A New Approach to Digital Reader Privacy: State Regulations and Their Protection of Digital Book Data

ANDREW A. PROIA*

INTRODUCTION

The literary world is evolving. The thought of traveling to bookstores and libraries to get our hands on the newest novels seems like a distant memory as the Internet continues to transform the way individuals act, think, and even read. Recent developments in digitized books and electronic reading devices ("e-readers") have instantly made these formats one of the dominant ways in which society reads and purchases books today.[1] Amazon.com, for instance, reported in 2011 that it had sold more digital books than either hardback or paperback books[2]—a trend that has strengthened over time.[3] When the comic book company DC Entertainment granted the exclusive rights to some of its digital content to Amazon.com, Barnes & Noble started pulling DC's graphic novels off its shelves, stating that the company "won't stock physical books in [Barnes & Noble] stores unless [it is] offered the content in all formats."[4] Accompanying this transition are even reports that the introduction of e-readers has resulted in an increase in the overall readership habits of Americans.[5]

This revolutionary new means of literary enjoyment, however, sparks a considerable amount of privacy concerns. Currently, service providers and e-readers have the ability to store their users' reading habits with precise detail, knowing not only what books a reader has purchased but also what books a reader has browsed, what pages a reader has viewed, and even the amount of time a reader

---

* J.D., Indiana University Maurer School of Law, 2013; B.S. in Criminal Justice, University of Central Florida, 2010. I would like to thank Professor Fred Cate for his guidance and insight. Special thanks to my fiancée, Katie, my parents, Karen and Jim, and my sister, Krista, for their encouragement and support.

1. *See* LEE RAINIE, KATHRYN ZICKUHR, KRISTEN PURCELL, MARY MADDEN & JOANNA BRENNER, THE RISE OF E-READING 3 (2012) (discussing the "shift from printed to digital material[s]" in American culture).

2. Press Release, Amazon.com, Amazon.com Now Selling More Kindle Books than Print Books (May 19, 2011), *available at* http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1565581 ("Since April 1, [2011,] for every 100 print books Amazon.com has sold, it has sold 105 Kindle books.").

3. Press Release, Amazon.com, Amazon.com Announces Fourth Quarter Sales up 22% to $21.27 Billion (Jan. 29, 2013), http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1779049 (quoting Amazon CEO, Jeff Bezo, as stating, "After 5 years, eBooks is a multi-billion dollar category for us and growing fast – up approximately 70% last year. In contrast, our physical book sales experienced the lowest December growth rate in our 17 years as a book seller, up just 5%").

4. Jeffrey A. Trachtenberg, *B&N Boots Some DC Graphic Novels*, WALL ST. J., Oct. 10, 2011, at B6.

5. RAINIE ET AL., *supra* note 1, at 4, 18 (finding that individuals using digital devices are reading more frequently "since the advent of e-content").

has dedicated to a single page.[6] This can be quite concerning, considering that the books individuals read can tell more about them than simply what their favorite literary genre might be but can allow others to draw conclusions on their viewpoints, their life's perspectives, and their personal knowledge.[7] Privacy protections of physical books, the center of much debate throughout this country's history, have been afforded adequate legal safeguards in order to protect reader privacy.[8] Because they are obtained through the Internet, digital books exist in society with fewer privacy protections than their physical counterparts.[9] In fact, it has even been suggested that society is apathetically shifting to "a world of automatic, always-on disclosure."[10] Companies are free to collect personal information at their leisure, restrained by little to no regulatory guidelines for protecting consumer privacy.[11] Combine a company's boundless collection abilities with the government's rights to intercept this information, in most cases outside the confines of the Fourth Amendment,[12] and almost instantaneously society begins to witness the erosion of an individual's "right to be let alone."[13]

---

6. *See* NICOLE A. OZER, DIGITAL BOOKS: A NEW CHAPTER FOR READER PRIVACY 4–5 (2010), *available at* http://www.dotrights.org/sites/default/files/Digital%20Books.A%20New%20Chapter%20for%20Reader%20Privacy.pdf.

7. Many in the literary world are quite aware of the unintended information that can be communicated by reading a book. In a recent interview with Goodreads.com, Pulitzer Prize-winning author Jeffrey Eugenides stated, "I think you can know a lot about someone from their books . . . . You can certainly know what someone's interests are. You can place them socially and intellectually." *Interview with Jeffrey Eugenides*, GOODREADS.COM (Oct. 2011), http://www.goodreads.com/interviews/show/617.Jeffrey_Eugenides.

8. Cindy Cohn & Kathryn Hashimoto, *The Case for Book Privacy Parity: Google Books and the Shift from Offline to Online Reading*, HARV. L. & POL'Y REV. BLOG (May 16, 2010), http://hlpronline.com/2010/05/the-case-for-book-privacy-parity-google-books-and-the-shift-from-offline-to-online-reading/ ("Historically, government and social institutions have established safeguards that protect an individual's right to select and peruse printed material free of surveillance and prolonged recordkeeping.").

9. *See id.* (arguing that the privacy protections for physical books should be extended to digital books as well); *see also* OZER, *supra* note 6, at 3 ("[C]ourts have not yet had many opportunities to specifically consider digital book records, leaving their legal protection less clear than is the case for printed works.").

10. Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 690–93 (2013) (arguing for a digital world away from "frictionless sharing" and where "intellectual privacy" is shared "consciously and deliberately, not automatically and unconsciously").

11. *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 6 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("Much of the personal data used on the Internet . . . is not subject to comprehensive Federal statutory protection, because most Federal data privacy statutes apply only to specific sectors . . . .").

12. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 435 (2008) ("[T]he Supreme Court has refused to extend the Fourth Amendment to restrict the government's access to data held by third parties.").

13. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (finding privacy as an extension of the "right to life," which "has come to mean . . . the right to be let alone; the right to liberty secures the exercise of extensive civil

As users' habits in cyberspace continue to be recorded, tracked, and categorized into online data, third parties like government agencies, law enforcement officials, and business entities have realized the information's beneficial possibilities.[14] In order to capitalize on its high value and low gathering costs, these entities have developed new methods in order to gain access to this stored data, even when most in the general public have an expectation that consumer information should remain private,[15] or at least that the consumer should remain in control of how collected information is used.[16] Laws and other governmental restrictions on accessing personal information, such as the Electronic Communications Privacy Act,[17] have made some strides, but "fail[] to be effective when confronted by the problems of the Information Age."[18] As this rapid growth of "trackable" data continues, coupled with an intensified craving by both public and private entities to gain access to that data, some fear that electronically stored personal information related to a user's reading habits could be easily exploited, causing a chilling effect on digital reading.[19] Some have suggested legal responses to curb these problems,[20] though most legislatures have yet to act on the issue.

The most prominent exception to this legislative inertia came on October 3, 2011, when California Governor Jerry Brown signed the Reader Privacy Act[21] into law.[22] Currently, book service providers within California are prohibited from

---

privileges; and the term 'property' has grown to comprise every form of possession—intangible, as well as tangible").

14. *See, e.g.*, Newton N. Minow & Fred H. Cate, *Government Data Mining*, *in* THE MCGRAW-HILL HOMELAND SECURITY HANDBOOK 1063 (David G. Kamien ed., 2005) (discussing the widespread data mining programs within federal agencies); Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 7–43 (2011) (discussing the collection of user data by companies for behavioral targeting practices in advertisements).

15. *See* OZER, *supra* note 6, at 6–7 (reviewing nation-wide surveys that show customer "dissatisfaction" with business methods that track user habits in order to provide content).

16. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 163–65 (2007) (discussing the advancement of new technologies, and examining the expectation the general public might have that some aspects of their lives should be free from Internet tracking and recording).

17. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in 18 U.S.C. §§ 1367, 2232, 2510–21, 2701–10, 3117, 3121–26).

18. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 6–7 (2004).

19. *See, e.g.*, OZER, *supra* note 6, at 6–7; Cohn & Hashimoto, *supra* note 8.

20. *See, e.g.*, Marc Jonathan Blitz, Stanley *in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 HASTINGS L.J. 357 (2010) (arguing that First Amendment privacy protections should be extended to protect web-based interactions); Anne Klinefelter, *Library Standards for Privacy: A Model for the Digital World?*, 11 N.C. J.L. & TECH. 553 (2010) (advocating for digital books to have the same standards as records currently maintained in libraries); OZER, *supra* note 6, at 8–9 (advocating for an extension of privacy policies addressing basic reader protections to digital book formats); Richards, *supra* note 10, at 718–24 (advocating that the consensus "key fair information practices" be extended to reader records).

