harm Than Good*, WIRED (Sept. 28, 2017, 8:00 AM), https://www.wired.com/story/dhs-social-media-immigrants-green-card/.

online chats, and browsing history of millions of people.[120] In Abby's case, the NSA could have flagged specific keywords through XKeyscore to uncover Abby's ISIS-related search activity, then subsequently gained access to and searched all of her personal digital information—despite the fact that she was not a real terrorist threat.

Additionally, police may have also paid a visit to Abby's home because of her internet search history. Another Guardian article stated that a woman and her family were visited by counterterrorism police because they were flagged for suspicious activity relating to their internet searches.[121] The woman had searched online about a pressure cooker.[122] Her husband had searched about getting a backpack.[123] Together with their son's online reading habits, which entailed clicking on links about popular terrorism news stories, the family was flagged for suspicious terrorist activity.[124] Consequently, the woman stated that if she ever bought a pressure cooker, she would not do so online.[125] This illustrates that having one's private information searched or being paid a visit by investigators to one's home can prevent a person from engaging in enhancing one's knowledge, a valuable tool in a democracy.

In addition to self-censorship, another risk posed by the lack of data privacy is that data analytics will actually reduce exposure to competing ideas.[126] This decline can occur through data analytics assessing an individual's data pertaining to politics and news sources, then using the data to suggest other news sources that that individual will like based on their political viewpoint. This decreases an individual's exposure to news sources with differing perspectives and creates an "echo chamber" exposing individuals only to viewpoints that align with their own.[127]

Professor Julie Cohen has voiced her concerns about echo chambers, affirming that they do not foster political dialogue among diverse

120. Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet*,' THE GUARDIAN (July 31, 2013), https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

121. Michele Cantalano, *My family's Google searching got us a visit from counterterrorism police*, THE GUARDIAN (Aug. 1, 2013), https://www.theguardian.com/commentisfree/2013/aug/01/government-tracking-google-searches.

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. Bambauer, *supra* note 42, at 102 n.208.

127. William Saletan, *How to escape a partisan echo chamber*, SLATE (May 3, 2010), https://slate.com/news-and-politics/2010/05/how-to-escape-a-partisan-echo-chamber.html.

perspectives.[128] She explains that the purpose of Big Data is to "produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories."[129] Big Data analysts can then subtly nudge citizen-consumers via advertisements into directions that correspond with profit-maximizing goals.[130]

Professor Cohen argues that decisions made by today's citizens, with Big Data predicting their paths for them, do not "resemble the independent decisions, formed through robust and open debate, that . . . liberal democracy requires to sustain and perfect itself."[131] This Big Data infiltration of privacy has enabled commercial and government actors to render individuals as fixed, transparent, and predictable.[132] Without some privacy, individuals become predictable and can be more easily guided in the direction commercial or government actors want, and the First Amendments policy objectives will be rendered useless. This diminishes critical thinking among individual citizens, the emergence of differing ideas, and, ultimately, threatens the form of self-governance envisioned by the Founding Fathers.

IV. A SOLUTION FOR PROTECTING DATA

A. Lack of Transparency in First Amendment Law

The First Amendment right to freedom of speech is a murky[133] area of law that seems to receive inconsistent treatment by Supreme Court Justices. Both the Court and legal scholars have acknowledged that not all speech is protected.[134] Justice Holmes notably declared in *Schenck v. U.S.* that "[t]he most

128. Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1917 (2013).
129. *Id.*
130. *Id.*
131. *Id.* at 1917–18.
132. *Id.* at 1905.
133. The word "murky" is used to refer to inconsistencies in which the Court has created case law but has seemingly reversed such law without explicitly saying so. For example, in *Chaplinsky*, which regarded the unprotected category of fighting words, the Court carved out an exception to First Amendment protection for words that "by their very utterance inflict injury or tend to incite an immediate breach of peace." Chaplinsky v. N.H., 315 U.S. 568, 572 (1942). The Court has since never upheld a conviction against a speaker for fighting words. *See* Burton Caine, *The Trouble with "Fighting Words":* Chaplinsky v. New Hampshire *Is a Threat to First Amendment Values and Should Be Overruled*, 88 MARQ. L. REV. 441, 536 (2004); *The Demise of* Chaplinsky *Fighting Words Doctrine: An Argument for Its Interment*, 106 HARV. L REV. 1129, 1129 (1993).
134. Schauer, *supra* note 877, at 1284.

stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic."[135] In his opinion in *Frohwerk*, written only a few days after the *Schenck* decision, Holmes expanded on *Schenck* by stating that the First Amendment was not "intended to give immunity for every possible use of language."[136] Despite the consensus that the First Amendment does not afford protection to all speech, there is still much confusion about its scope. The question of its scope becomes particularly difficult when freedom of speech is at odds with other generally accepted societal values.[137]