21. Reader Privacy Act, CAL. CIV. CODE §§ 1798.90, 1798.90.05 (West 2013).

22. *See* Beverly Goldberg, *Librarians Weigh Kindle Ebook Lending Against Reader Privacy*, AM. LIBRARIES ASS'N (Oct. 19, 2011), http://americanlibrariesmagazine.org/e-

disclosing to third parties personal information related to their users,[23] including (1) information that "identifies, relates to, describes, or is associated with a particular user,"[24] (2) a "unique identifier or Internet Protocol Address,"[25] and (3) information that shows a "user's access to or use of a book service or a book, in whole or in partial form."[26] The Act seeks to specifically protect *all* book formats, including electronic formats.[27] Additionally, the Act establishes a highly protective court order process, requiring an entity to show a compelling interest in the book record and that the record sought cannot be obtained through less intrusive means before the record can be disclosed.[28] For many, the Act is a triumph for privacy protection and champions a first-of-its-kind approach to a clear cut rule about when an entity can access an individual's digital information related to his or her book reading habits.[29] Others, however, see it as nothing more than protecting a miniscule segment of data available to exposure and can provide little protection against mass data collection by other state and federal entities.[30] Thus, California's Reader Privacy Act poses a critical question as new initiatives begin to shape the digital

---

content/librarians-weigh-kindle-ebook-lending-against-reader-privacy.

23. CAL. CIV. CODE § 1798.90. "Provider" is defined by the statute as "any commercial entity offering a book service to the public." *Id.* at § 1798.90(b)(6). A "book service" is defined by the statute as "a service that, as its primary purpose, provides the rental, purchase, borrowing, browsing, or viewing of books," and excludes "a store that sells a variety of consumer products when the book service sales do not exceed 2 percent of the store's total annual gross sales of consumer products sold in the United States." *Id*. at § 1798.90(b)(2). "Book" is defined as "paginated or similarly organized content in printed, audio, electronic, or other format, including fiction, nonfiction, academic, or other works of the type normally published in a volume or finite number of volumes," but excludes "serial publications such as a magazine or newspaper." *Id*. at § 1798.90(b)(1). *See also infra* Part II.E.

24. CAL. CIV. CODE § 1798.90(b)(5)(A).

25. *Id.* at § 1798.90(b)(5)(B).

26. *Id.* at § 1798.90(b)(5)(C).

27. *Id.* at § 1798.90(b)(1).

28. *Id.* at § 1798.90(c)(1), (2)(B).

29. *See, e.g.*, Leslie Miller, *Digital Due Process for E-Book Readers*, GOOGLE PUB. POLICY BLOG (Oct. 3, 2011, 4:10 PM), http://googlepublicpolicy.blogspot.com/2011/10/digital-due-process-for-e-book-readers.html ("[The Act] clarifies the law and ensures that there are high standards before booksellers . . . can be compelled to turn over reading records. . . . [It] takes a careful, balanced approach [in] protecting readers' privacy . . . .").

30. *See, e.g.*, Joe Brockmeier, *California Gets Reader Privacy Act: Still Not Enough*, READWRITE ENTERPRISE (Oct. 3, 2011), http://www.readwriteweb.com/enterprise/2011/10/california-gets-reader-privacy.php ("[The Act is] a positive step, but only a short one."); *see also* Bradley Schaufenbuel, Comment, *Revisiting Reader Privacy in the Age of the E-Book*, 45 J. MARSHALL L. REV. 175, 198 (2011) (stating that "extending state library confidentiality laws to apply to e-book providers" would prevent uniform protection and that it would be "questionable whether individual states [could] regulate what is largely an intrastate activity under the Dormant Commerce Clause of the U.S. Constitution"). Some issues have also been raised as to whether the Act would include online blogs within the statute's broad definition of "books." *See*, *e.g.*, Paul Alan Levy, *Does California's New Reader Privacy Act Threaten Individual Bloggers?*, CONSUMER L. & POL'Y BLOG (Oct. 21, 2011, 6:50 PM), http://pubcit.typepad.com/clpblog/2011/10/does-californias-new-reader-privacy-act-threaten-individual-bloggers.html. This Note does not address this issue and assumes for its purposes that blogs are not included within the definition.

book landscape: What can state regulations really do for protecting reader privacy as digital books become more prominent in today's society?

This Note argues that state regulations, such as California's Reader Privacy Act, can provide the foundational framework for true digital reader privacy. With such a lack of regulations geared toward protecting the privacy interests of an individual's digital content, specifically his or her digital book data, this Act could serve as the catalyst to multistate and federal regulations that effectively and efficiently create legal barriers in order to protect personal information related to digital books. Part I examines the architecture of digital books, and how their integration with technology and the Internet has created new legal issues about third-party access to a digital book reader's personal information. Part II details how reader privacy has traditionally been addressed on the private, federal, and state levels. This Part also analyzes how California's Reader Privacy Act seeks to address some of the concerns of digital reader privacy. Part III discusses how state regulations can fill the digital void left by laws and policies currently addressing reader privacy and online privacy, and how this could help formulate a national approach to protecting reader privacy in the digital age.

I. THE COMPLEXITIES OF DIGITAL BOOKS AND ONLINE PRIVACY

Digital books are a breakthrough in literary enjoyment and are full of opportunities for expanding the reach of the written word. The architecture of these digital books, by way of utilizing the Internet, is the source of this effortless expansion. However, this expansion results in multiple avenues for third parties to exploit personal information. This Part seeks to understand that architecture and the possibilities for exploitation.

A. Understanding Digital Books

The process of how book service providers obtain and store their users' digital reading habits is much akin to obtaining and storing digital information through more traditional Internet activities. Currently, the two common forms of digital books are formats that utilize an Internet web browser for a provider's users to read directly on the web, such as Google's Google Play,[31] or formats that utilize a unique digitized format that require a compatible e-reader to view the book, like Amazon.com's Kindle, Barnes & Noble's Nook, and Apple's iPad.[32] Information

---

31. *See Features of a Book on Google Play*, GOOGLE, http://books.google.com/help/ebooks/content.html.

32. *See iBooks*, APPLE, http://www.apple.com/apps/ibooks/; *Kindle*, AMAZON.COM, http://www.amazon.com/Kindle-eReader-eBook-Reader-e-Reader-Special-Offers/dp/B0051QVESA; *Nook*, BARNES & NOBLE, http://www.barnesandnoble.com/u/nook/379003208/. These descriptions are merely a guide to understanding various forms of e-readers and are by no means intended to exhaust the forms of digital books. For a basic, yet more detailed, guide to e-readers, see generally, John Biggs, *Books Under Glass: The Many Faces of E-Readers*, N.Y. TIMES, May 31, 2012, at F3, *available at* http://www.nytimes.com/2012/05/31/technology/personaltech/a-guide-to-electronic-books.html.

related to digital books accessed from webpages can be easily identified by online book service providers through a unique identifier known as an Internet Protocol (IP) address.[33] These identifiers allow book service providers to record the exact device reading its digital content, and know precise information about the device's user, even identifying the exact pages of a book the device has viewed.[34]

E-readers that require account identification in order to purchase and view digital material have the capabilities of recording and tracking even more content about a user's device habits. Amazon.com, for example, maintains on its servers all data about a user's Kindle interactions, including "information related to the Digital Content on your Kindle[,] . . . your use [of that content,] . . . [and] annotations, bookmarks, notes, highlights, or similar markings you make using your Kindle."[35] A service provider's ability to track and record this information can even go one step further, allowing the provider the capability to manipulate the digital information on a user's device.[36] Accessing this information could tell a lot about a person, and has been described as being equivalent to an "offline library or bookstore hiring an agent to follow each individual patron around the stacks, throughout their day, and finally into their homes."[37]

As these methods of providing users with digital books continues to grow more expansive, legal scholars have started to examine how controlling this information can affect an individual's privacy rights.[38] In the context of personal data obtained from users' reading habits, one of the main legal focuses of the privacy debate is on

---

33. For example, Google's new service, Google Play, will maintain the "unique ID numbers" of the devices that access the site. *Google Play - Privacy Policy for Books*, GOOGLE (Oct. 13, 2011), http://books.google.com/googlebooks/privacy.html. *See generally* HAL ABELSON, KEN LEDEEN & HARRY LEWIS, BLOWN TO BITS, YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 301–16 (2008) (providing information about the Internet and how IP addresses function to track and record a user's Internet activity).

34. *See Google Play - Privacy Policy for Books*, *supra* note 33 (stating that Google will "store the last five pages (only) in each book a user has viewed with the user's account" and "store pages viewed for security monitoring and/or if the user elects to use the Web History service"); *see also* OZER, *supra* note 6, at 4.

35. *Amazon Kindle Terms of Use*, AMAZON.COM (Sept. 6, 2012), http://www.amazon.com/gp/help/customer/display.html?nodeId=200506200; *see Amazon.com Privacy Notice*, AMAZON.COM (Apr. 6, 2012), http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496; *see also* OZER, *supra* note 6, at 5.

36. *See* Mariel L. Belanger, Comment, *Amazon.com's Orwellian Gaffe: The Legal Implications of Sending E-Books Down the Memory Hole*, 41 SETON HALL L. REV. 361, 361–62 (2011) (discussing a July 2009 event where Amazon.com, after discovering licensing issues with a company selling George Orwell's *1984* and *Animal Farm* on Kindle devices, "immediately removed the unlicensed content from the Kindle Store[,] . . . reached into users' Kindle devices[,] and deleted the e-books directly from the Kindles of all who had purchased them"); *see also* Blitz, *supra* note 20, at 368–69.