Historically, in determining the scope of First Amendment protection for freedom of speech, the Court balanced the value of speech against the social harm it caused.[138] The Court carved out categories of low-value unprotected speech by performing a balancing test that was based on intuition rather than any data or hard facts.[139] In part, through balancing, the Court created the free speech exceptions of fraud, obscenity, and true threats.[140] Further, in establishing the low-value category of fighting words, the Court applied a balancing test, reasoning such words "are of such slight social value . . . that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[141]

However, because of the administrative unpredictability that comes with an *ad hoc* balancing approach, recently the Court has shifted to a more rules-based approach in its low-value speech analysis.[142] In *United States v. Stevens*, the Court rejected the government's argument to use a balancing approach in order to uphold a law criminalizing the creation, sale, or possession of certain depictions of animal cruelty.[143] Although the Court acknowledged that the government's argument did not arise out of a vacuum—because the Court had used balancing approaches in the past—it nevertheless rejected the

135. Schenck v. U.S., 249 U.S. 47, 52 (1919) (holding speech circulated on leaflets during wartime calling for opposition to the draft as unprotected for posing a clear and present danger).

136. Frohwerk v. U.S., 249 U.S. 204, 206 (1919) (holding that a speech disseminated during World War I criticizing the U.S.'s involvement in the war was unprotected).

137. Schauer, *supra* note 87, at 1285.

138. Davis S. Han, *Transparency in First Amendment Doctrine*, 65 EMORY L.J. 359, 365 (2015).

139. *Id.* at 366.

140. *Id.*

141. Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

142. Han, *supra* note 138, at 367.

143. United States v. Stevens, 559 U.S. 460, 470–72 (2010).

government's approach.[144] The Court instead implemented the historical test in carving out unprotected categories of speech, basing its analysis on whether the categories of speech at issue have been "historically unprotected."[145] The Court reiterated that this was always the approach to recognizing a category of low-value speech, despite using a balancing analysis with other categories.[146]

Because the Court has been unclear on how to determine the scope of the First Amendment's protection, crafting a solution that will afford data information privacy is difficult. It is not evident whether the Court will at any point revert back to a more equitable balancing approach, weighing the value of the speech against the harm posed. Further, with regard to future application of the current historical test, it is unclear how far the Court will go in using historical analogies to render decisions. For example, will the Court allow for more creative, modern arguments that were likely not considered by the Founding Fathers upon the enactment of the First Amendment? Or, does the specific harm have to have existed during the founding of the United States? Because of the lack of clarity concerning how to render certain speech unprotected under the First Amendment, this Article takes the position that the most feasible approach for enacting data privacy regulations is to use the Commercial Speech Doctrine.

B. History of the Commercial Speech Doctrine

The Commercial Speech Doctrine, though firmly established, comes with its own set of issues that could lead to confusion. Like with the First Amendment, the Court has been unclear about the scope of the doctrine. When the doctrine was first introduced, the Court said that commercial speech was fully unprotected speech. However, the Court later stated that commercial speech is somewhat protected and is subject to intermediate scrutiny. Despite this lack of consistency within the Commercial Speech Doctrine, it still seems to be the best solution for data information privacy.

The Commercial Speech Doctrine originated in 1942, when the Court, in *Valentine v. Chrestensen*, held that commercial speech was an unprotected category of speech.[147] In this case, F.J. Chrestensen owned a former United

144. *Id.*
145. *Id.*
146. *Id.* at 471.
147. *Valentine v. Chrestensen*, 316 U.S. 52, 54–55 (1942), *overruled by* Payne v. Tennessee, 501

States Navy submarine which he brought to a New York City pier.[148] Chrestensen allowed the public to tour the vessel in exchange for an admission fee.[149] Chrestensen passed out a double-sided handbill on the streets, with one side advertising the vessel, but the other side protesting against the department in charge of the dock.[150] He created the double-sided handbill because he was trying to advertise his tours without violating a New York sanitary code, which prohibited distribution of commercial material in the street.[151] After Chrestensen was charged in violation of the code, he argued the code violated his First Amendment right to free speech.[152]

The Court upheld New York City's code, reasoning that the Constitution does not constrain the government from regulating purely commercial advertising.[153] The Court further explained that it would be up to legislative judgment to determine whether and to what extent someone "may promote or pursue a gainful occupation in the streets."[154] The Court's opinion did not parse out the content of Chrestensen's handbill to see how much of it was commercial speech, because Chrestensen intentionally added the other information only to try to convert his speech into non-commercial speech.[155]

However, in 1976, in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.* (*Virginia State Board*), the Court departed from its ruling that commercial speech is completely unprotected and instead found it be partially protected.[156] In *Virginia State Board*, consumers of prescription drugs brought an action to strike down a law prohibiting pharmacists from advertising the price of prescription drugs.[157] The Court held that the regulation was unconstitutional and in violation of the First Amendment.[158] The Court reasoned that commercial speech is not so far removed from the exposition of ideas so as to render it unprotected.[159] The Court then explained how

U.S. 808 (1991).
148. *Id.*
149. *Id.* at 53.
150. *Id.*
151. *Id.*
152. *Id.* at 54.
153. *Id.* at 54–55.
154. *Id.* at 54.
155. *Id.* at 55.
156. Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 748 (1976).
157. *Id.*
158. *Id.* at 773.
159. *Id.* at 762.

price information on prescription drugs may be information more useful to the receiver than "the day's most urgent political debate."[160] Prescription drugs are often very expensive and inability to compare prices harms the poor, sick, and aged.[161] Finally, the Court stressed that purely commercial speech may still be of public interest.[162]

In 1980, the Court expanded on the Commercial Speech Doctrine and set out the doctrine's current test in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York* ("*Central Hudson*").[163] There, Central Hudson challenged a law that prohibited advertising that promoted the use of electricity.[164] The Court adopted and applied a four-step test and found that the law was unconstitutional.[165] The Court laid out the test as follows:

> At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.[166]

The Court applied this analysis to the regulation in question. First, the Court determined the commercial speech fell under the protection of the First Amendment because it did not relate to unlawful activity, and it was not misleading.[167] As to the second factor, the Court determined that the government has a substantial interest in conserving energy.[168] For the third factor, the Court concluded that the state's interest was directly advanced by the regulation because advertising is directly connected to demand.[169] The Court reasoned that Central Hudson would not be fighting this ban if it did not believe

160. *Id.* at 763.
161. *Id.*
162. *Id.* at 764.
163. 447 U.S. 557 (1980).
164. *Id.* at 558–59.
165. *Id.* at 566, 572.
166. *Id.* at 566.
167. *Id.*
168. *Id.* at 568.
169. *Id.* at 569.

that advertising would increase sales.[170] However, the Court found that the regulation failed factor four.[171] Finally, in applying the fourth factor, the Court found that the government failed to prove that a more limited regulation could not serve the same interests it had in conserving power.[172]

Most recently, as mentioned in Part II, the Court's controversial decision in *Sorrell v. IMS Health Inc.* struck down a law which prohibited the sale, disclosure, or use of information about doctors' prescribing habits for marketing purposes.[173] The majority opinion analyzed the constitutionality of the law under heightened scrutiny because the regulation was content-based.[174] However, the dissent disagreed with the majority's decision to apply a higher standard.[175] Justice Breyer argued that the First Amendment does not require extra heightened scrutiny when the government's regulation burdens speech in an effort to regulate the commercial industry.[176] Breyer called the heightened scrutiny applied by the majority in commercial speech cases "unprecedented."[177] The dissent argued that the regulation should have been analyzed under intermediate scrutiny and upheld for meeting the standard.[178]

C. Regulating Data Privacy Under the Commercial Speech Doctrine

Despite the lack of transparency regarding First Amendment free speech jurisprudence, and even the commercial speech doctrine, the most feasible way to tackle the data privacy issue is with the Supreme Court's most recent four-step test.

The Supreme Court has defined commercial speech as speech that proposes a transaction.[179] The sale and use of consumer data for marketing purposes falls into the category of commercial speech. The Court has defined commercial speech as speech that proposes a transaction.[180] The data-mining

170. *Id.*
171. *Id.* 569–570.
172. *Id.* at 570.
173. Sorrell v. IMS Health Inc., 564 U.S. 552 (2011) (Kennedy, J., majority opinion).
174. *Id.* 563–64, 566 (Kennedy, J., majority opinion).
175. *Id.* at 581 (Breyer, J., dissenting).
176. *Id.* (Breyer, J., dissenting).
177. *Id.* at 590 (Breyer, J., dissenting).
178. *Id*. at 581 (Breyer, J., dissenting).
179. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y. ("*Central Hudson"*), 447 U.S. 557, 562 (1980).
180. *See, e.g.*, *id*. at 562.

industry primarily exists to sell consumer data to third parties or directly use the data it has collected for marketing purposes, ultimately, in order to enter into a transaction for the sale of consumer goods or services. In both scenarios, profits are being made based off of the data information collected from consumers.

Regulating data information collection through the Commercial Speech Doctrine may not directly address the hypothetical posed earlier where Abby self-censored herself by not visiting terrorist-affiliated websites out of fear she would be flagged. However, by addressing data information privacy in the commercial context, the widespread trails of information produced by private actors would be reduced.

Consequently, less information would be available for the government to tap into. Regulating private search engine's use and sale of consumer data information collection would not only diminish other private companies from using such information for commercial purposes, but it would also prevent the government from gaining access to use it for its own purposes.