37. Nicole A. Ozer & Jennifer A. Lynch, Protecting Reader Privacy in Digital Books, Association for the Advancement of Artificial Intelligence Privacy 2010 Symposium 2–3 (Apr. 13, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588187; *see also* OZER, *supra* note 6, at 4.

38. *See, e.g.*, Cohn & Hashimoto, *supra* note 8 (advocating for online book privacy to be, at a minimum, equal to the reader privacy associated to offline book privacy).

an individual's right to "avoid[] disclosure of personal matters,"[39] commonly referred to as "information privacy." Information privacy is a relatively new area of privacy law, formed as an eclectic combination of common law, state law, federal law, and constitutional law that revolves around regulating "the collection, use, and disclosure of personal information."[40] While book service providers' utilization of this information sparks its own privacy concerns,[41] the focus of this Note limits its inquiry to the concern of third parties accessing a service provider's stored information related to its users' digital book data for the third party's own independent factfinding, data collecting, or judicial purposes.

The increasing use of the Internet to electronically exchange information has rejuvenated discussion of how information privacy rights for individuals should be addressed by the law.[42] Professor Daniel Solove, the John Marshall Harlan Research Professor of Law at the George Washington University Law School and author of multiple works concerning information privacy, has stated that the concerns of data traveling over the Internet arise as a result of two unique aspects of the Internet.[43] First, the Internet "gives many individuals a false sense of privacy."[44] While this aspect seems to become diluted as advocates and scholars continue to make the lack of online privacy more apparent to society,[45] many still seem to be persuaded that using the Internet in the privacy of one's own home protects the user from intrusive actions.[46] Studies have even suggested that an

---

39. Whalen v. Roe, 429 U.S. 589, 599–600 (1977). *Whalen* also recognized another widely acknowledged form of privacy in the "independence in making certain kinds of important decisions." *Id.* This "decisional privacy" is not discussed in this Note.

40. DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1–2 (2d ed. 2006).

41. *See, e.g.*, Berger, *supra* note 14 (discussing the concerns of companies using personally identifiable information for behavioral targeting).

42. *See, e.g.*, Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages*, 32 HASTINGS COMM. & ENT. L.J. 365 (2010) (examining how privacy laws could apply to the increasing trend of Internet "cloud computing"); Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433 (examining privacy concerns associated with Internet search engines).

43. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1092 (2002).

44. *Id.*

45. *See* Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 217–221 (2012) (recognizing that, since 2009, a variety of factors "have enabled the privacy community to create the climate necessary for a social movement to finally start to coalesce in support of real change in this area").

46. *See, e.g.*, Laura J. Tyson, Comment, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User's Identity*, 40 SETON HALL L. REV. 1257, 1257–58 (2010) (giving an anecdote of a savvy computer user's knowledge of Internet tracking, while informing the readers that such users are in the minority). A false sense of privacy may also derive from an individual's failure to understand how to properly utilize the privacy settings provided by websites. *See, e.g.*, Richards, *supra* note 10, at 713–14 (addressing the difficulties in properly using privacy settings and sharing a rather embarrassing anecdote of the author's colleague, whose lack of understanding resulted in the inadvertent disclosure of the colleague's reading of a somewhat

individual's knowledge of the false sense of privacy in Internet communications would do little to change the behavior of users, who would forgo their awareness of privacy risks for the "immediate gratification" that the Internet provides.[47] While some in the legal community have concluded that such a perception of apathy to Internet privacy is unfounded or diminishing,[48] Professor Solove's observation of the "false sense of privacy" created by the Internet should continue to be a factor in the issues surrounding the Internet's digital privacy concerns.

"Second, the Internet is unprecedented in the degree of detailed information that can be gathered and stored."[49] Technological trends have resulted in computing hardware's ability to increase the speed that data can be accessed, the amount of data that can be stored, and the "connectedness of this hardware over networks."[50] Research suggests that advancements in technology have resulted in computing speeds that double, on average, every eighteen months.[51] Additionally, the decrease in cost to manufacture new computing advancements continues to be a major factor in technological development.[52] Put briefly, computing is cheap, and getting cheaper.

Professor Solove's concerns parallel the privacy concerns associated with digital books as they transition onto the Internet and continue to grow in popularity. Purchasing and reading digital books can occur in the privacy of one's home, often with virtually no interaction with another human being.[53] Even if a sophisticated reader knew such activities were being tracked and analyzed, research suggests that the "immediate gratification" of immediately receiving and reading a digital book might be more important to a reader than taking the time to understand the complexities associated with the user's online exposure.[54] Furthermore, the personal data that service providers track and record about their users is much more expansive than the data collected at traditional brick and mortar bookstores.[55] If the

---

taboo *Washington Post* article).

47. *See* Alessandro Acquisti, *Privacy in Electronic Commerce and Economics of Immediate Gratification*, *in* EC '04: PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE 21 (2004).

48. *See* Cohn & Hashimoto, *supra* note 8 ("[T]he proposition that people care less about their privacy online than offline appears to be untrue."); Ozer, *supra* note 45, at 220–21 ("Surveys performed over the past decade have consistently shown that a large percentage of the American public is concerned about their online privacy.").

49. Solove, *supra* note 43, at 1093.

50. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 88–89 (2007).

51. *Id.* at 90–91 ("Tasks that took an hour 10 years ago now take less than a minute.").

52. *Id.* at 90 ("While the increase in computing power . . . is well known and often cited, less appreciated are the economic implications of that trend, which entail a decrease in the cost of computation by a factor of more than 100 over the past 10 years.").

53. Apple, Google, Amazon.com, and Barnes & Noble, as well as others, all offer the ability to purchase both their reading devices and their digital books online. *See supra* notes 32–33.

54. Reader privacy advocates, however, have argued that this is not the case. *See* Cohn & Hashimoto, *supra* note 8 (criticizing the argument that "privacy protections for books online should be low because people tolerate low privacy norms for online non-book reading").

55. *See* OZER, *supra* note 6, at 4 (stating that, in addition to the detailed information that

last decade's technological developments are any indication, the amount of personal data that service providers will be able to collect about its users' reading habits will only become more detailed and more cost effective over the coming years. While data-based advertisement programs, for instance, create a large incentive for Internet companies to continue collecting data,[56] it is likely that the tracking of personal data related to digital books will also continue to grow along with the Internet's technological advancements.

B. Gaining Access to Digital Book Records

Recognizing a societal interest in protecting personal data as it is collected by government and other third-party entities, federal and state laws have been enacted over the past half century to protect personal information.[57] However, as technology continues to grow more expansive, these older privacy laws are quickly becoming irrelevant, burdensome, or obsolete.[58] This has been most apparent over the last decade's increasingly Internet-dependent society, coupled with an increase in the value of personal data in commercial and governmental data-gathering initiatives.[59] As laws continue to stall in adequately addressing increasing technologies, the ability of third parties, such as governmental and corporate entities, to exploit the Internet's advancements has become more of a privacy concern to the public at large.[60]

The government has been especially cognizant of its ability to gain an increasingly large amount of data with little to no oversight or restriction.[61] The government currently has the ability to access on its own, or purchase from private entities, an unlimited amount of personal data on individuals, with or without

---

digital book service providers are able to obtain about their customers' digital reading habits, it is easy for these companies "to link books that are browsed or read with a reader's other online activities, such as Internet searches, emails, cloud computing documents, and social networking").

56. *See* Berger, *supra* note 14, at 31 ("The market for behavioral advertising is expected to grow 'from $350 million in 2006 to $3.8 billion by 2011.'" (quoting Andrew Hotaling, Comment, *Protecting Personally Identifying Information on the Internet: Notice and Consent in the Age of Behavioral Advertising*, 16 COMMLAW CONSPECTUS 529, 539 (2008)).

57. *See* SOLOVE ET AL., *supra* note 40, at 35–38 & nn.38–44 (providing an overview and a brief description of federal and state privacy statutes, including the Electronic Communications Privacy Act, the Children's Online Privacy Protection Act of 1998, and the Video Voyeurism Prevention Act of 2004).

58. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1461 (2000).

59. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 588–91 (2011).

60. *See* James Ridge, Comment, *What Happens When Everything Becomes Connected: The Impact on Privacy When Technology Becomes Pervasive*, 49 S. TEX. L. REV. 725 (2008) (arguing that unclear information privacy laws are causing an increased invasion on individual privacy).

61. *See* Cate, *supra* note 12, at 436 (stating that government concerns, including national security and ineffective interagency communications, have "helped to fuel an apparently insatiable government appetite for access to and retention of personal data, especially from the vast databases routinely maintained by the private sector").

reasonable suspicion of the individual's behavior.[62] Within the current legal framework, the "digital dossier" of an individual that these government and third-party entities can create increases exponentially as the utilization of new technologies, like digital books, continues to grow.[63]

Although the Fourth Amendment has long protected individuals from the search and seizure of private records by the government without reasonable justification,[64] advancements in technology and the way that data is processed over the Internet have caused issues with how the Fourth Amendment can protect digital, personal data.[65] Just prior to the 1970s, the Supreme Court's decision in *Katz v. United States* focused the Amendment's underlying framework on an individual's "expectation of privacy."[66] This new interpretation influenced the Court's decision in *United States v. Miller*, where the Court ruled that the government's acquisition of Miller's bank records was constitutional.[67] In ruling that Miller had no expectation of privacy that would warrant the protection of the Fourth Amendment, the Court opined that because the records "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," Miller had no expectation of privacy in the records themselves.[68] The Court stated that Miller, and all patrons of the bank for that matter, "takes the risk, in revealing his [or her] affairs to another, that the information will be conveyed by that person to the Government."[69] What resulted is the "Third Party Doctrine," which holds that the Fourth Amendment offers no protections when information is voluntarily given to a third party who, in turn, reveals that information to the government.[70]

The Court expanded the Third Party Doctrine over time, and eventually determined that even the automated process of handling data was enough to trigger the Doctrine,[71] leaving all information flowing through automatic processes

---

62. *Id.* at 436–37 ("In the absence of either practical obscurity or effective legal privacy protections, the government has unprecedented and virtually unlimited access to an extraordinary volume and variety of personal data . . . of individuals who have done nothing to warrant suspicion.").

63. For a look at the accessibility of what digital data can be tracked, recorded, and categorized about an individual, creating what Professor Solove calls the "digital dossier," see SOLOVE, *supra* note 18, at 1–22.

64. *See* U.S. CONST. amend. IV.

65. *See* Tokson, *supra* note 59, at 584 ("Virtually every form of personal data on the Internet, no matter how revealing, seems likely to remain unprotected by the Fourth Amendment, and again to receive only ineffectual statutory protection." (footnote omitted)).

66. 389 U.S. 347, 360 (1967) (J. Harlan, concurring); *see also* Tokson, *supra* note 59, at 597 ("[I]n the 1967 case *Katz v. United States* . . . [t]he Fourth Amendment's scope would no longer depend on property interests and the law of trespass, but instead on citizens' expectations of privacy." (footnote omitted)).

67. 425 U.S. 435, 445 (1976).

68. *Id.* at 442.

69. *Id.* at 443.

70. *See* Tokson, *supra* note 59, at 584.

71. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the use of a pen registry does not constitute a "search" under the Fourth Amendment, even when the information collected is only exposed to a telephone company's equipment).

susceptible to constitutionally acceptable government access without suspicion. Today, some courts have found that an individual's IP address falls victim to the Third Party Doctrine.[72] There is a growing fear that some data traveling through Internet servers could arguably be without Fourth Amendment protection.[73] Thus, the continuous expansion of automated data processes will likely result in an expansion of digital information that is constitutionally unprotected under the Fourth Amendment.[74] As an individual's personal information related to digital books continues to be stored and transmitted through online book service providers' servers, it too runs the risk of having no constitutional protection under the Fourth Amendment.

Congress has tried to establish some semblance of personal data protection associated with electronic communications and stored data, but these attempts have often led to confusion in interpreting the law's language in the context of today's technological practices.[75] For example, the Electronic Communications Privacy Act (ECPA), adopted in 1986, amended the federal wiretapping statute to include protections of other up-and-coming forms of communications, including "electronic communication."[76] The law's protection of stored electronic communications today, however, leaves peculiar holes in the modern understanding of the law's framework, now that Internet communications have come into existence and electronic communications have advanced since the late 1980s.[77] A portion of ECPA enacted the Stored Communications Act (SCA), which provides a specific process for compelling disclosure of stored data maintained by a third-party service provider.[78] At the time of SCA's enactment, "small businesses sometimes used third-party remote data-processing services to assist them in

---

72. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2008) (holding that Internet users have no expectation of privacy in their IP address because the information is voluntarily turned over by the user).

73. *See* Tokson, *supra* note 59, at 602–09 (hypothesizing that the continued use of the "automation rationale" to the Third Party Doctrine will leave "enormous quantities of users' personal Internet data" at risk to exposure).

74. *See id.* at 601–03 (arguing that the Third Party Doctrine leaves unprotected under the Fourth Amendment virtually all personal online data exposed to third-party equipment).

75. *Id.* at 592–96 (claiming that federal statutes that came as a result of the Court's Third Party Doctrine "did little" to prevent government surveillance).

76. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in 18 U.S.C. §§ 1367, 2232, 2510–21, 2701–10, 3117, 3121–26).

77. For instance, ECPA has been interpreted to allow government access with an administrative subpoena—as opposed to a standard search warrant—to an individual's e-mail messages, if the e-mail has been on a service provider's server for a term of more than 180 days. *See* 18 U.S.C. § 2703 (2006). Additionally, the government has interpreted ECPA to mean that "all opened e-mails that remain on Google or Yahoo!'s servers can be accessed with a subpoena as soon as they are opened, rather than 181 days after they are sent." Tokson, *supra* note 59, at 594; *see also* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 122–25 (3d ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

78. *See* 18 U.S.C. §§ 2701–2711 (2006); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210–13 (2004) (explaining the congressional intent of implementing the SCA).

managing computerized data."[79] Because, at the time, the typical third-party remote data-processing service handled only non-sensitive data, it was given minimal protections.[80] Internet companies like Google, which handles and stores enormous amounts of individual consumer data daily,[81] did not exist. In today's Internet-dependent society, remote computing services are much more prevalent,[82] and SCA only requires that the government procure an administrative, grand jury, or trial subpoena—rather than a more protective court warrant—to access the information, as long as the subscriber or customer is notified.[83] Because of the current system that digital book services use to deliver their digital books, it is likely that these "remote computing services" would only require the government to obtain a subpoena and notify the user in order to comply with SCA, "regardless of how personal or intimate [the information] might be."[84]

Additionally, personal information related to digital books could be susceptible to federal government regulations on data collection, irrespective of any actual criminal or civil charges.[85] One of the most notable regulations sparking public debate over the past decade from reader privacy advocates is the Foreign Intelligence Surveillance Act,[86] which has been amended over time to enhance the government's surveillance abilities while enacting less restrictive judicial restraints on utilizing those abilities.[87] The USA PATRIOT Act's section 215 amendment, for instance, expanded the process and scope of the Federal Bureau of

---

79. Tokson, *supra* note 59, at 594.

80. *Id.*; *see also* Kerr, *supra* note 78, at 1233 ("Only unretrieved e-mail and other temporarily stored files held pending transmission for 180 days or less receive the protection of a full warrant requirement. The lower standard that applies to other stored content covered by the statute is surprisingly low . . . ." (footnote omitted)).

81. One report suggests that Google processes about twenty petabytes, or twenty quadrillion bytes, of information daily. Jeffrey Dean & Sanjay Ghemawat, *MapReduce: Simplified Data Processing on Large Clusters*, 51 COMM. THE ACM 107, 107 (2008).

82. *See* Tokson, *supra* note 59, at 594–95 ("Today, millions of Internet users use remote computing services such as Google Docs to create documents and spreadsheets, store personal photos, videos or other files, or to back up their entire hard drives on remote servers." (footnote omitted)).

83. *See* 18 U.S.C. § 2703(b). For a more detailed understanding of a very complex statutory scheme, see generally Kerr, *supra* note 78, at 1218–33.

84. Tokson, *supra* note 59, at 595.

85. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 50, at 242–43. In an effort to combat national security issues, including eradicating terrorism, the government has utilized a procedure called "predictive data mining" by collecting vast amounts of data in an effort to calculate patterns of terrorist-related behavior. *See* Cate, *supra* note 12, at 473–76 (discussing predictive data mining and some of the issues related to its use as a national security tool). *See generally* Jim Harper, *The Privacy Implications of Government Data Mining Programs*, 8 PRIVACY & INFO. L. REP., no. 1, Jan. 2007, at 1.

86. *See, e.g.*, Michael J. O'Donnell, *Reading for Terrorism: Section 215 of the USA PATRIOT Act and the Constitutional Right to Information Privacy*, 31 J. LEGIS. 45, 48 (2004) (arguing that Section 215 of the USA PATRIOT Act may violate "the Fifth and Fourteenth Amendment constitutional right to information privacy"); Richards, *supra* note 10, at 712 (describing the American Library Association's efforts to overturn Section 215 of the USA PATRIOT Act).

87. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 50, at 242–44.

Investigation's access to records related to international terrorism and foreign intelligence investigations.[88] The Act expanded the scope of "tangible things," as defined by the law, to allow government access to "books, records, papers, documents, and other items."[89] In addition to increasing the scope of accessible records, the PATRIOT Act eased the ability of FBI officials to gain access to those records by requiring that they show to a Foreign Intelligence Surveillance Act (FISA) court that the records are "relevant" to a foreign terrorist investigation.[90] The changes to FISA are still in effect,[91] and opponents to this expansive power argue that the government could gain access to a citizen's book records with little judicial oversight and with little evidence to compel the FISA court to allow access to the records.[92]

As personal information related to digital books becomes more Internet dependent, the more severe the potential exposure of personal information to government entities becomes. Because of the Third Party Doctrine, an individual would likely have no constitutional protection from government access to an individual's digital book records. While federal regulations like ECPA have attempted to protect content traveling through electronic communications, the system in which digital books are currently used would allow the government to gain access to some data connected to a digital book transaction with little more than an administrative subpoena. Attempts to protect data specifically related to reader privacy rights have been enacted over time, but as Part II addresses, these laws still have many issues to address as books transition to digital formats and Internet processing.