Further, if the government wants to create its own data trails directly and use that information, the legislature can directly regulate this because such laws would be regulating the government itself. There are no First Amendment issues at play when the government regulates its own speech. Therefore, data privacy protection through applying the Commercial Speech Doctrine would prevent the government and commercial industries from having unlimited and unrestricted access to the that data citizen-consumers produce online.

Moving forward, the Supreme Court should analyze the constitutionality of data information regulations relating to marketing by applying the *Central Hudson* test. First, the Court should determine whether the commercial speech concerns lawful activity and is not misleading.[181] Assuming the speech is lawful and not misleading, it will fall within First Amendment commercial speech protection.[182]

For the second factor, the Court should recognize general privacy concerns for citizens as a substantial governmental interest.[183] As explained in parts 1-III, if there are no safeguards to online privacy and everyone is constantly exposed, democracy itself is threatened.

Regarding the third factor, the Court must address whether the law at

181. *Central Hudson*, 447 U.S. at 566.
182. *Id.*
183. *Id.*

issue directly advances the government's substantial interest.[184] If the law is prohibiting the dissemination or use of certain data information, it will directly advance the government's substantial interest in securing the privacy of U.S. citizens. Limiting the disclosure and use of data prevents would-be Big Data users from obtaining personal information about individuals that Big Data users would consequently use to make predictions about such individuals.

If U.S. citizens are going to be afforded any data information privacy, the last factor is where legislatures and the Court should take extra care. The fourth factor requires that the regulation at issue be no more extensive than is necessary to serve the government's interest.[185] To clarify this point, the Court has *not* interpreted this to require the least restrictive regulation as possible, but rather requires a rational balance between the government's end and the means chosen to achieve it.[186] This can be "a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is 'in proportion to the interest served . . . .'"[187] Thus, the Court can uphold a data information regulation even if it is not the least restrictive means possible for securing the government's interest in preserving citizens' information privacy.

In the future, legislatures and the Court should delineate what is "not more extensive than is necessary" to mean data privacy laws that directly pertain to securing the four protections common in codes of fair information practices. Regulation of data information should constitute a reasonable fit where the scope of the protection proportionate to the interest it is meant to serve. These laws will likely pass constitutional muster if such regulations pertain to protecting: (1) the use of data consistent with the reason for collecting the data;[188] (2) individuals' right to notice and the ability to participate in how their information is being used;[189] (3) sensitive data pertaining to race, sexual orientation, political views, and religion by providing more protections;[190] and (4) available remedies for individuals who have been violated pursuant to the three principles just listed.[191]

184. *Id.*
185. *Id.*
186. Bd. of Trs. of the State Univ. of N.Y. v. Fox, 492 U.S. 469, 480 (1989).
187. *Id.*
188. Reidenberg, *supra* note 19, at 515.
189. *Id.*
190. *Id.*
191. *Id.* at 515–16.

By following these principles, laws should constitute a reasonable fit—and pass the commercial speech test employed by the Supreme Court—because their scope is proportional to the substantial public interest served in protection the privacy of U.S. citizens online.

V. CONCLUSION

Given the increased role that technology plays in individuals' lives today, it is necessary for the Supreme Court to afford some level of protection towards the disclosure and use of personal data information. Today, individuals are constantly interacting with technology and are largely not afforded the option to "opt out" of these modes of engagement in professional, social, and political settings.

The ubiquity of technology creates an increasing threat to privacy and diminishes the welfare of the populace. Specifically, the objectives behind a robust First Amendment—the constant introduction and proliferation of competing ideas and a participatory citizenry that critically engages in self-governance—are threatened if privacy protections are not implemented for individuals online. People will be less informed and rendered predictable, consequently becoming pigeonholed into their foreseeable place in society.[192] Thus, it is necessary for courts in the U.S. to recognize the significant government interest in preserving privacy for the U.S. citizenry and upholding laws that reasonably advance this interest.

The most feasible way to achieve data information privacy is through the Commercial Speech Doctrine. Laws regulating data likely regulate speech, and the First Amendment has been interpreted not only to protect speech, but also the ideas that form *before* speech and, consequently, make speech possible. Therefore, data is likely speech and laws regulating data also regulate speech.[193]

A huge commercial industry exists around data mining and using Big Data to increase profits. Clearly, the commercial industry is involved because behind all the information gathered from consumer data, commercial transactions are being proposed. These transactions are either to sell the data itself or use the data directly in order to sell goods or services.

Ultimately, the government has a significant interest in preserving a level

192. Cohen, *supra* note 128.
193. *See supra* Part II.C.

of privacy amongst citizens so that the United States can continue to function through democratic self-governance. The time is ripe for the Court to view future laws enacted to secure the protections embodied in codes of fair information practices as a reasonable fit to achieving the government's ends in preserving privacy.