II. READER PRIVACY IN THE LAW

What makes the possibility of exploiting a person's digital reading habits so concerning is in part related to the historical significance, and long history of legal protection, that *physical* books have enjoyed throughout our nation's history.[93] Books have the ability to inscribe vast amounts of information to the general public, while simultaneously revealing much about the individuals who choose to read the material. The books we choose to read can say "a lot about who [we] are, what [we] value, and what [we] believe."[94] Throughout American history, we have

---

88. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88 (2001) (codified at 50 U.S.C. § 1861 (2006)).

89. *See id.*; O'Donnell, *supra* note 86, at 45–46. *Compare* USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88 (2001), *with* 50 U.S.C. § 1861 (prior to 2001 Amendment).

90. *See* 50 U.S.C. § 1861(b) (2006); *see also* O'Donnell, *supra* note 86.

91. *See* 50 U.S.C. § 1861. The FISA Amendments Act of 2008 amended some of the language of the statute, but did little to affect the ability of the government to access records. *See* FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

92. *See, e.g.*, O'Donnell, *supra* note 86, at 46 & nn.10–12 (2004) (reviewing multiple organizations' discontent and opposition to Section 215 of the PATRIOT Act).

93. *See, e.g.*, OZER, *supra* note 6, at 2 ("There is a long and proud history of legal protection for reading privacy in the United States.").

94. OZER, *supra* note 6; Ozer & Lynch, *supra* note 37, at 1.

seen many individuals point to books as a way of understanding how a person acts. In the early 1950s, Senator Joseph McCarthy and the Senate Permanent Subcommittee on Investigations interrogated individuals believed to have communist ties by questioning whether they had ever read literature by Karl Marx and Vladimir Lenin, two influential leaders of the communist movement.[95] Controversial books, such as J.D. Salinger's *The Catcher in the Rye*, have been immersed in controversy over the possible influence these books have had on their readers, like John Lennon's murderer, Mark David Chapman, and President Ronald Regan's assailant, John Hinckley Jr.[96] In understanding the chilling effect on reading that such practices may produce, the general landscape of the law has been to protect a book reader's right to remain anonymous.[97] However, traditional avenues have brought added difficulties when transitioning over to digital books.

A. Book Service Provider and Private Entity Protections

While many service providers have a strong incentive to collect data related to their users' reading habits, they have traditionally been very protective of releasing that information to third-party entities.[98] Google, for example, has been a strong advocate of reader protection and was a supporter of California's Reader Privacy Act.[99] Google has proactively developed additional privacy protections for its users by focusing on transparency, dedicating sections of its website to explaining the company's privacy policies,[100] and providing detailed information related to requests by the world's governments to alter, remove, or access data collected by the company's websites.[101] Amazon.com has also taken a hardened stance on not

---

95. *See* 5 COMM. OF GOV'T AFFAIRS, 107TH CONG., EXEC. SESSIONS OF THE SENATE PERMANENT SUBCOMM. ON INVESTIGATIONS OF THE COMM. ON GOV'T OPERATIONS 356–57 (Comm. Print 2003) (releasing the transcript of a January 15, 1954 meeting of the U.S. Senate Permanent Subcommittee on Investigations of the Committee of Government Operations, where Assistant Counsel C. George Anastos questioned George Frederick Moore, a General Electric Employee, about whether he had ever "read the works of Marx and Lenin"); *see also* OZER, *supra* note 6, at 6.

96. *See* Stephen J. Whitfield, *Cherished and Cursed: Toward a Social History of The Catcher in the Rye*, 70 NEW ENG. Q. 567, 571–78 (1997) (recounting the connection of *The Catcher in the Rye* to the two individuals, as well as the reaction by many to ban the book from libraries and schools).

97. *See* OZER, *supra* note 6, at 1 ("It has long been recognized that the freedom to read without worrying about who is looking over your shoulder plays an essential role in the freedom of thought . . . .").

98. The Electronic Frontier Foundation has found that some of the major internet companies—including Amazon.com, Google, Comcast, Twitter, and Yahoo!—have all fought for user privacy in court against government requests for data. MARCIA HOFFMAN, RAINEY REITMAN & CINDY COHN, 2012: WHEN THE GOVERNMENT COMES KNOCKING, WHO HAS YOUR BACK?: THE ELECTRONIC FRONTIER FOUNDATION'S SECOND ANNUAL REPORT ON ONLINE SERVICE PROVIDERS' PRIVACY AND TRANSPARENCY 6 (2012), *available at* https://www.eff.org/sites/default/files/who-has-your-back-2012_0_0.pdf.

99. *See* S. RULES COMM., 2011 Leg. Bill Hist. S.B. 602 (Cal. Sept. 1, 2011).

100. *See Privacy Policy*, GOOGLE, http://www.google.com/intl/en/policies/privacy/.

101. *See Google Transparency Report*, GOOGLE, http://www.google.com/

releasing information that could compromise the privacy of its users' reading habits in fear that such action might "chill" a user's right to read.[102] However, these proactive steps are entirely at the hands of the companies, and they face few legal obstacles in choosing to voluntarily release the acquired information to government entities if these companies so choose.[103]

Non-profit organizations have also been very proactive in addressing the issues of digital reader privacy. The Electronic Frontier Foundation and the American Civil Liberties Union of Northern California, for example, have provided strong support in reader privacy protection and have provided multiple resources for individuals to stay protected while using e-readers.[104] These groups have advocated privacy regulations that mirror the protection given to physical books, and have developed basic principles for policy-makers to follow when addressing the issue of privacy.[105] During the recent settlement negotiations between Google and the Author's Guild concerning Google's e-book services, the Electronic Frontier Foundation, on behalf of multiple authors, filed an objection to a proposed settlement agreement because of the settlement's failure to address any reader privacy safeguards.[106] While advocacy and transparency are very valuable in

---

transparencyreport/removals/government/.

102. *See infra* Part II.B. As another example of its protection of users' book records, Amazon.com has refused to publicly verify the creator of a "wishlist" that is suspected to have belonged to Boston Marathon bombing suspect, Tamerlan Tsarnaev. As *The New York Times* reports, "Amazon would not confirm whose list it was, citing its privacy policy." Michiko Kakutani, *Unraveling Brothers' Online Lives, Link by Link*, N.Y. TIMES, Apr. 24, 2013, at A1, *available at* http://www.nytimes.com/2013/04/24/us/unraveling-brothers-online-lives-link-by-link.html.

103. *See* Ozer & Lynch, *supra* note 37, at 2 ("[T]he technological advances in moving books into the digital environment have outpaced existing book privacy laws, leaving few protections currently in place to prevent providers from exposing readers' information . . . to third parties and to the government."); *see also* Richards, *supra* note 10, at 700–02 (suggesting that the protection of reading records by companies is based on "[c]orporate self-interest," and "[w]hen there is financial incentive to disclose information, it should be no surprise that the trend towards data aggregation and disclosure has begun to affect reader records").

104. The American Civil Liberties Union, for instance, has created *Dotrights.org*, which advocates a demand for greater online privacy protection and dedicates sections of the site to informing users of privacy concerns about digital books. *See Demand Your dotRights*, DOTRIGHTS, http://dotrights.org/. The Technology and Civil Liberties Policy Director at the ACLU of Northern California, Nicole A. Ozer, authored *Digital Books: A New Chapter for Reader Privacy*, as a free guide that details the history of privacy rights and calls for reader privacy reform in digital books. OZER, *supra* note 6. Additionally, the Electronic Frontier Foundation has published a check-list for users looking to protect their rights while reading digital books. *See* CORYNNE MCSHERRY & CINDY COHN, DIGITAL BOOKS AND YOUR RIGHTS: A CHECKLIST FOR READERS (2010), *available at* https://www.eff.org/sites/default/files/eff-digital-books_0.pdf.

105. For instance, the Electronic Frontier Foundation and the Center for Democracy and Technology advocate for: (1) "Limited Tracking of User Information," (2) "Adequate Protection Against Disclosure," (3) "User Control over Personal Information," and (4) "Sufficient Transparency in Data Use and Enforceability of Commitments." Cohn & Hashimoto, *supra* note 8.

106. Privacy Authors and Publishers' Objection to Proposed Settlement, Authors Guild,

informing users on how to take their own proactive steps to protect their privacy online, they unfortunately provide no legal authority to protect an individual who chooses to enjoy a digital book.

B. First Amendment Protections

Many reader privacy advocates have suggested,[107] and some courts have acknowledged,[108] that the First Amendment's Free Speech Clause protects the privacy interests of individuals reading books. While the Supreme Court has directly interpreted the First Amendment to protect anonymous speech,[109] many have understood the Amendment to protect anonymous reading in some instances as well. In *United States v. Rumely*, for instance, the Supreme Court overturned a conviction based on the defendant's reluctance to release book records demanded by the United States House of Representatives.[110] The House Select Committee on Lobbying Activities was given the authority to investigate activities intended to influence legislation.[111] Mr. Rumely, the Secretary of the Committee for Constitutional Government, was charged and convicted for refusing to release the names of individuals who made bulk purchases of books that the Court described as being "of a particular political tendentiousness."[112] The Court ruled that the House Committee's power to inquire into the book distribution "raises doubts of constitutionality in view of the prohibition of the First Amendment."[113]

Since the Supreme Court's ruling in *Rumely*, lower federal and state courts have continuously protected book distributors from releasing personal information related to their book sales under the protections of the First Amendment.[114] In 2006, Amazon.com successfully prevented a federal wire fraud investigation of Robert B. D'Angelo from requiring the company to release thousands of its customers' personal information.[115] Viewing the subpoena as "troubling," the

---

Inc. v. Google Inc., 770 F. Supp. 2d 666 (S.D.N.Y. 2011) (No. 05 CV 8136-DC). The settlement agreement was later vacated on other grounds. *See* Authors Guild, Inc. v. Google Inc., 770 F. Supp. 2d 666, 670 (S.D.N.Y. 2011).

107. *See, e.g.*, Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1003–19 (1996); Schaufenbuel, *supra* note 30, at 189 ("[L]egal scholars have long argued that reader privacy is implicitly guaranteed by the First Amendment of the U.S. Constitution.").

108. *See, e.g.*, Lubin v. Agora, Inc., 882 A.2d 833, 846 (Md. 2005) (holding that a subpoena that seeks to disclose the identities of a publisher's readers "seek[s] information within the protective umbrella of the First Amendment").

109. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment."); Talley v. California, 362 U.S. 60, 64 (1960) ("Anonymous . . . books have played an important role in the progress of mankind.").

110. *See* 345 U.S. 41 (1953).

111. *Id.* at 42–45.

112. *Id.* at 42.

113. *Id.* at 46.

114. *See, e.g.*, *In re* Grand Jury Subpoena to Kramerbooks & Afterwords, Inc., 26 Med. L. Rptr. 1599 (D.D.C. 1998) (denying the government's subpoena to obtain the book purchase records of Monica Lewinsky as part of the Clinton-Lewinsky investigation).

115. *See In re* Grand Jury Subpoena to Amazon.com Dated August 7, 2006, 246 F.R.D.

district court found legitimate First Amendment concerns with a subpoena that "permits the government to peek into the reading habits of specific individuals without their prior knowledge or permission."[116] In *Amazon.com v. Lay*, Amazon.com successfully prevented the North Carolina Department of Revenue from requiring the company to release the names of many of its customers who had purchased books on their site.[117] In ruling that the disclosure would violate the users' rights, the court made clear: "[T]he fear of disclosure of [the customer's] reading . . . habits poses an imminent threat of harm and chill to the exercise of First Amendment rights."[118]

While some believe a right to anonymous reading is inherent within the First Amendment, the Supreme Court has never definitively established a right to "anonymous reading" like the Court has with "anonymous speech." While some lower courts have protected such rights, government entities in many jurisdictions are still free to access such information. Additionally, the landscape of digital books on the Internet, as opposed to physical books in the home or bookstores, could potentially play a factor of how courts view "anonymous reading" and its First Amendment implications.

C. State Judicial Protections

State courts have also found privacy interests in book records through an understanding of the First Amendment alone, or through a "hybrid" analysis of the state's constitutional privacy clauses in tandem with First Amendment protections. In *Tattered Cover, Inc. v. City of Thornton*, the Supreme Court of Colorado addressed the ability of state law enforcement officers to compel the release of an individual's book purchases.[119] During an investigation into a methamphetamine lab, the police seized two books that they believed would link the lab to the true perpetrator.[120] Believing that the suspects purchased the books from the Tattered Cover bookstore, an administrative subpoena was served on the store to release the names of all individuals who had purchased the books.[121] The bookstore refused, and the court found that the First Amendment and Colorado's constitutional privacy clause "protect[s] an individual's fundamental right to purchase books anonymously, free from governmental interference."[122]

Other state courts have also found a right to anonymous reading through their own interpretation of the First Amendment.[123] That being said, few states have designated blanket privacy protections within their state's constitution, like the one

---

570, 571–72 (W.D. Wis. 2007).

116. *Id.* at 572.

117. *See* 758 F. Supp. 2d 1154 (W.D. Wash. 2010).

118. *Id.* at 1163.

119. *See* 44 P.3d 1044, 1044 (Colo. 2002).

120. *Id.* at 1049.

121. *Id.*

122. *Id.* at 1047.

123. *See e.g.*, Lubin v. Agora, Inc., 882 A.2d 833 (Md. 2005) (holding that the First Amendment's protection of anonymity prevented a newsletter subscriber list published by Agora from being disclosed without a compelling interest).

found in Colorado.[124] States that do not have such protective privacy clauses could potentially leave their citizens with no avenue to protect against third party requests of their personal information related to their reading habits.

D. State Legislative Protections

This Note contends that new initiatives in state regulations are an effective way to address some of the privacy issues associated with digital books. However, the current state of these laws contains just as many problems as the other methods of protection discussed above. State laws account for a large spectrum of privacy rights in a wide variety of areas, differing from state to state.[125] In the context of reading records, many states have implemented large initiatives to protect libraries.[126] Currently, forty-eight states and the District of Colombia all have laws that protect information and records maintained at libraries, including data related to patron reading records,[127] while a number of states specifically name library records as "confidential."[128] However, few states extend these protections to all book services that might have information related to an individual user.[129] While state legislation has been effective in preventing the disclosure of information at libraries to third-party entities, the current laws lack protections when faced in an online environment.[130]

E. The Aims of California's Reader Privacy Act

California's Reader Privacy Act was proposed to address some of the modern privacy concerns facing digital book users and to create a law that provides clear guidelines for government and third-party access to sensitive reading records.[131] The Act places into law three unique factors that establish an unprecedented step for digital reader privacy protection.

---

124. *See* ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 56–57 (2002 & Supp. 2011) (listing only twelve states that have a blanket privacy clause within their constitution: Alaska, Arizona California, Florida, Hawaii, Illinois, Louisiana, Montana, New York, Pennsylvania, South Carolina, and Washington).

125. *See generally id.* at 2 (providing a table of states' privacy protection on a variety of topics, including arrest records, bank records, credit information, library records, social security numbers, student records, and tax records).

126. *E.g.*, D.C. CODE § 39-108 (2001); FLA. STAT. ANN. § 257.261 (West 2009); N.Y. C.P.L.R. 4509 (McKinney 2012); VT. STAT. ANN. tit. 22, § 172 (2009); *see also* OZER, *supra* note 6, at 3 ("Virtually every state protects public library reading records from disclosure by statute.").

127. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 50, at 237.

128. SMITH, *supra* note 124, at 40–41; *see also* Richards, *supra* note 10, at 708–12 (describing the efforts made by librarians to protect reading records).

129. *See* Ozer & Lynch, *supra* note 37, at 2; Schaufenbuel, *supra* note 30, at 183.

130. Professor Neil Richards of Washington University Law School states that "[o]ur law is thus in a muddle when it comes to reader records . . . . The rise of social media platforms has increased the importance of the issue, as well as the problems cause by our law's inconsistency." Richards, *supra* note 10, at 702.

131. *See* S. RULES COMM., *supra* note 99.

First, the Act adopts a definitional framework that more appropriately addresses some of the issues facing consumers who utilize digital books. Specifically, the Act protects digital and Internet-related personal information by specifically including in its definition all "electronic" book formats,[132] and includes "[a] unique identifier or Internet Protocol address" as a protected form of personal information.[133] Privacy laws that lack specificity run the risk of inviting confusing decisions by courts and administrative agencies, especially when trying to protect privacy concerns in the ever-changing realm of technology.[134] By specifically and clearly targeting books in all electronic formats, California's courts should have little trouble understanding the true scope and purpose of the law.[135] Additionally, by adding a user's IP address as personal information that is protected under the Act, it is now unmistakable that third parties need a warrant before gaining access to one of the most telling pieces of data that can connect readers to their digital books.

Second, the Act establishes heightened requirements for third party access to a user's personal book information. To begin with, the default rule prohibits book service providers from knowingly disclosing personal book information to any government entity, or from being compelled to disclose any personal book information to a person, private entity, or government entity.[136] However, in addition to a small number of other exceptions,[137] government entities, law enforcement entities, and private entities will be able to gain access to personal book information stored by a book service provider only through a court order establishing, among other requirements: (1) that the entity has a compelling interest in obtaining the information sought and (2) that the information cannot be obtained through less intrusive means.[138] This heightened court order requirement is similar to the "necessity" requirement for federal wiretaps, which require that the government demonstrate in its warrant request that other investigatory techniques would be unlikely to succeed in gaining the information sought.[139] Such a

---

132. CAL. CIV. CODE § 1798.90(b)(1) (West 2013).

133. *Id.* § 1798.90(b)(5)(B).

134. *See, e.g.*, Tokson, *supra* note 59, at 592–94.

135. *But see supra* note 30.

136. CAL. CIV. CODE § 1798.90(c).

137. Included within the Act is the right of the book service provider to disclose the personal information if "informed, affirmative consent" is given by the user, if there is a good faith belief that "imminent danger of death or serious physical injury" will occur and "there is insufficient time to obtain a court order," or if the book service provider in good faith believes the information "is evidence directly related . . . to a crime against the provider or that user." CAL. CIV. CODE § 1798.90(c)(3)–(5).

138. *Id.* § 1798.90(c)(1)–(2). An additional section was added by the Act to clarify that

> Section 1798.90 does not make it unlawful for a law enforcement entity . . . to obtain a search warrant for the personal information of a user pursuant to otherwise applicable law in connection with the investigation or prosecution of a criminal offense when probable cause exists to believe that the person possessing the personal information has committed, or is committing, a criminal offense involving . . . child pornography . . . .

Id. § 1798.90.05.

139. *See* 18 U.S.C. § 2518(1)(c) (2006) ("[A] full and complete statement as to whether or not other investigative procedures . . . reasonably appear to be unlikely to succeed if

heightened requirement for obtaining search warrants is desirable because it creates less of an incentive for government entities to utilize warrants for personal information as a "traditional" or "routine" step in an investigation.[140] Therefore, adding these more burdensome requirements makes it so third party entities seek court orders for personal book information only when absolutely necessary.

Third, the Act provides notice requirements that are intended to accommodate the provider whose information is being requested, the individual whose information is being disclosed, and the citizens of California at large. In regards to a specific court order to disclose a user's personal book information, the Act requires the requesting entity to give notice of the order to the book service provider so that the provider has time to properly contest the request.[141] If the requesting entity is law enforcement, as defined by the Act,[142] the law enforcement entity must give notice of the court order to the provider's user "contemporaneously with the execution of the order."[143] If the requesting entity is one of the other entities eligible to request a court order for a user's personal book information,[144] then the book service provider must provide timely notice to the user "about the issuance of the order" and the user's "ability to appear and quash the order."[145] So even if one of the entities eligible to request a court order for a user's personal book information is able to succeed in meeting the rigorous requirements, adequate notice must still be given to both the book service provider and the user before any information can be disclosed.

---

tried . . . .").

140. *See* United States v. Foy, 641 F.3d 455, 464 (10th Cir. 2011) (explaining that the "necessity" requirement in wiretap warrants prevents government entities from using wiretaps when alternative techniques would be equally effective).

141. CAL. CIV. CODE § 1798.90(c)(1)(D), (c)(2)(B)(iii).

142. A "[l]aw enforcement entity" means

> [A] district attorney, a district attorney's office, a municipal police department, a sheriff's department, a county probation department, a county social services agency, the Department of Justice, the Department of Corrections and Rehabilitation, the Department of Corrections and Rehabilitation Division of Juvenile Facilities, the Department of the California Highway Patrol, the police department of a campus of a community college, the University of California, or the California State University, or any other department or agency of the state authorized to investigate or prosecute the commission of a crime.

Id. §1798.90(b)(4).

143. *Id.* § 1798.90(c)(1)(E). The law enforcement entity may forgo notice to the user if "there is a judicial determination of a strong showing of necessity to delay that notification for a reasonable period of time, not to exceed 90 days." *Id.*

144. Specifically, this would only include (1) "[a] government entity, other than a law enforcement, pursuant to a court order issued by a court having jurisdiction over an offense under investigation by that government entity," or (2) "[a] government entity, other than a law enforcement entity, or a person or private entity pursuant to a court order in a pending action brought by the government entity or by the person or private entity." *Id.* § 1798.90(c)(2)(A).

145. *Id.* § 1798.90(c)(1)(B)(iv). Additionally, the user whose information is being requested must be given "a minimum of 35 days prior to disclosure of the information within which to appear and quash the order." *Id.*

In regards to requests for personal book information more generally, the Act requires a book service provider to publicly report instances in which "it has disclosed personal information related to the access or use of a book service or book" when thirty or more disclosures have been made by the book service provider.[146] These reports are required to be "publicly available in an online, searchable format" either on the book service provider's website or sent to California's Office of Privacy Protection by March 1 of each year.[147] Not only will these notice requirements allow for the individual users to have a formal way of protecting their information prior to a third party's actual access, but it will also allow the public at large to be informed about a service provider's activities, like what requests have been made, when the requests were made, and how many requests were made.[148] With the process in place, many of the privacy fears associated with digital books are adequately addressed for California's digital book patrons.

III. THE IMPACT OF STATE REGULATIONS ON DIGITAL READER PRIVACY

State regulations like California's Reader Privacy Act can provide effective solutions to address the current problems of inadequate privacy protections for digital book information. While its practical effect will be concentrated in area and limited in scope, its framework can be the beginning of a "trickle up" approach to privacy protection that can lead to additional state and even federal regulations.

A. The Benefits of State Regulations

States with reader privacy regulations that specifically and textually target digital books will create far-reaching protections for their citizens. The constitutional concerns that the Fourth Amendment poses—including the Third Party Doctrine—will no longer be an issue. Statutory protections would supplement the lack of constitutional protections, regardless of the method that readers choose to access their books. With the Third Party Doctrine in place, a reader could have different constitutional protections in the same book depending on how the reader gained access to that book—either accessed physically or electronically through the Internet. The justification and reasoning that courts have used in protecting book records have had little to do with differentiating between how the reader accessed the book and more to do with the overall negative implications that would follow from allowing access to a reader's book records.[149] Therefore, by specifically

146. *Id.* § 1798.90(i)–(l).

147. *Id.* § 1798.90(j). In addition, providers subject to California's Business and Professions Code are required to place on their website that a disclosure report does not exist if the provider is exempt for not meeting the thirty disclosure request threshold. *Id.* § 1798.90(k).

148. *See id.* § 1798.90(i)(1).

149. *See, e.g.*, Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1056 (Colo. 2002) (holding that books are awarded protection from law enforcement officers because a lack of protection would likely "chill people's willingness to read a full panoply of books and be exposed to diverse ideas").

targeting the type of tangible records that the state believes should deserve privacy protections—like physical and digital book records—the means by which these books are delivered to the individual reader will no longer be the focus of whether or not the tangible record is worthy of protection from government search and seizure. Statutory protections would allow a reader to feel safe knowing that the digital or physical book that he or she is reading is protected, regardless of where the book came from or how it was finally placed in the hands of the reader.

In addition to answering some of the Fourth Amendment questions, state statutory protections can also provide answers to some of the unaddressed First Amendment questions related to anonymous reading. While many of the lower courts have understood the First Amendment to protect the anonymity of readers, without a definitive resolution by the Supreme Court, the constitutional protection is unresolved. With state regulation affirmatively providing the reader with a right to read anonymously, this lacking constitutional protection is addressed by statutory regulation.

Statutory regulations that protect personal information related to digital books are also likely to be more efficient than finding protection through state constitutions. While states like Colorado have precedential cases law like *Tattered Cover, Inc.* that address the protection of books through hybrid First Amendment and state constitutional privacy protections, many states will not be so lucky. In addition to states not having the necessary constitutional clauses to establish a specific privacy right to their citizens, the time, money, and stress that it takes to argue in front of a state supreme court for a simple restraint on government access to book records can be easily avoided by statutory provisions like California's Reader Privacy Act.[150] More importantly, statutes by their very nature are proactive steps that look to combat societal issues[151] and do not necessarily need to wait for an incident to take effect. Individual users would be better off with the knowledge that their personal information was safe through enacted state legislation, rather than waiting around for a digital book version of *Tattered Cover, Inc.* to allow citizens the opportunity to argue for protective action in front of a court.

States also have the added benefit of being an experimental ground for fine-tuning a law so that the issues may be effectively addressed on a national level. Courts have long recognized the states as a fertile ground for experimental initiatives on new issues facing society.[152] States have the unique ability to address an issue like reader privacy on a micro-level, adjusting to the needs of their citizens as they see fit, so that the federal legislature may see its practical effect and address

---

150. The court noted in *Tattered Cover, Inc.* that the police attempted to execute its first search warrant in April of 2000. *Id.* at 1050. However, it was not until two years later in 2002 that Tattered Cover was affirmatively vindicated in its refusal to hand over the book records to the police. *Id.* at 1044.

151. *See, e.g.*, JOHN C. DERNBACH, RICHARD V. SINGLETON II, CATHLEEN S. WHARTON, JOAN M. RUHTENBERG & CATHERINE J. WASSON, A PRACTICAL GUIDE TO LEGAL WRITING & LEGAL METHOD 91 (3d ed. 2007) (explaining that legislatures write rules "in broad strokes," and statutes are generally written "to cover categories of future situations").

152. *See, e.g.*, Cruzan v. Mo. Dep't of Health, 497 U.S. 261, 292 (1990) (O'Connor, J., concurring) (stating that the appropriate safeguards for liberty interests were left to the "laboratory of the States" (internal quotations omitted)).

the issue on a macro-level. For instance, California's Security Breach Information Act set requirements for companies to inform California's citizens if their unencrypted personal information had been acquired by an unauthorized source.[153] While the Act only legally affected the state government and businesses that obtained personal information about California citizens, companies nation-wide adjusted their business practices and started to notify customers outside the state of California of security breaches as well.[154] Other state legislation and even a federal data accountability law have been proposed as a result of the effectiveness of California's Security Breach Information Act.[155] This same concept of state laws "trickling up" to affect change in other states and at the federal level can occur with effective digital reader privacy laws. As the complexities of technologies and the Internet seem to be a major factor in the failure of adequate protections,[156] starting on a small scale and working up to address the problem seems to be an efficient way to provide answers to some of these complexities.

While some have suggested that a more effective approach to digital reader privacy would directly address the issue at the federal level,[157] starting with state regulations may be a more effective approach. Because federal legislation is difficult and very burdensome to change,[158] allowing state regulations to adopt varying approaches to the problem so that federal legislators can evaluate their positive and negative consequences may be a better long-term solution. This would provide more guidance in crafting a national policy on reader privacy that would in turn create the best opportunity for a national law protecting digital reader privacy to succeed.

B. Acknowledging the Boundaries of State Regulations on the Boundless Internet

Although there are many benefits to protecting digital readers by means of state regulations, there are a few obstacles that must be overcome for state level regulations to fully protect the personal data related to digital books. A concern worth addressing is how state regulations may inadvertently affect the national

---

153. *See* 2002 Cal. Legis. Serv. 1386 (West) (codified as amended at CAL. CIV. CODE §§ 1798.29, 1798.82, (West 2009 & Supp. 2013)); *see also* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 50, at 150 (referring to SB 1386 as the California Security Breach Information Act).

154. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 50, at 150.

155. *Id.*

156. *See* SOLOVE, *supra* note 18, at 223–28.

157. *See* Jennifer Elmore, Note, *Effective Reader Privacy for Electronic Books: A Proposal*, 34 HASTINGS COMM. & ENT. L.J. 127 (2011) (suggesting ECPA be amended to add additional protections for digital books); *see also* Kathleen E. Kubis, Note, *Google Books: Page by Page, Click by Click, Users Are Reading Away Privacy Rights*, 13 VAND. J. ENT. & TECH. L. 217 (2010) (suggesting that new federal statutes should be enacted to address the concerns created by Google Books and other service providers collecting personal data); Schaufenbuel, *supra* note 30, at 199–202 ("[A] federal reader privacy statute would provide nationally consistent and enforceable protection.").

158. *See* Larry E. Ribstein & Bruce H. Kobayashi, *State Regulation of Electronic Commerce*, 51 EMORY L.J. 1, 33 (2002) ("Once federal law is imposed, it is difficult for opponent interest groups to mobilize to change the law.").

practices of Internet companies in order to comply with state regulations. Laws enacted in one state that place a burden on an Internet company may require the company to either find a way to adjust its business's Internet activities within the specific regulation's jurisdiction, or adjust its activities for *all* its customers on a national level.

While this approach may be effective in some circumstances, like California's disclosure requirements in the Security Breach Information Act discussed above,[159] such an approach is to be taken with hesitation. Because of the complexities of how the Internet works,[160] being able to adjust a company's practices for a particular state's jurisdictional authority may be impossible, requiring that an Internet-based company apply a state regulation's mandates to all of its customers. For example, when Utah enacted the Trademark Protection Act, which attempted to regulate and prohibit the use of certain trademarks by Internet companies utilizing keyword advertising schemes,[161] many in the legal community criticized Utah's attempt to regulate all Internet activity through a state regulation.[162] With the fear that Utah's law would effectively strong-arm the national policy on keyword advertising in Utah's favor, some believed that any attempt to establish regulations on keyword advertising "should be the subject of national, not local, policy."[163] Utah's Trademark Protection Act has since been repealed,[164] but the idea of a state's regulation affecting Internet-based activity continues to be a legitimate fear in addressing Internet-related issues on a state level.

In looking at the adverse effects that Utah's Trademark Protection Act could have had, state legislators must tread lightly when attempting to regulate Internet activity. While there is a sharp divide between affecting business practice and prohibiting third-party action, laws that affect Internet activities can have a momentous effect on how businesses interact with not only a particular state but all states in the nation. Laws like California's Reader Privacy Act, however, can be easily confined to their target audience: the state government and third-parties operating within California. Utah's Trademark Protection Act, on the other hand, would have forced changes to online business practices entirely, likely requiring

---

159. *See supra* Part III.A.

160. No one entity "controls" the Internet, and the system works only because each entity that participates within the network expects the flowing data within the Internet's networks wil be processed through a participator's server to reach its required destination. *See* ABELSON ET AL., *supra* note 33, at 301–02. Therefore, it is likely that companies using the Internet would not be able to "control" the transmission of their activities from reaching one particular location, such as preventing their processing data from accessing the servers within a particular state.

161. *See* Trademark Protection Act, 2007 Utah Laws 2215 (repealed 2008).

162. *See, e.g.*, Ron Coleman, *Trademark Lobby Picks One up in Utah*, LIKELIHOOD OF CONFUSION (Mar. 30, 2007, 10:57 AM), http://www.likelihoodofconfusion.com/trademark-lobby-picks-one-up-in-utah/; Eric Goldman, *Utah Bans Keyword Advertising*, TECH. & MKTG. L. BLOG (Apr. 3, 2007, 1:58 PM) http://blog.ericgoldman.org/archives/2007/04/utah_bans_keywo.htm (claiming the Trademark Protection Act amendments would have been subjected to dormant Commerce Clause issues).

163. Coleman, *supra* note 162.

164. *See* Trademark Protection Act Amendments, 2008 Utah Laws 1676 (codified as amended in UTAH CODE ANN. §§ 70–3a -103; -203; -302; -304 to -306; -402; -501 to -502).

Internet companies using key word advertising to adjust their entire design to accommodate the newly enacted Utah law.[165] California's Reader Privacy Act will likely affect how companies like Google and Amazon.com handle government requests for book records by California-based entities, but should have little to no effect on the ways in which these companies choose to distribute their digital book products or respond to requests from other states.

C. Acknowledging the Issue of "Overregulation"

State regulations that protect digital reader privacy should be careful to avoid disrupting the unique characteristics of the Internet. When crafting laws like California's Reader Privacy Act, one significant concern facing state legislators is overregulation. The problem of "overregulation" has been seen by some legal scholars as an issue when state regulation serves as a mechanism to affect national policy.[166] States have the added benefit of adjusting their laws in order to address the needs of their specific population.[167] However, digital book service providers use a universal format to give the same user experience, and same potential for personal information exposure, regardless of a person's geographic location.[168] Because of the uniformity of the system, state laws like California's Reader Privacy Act that require specific action by digital book service providers—like requiring sections of the provider's website be dedicated to displaying disclosure information—could become burdensome if each state individually requires its own specific notice requirement. Because the Internet allows these book service providers to operate universally in every state, the effectiveness of state regulations to address reader privacy may become problematic when overrun with multiple, diverse state mandates. Consequently, this could possibly result in less of an incentive for states to adopt protective measures and less of an incentive for the book service providers to be receptive to supporting regulations. In adopting policies, states must be mindful that the "chilling" effect on reading books that these laws would attempt to prevent could potentially result in a "chilling" effect on digital book service providers' willingness to service customers if state regulations start to overregulate. As states begin to adopt laws similar to California's Reader Privacy Act, they should be aware of the potential for overregulation, especially when dealing with service providers that distribute through the Internet.

---

165. *See* Goldman, *supra* note 162 ("The practical reality is that every advertiser, wherever they are located, would have to check Utah's registry before buying keywords that might contain a trademark of a competitor . . . .").

166. Ribstein & Kobayashi, *supra* note 158, at 34–35 (addressing the overregulation problem in state regulations addressing electronic commerce).

167. For instance, California's Reader Privacy Act was intended to address "*Californians*[*'*] increasing [reliance] on online services to browse, read, and buy books." *See* S. RULES COMM., *supra* note 99 (emphasis added).

168. For instance, Google Books was implemented in order to fulfill the company's vision of "people *everywhere* being able to search through all of the world's books to find the ones they're looking for." *Google Books History*, GOOGLE, http://books.google.com/googlebooks/history.html (emphasis added).

CONCLUSION

Reader privacy concerns are nothing new, but we are beginning to face new challenges as books transition into cyberspace. As service providers increase their capabilities for tracking and recording personal information related to their users' reading habits, there is a fear that third parties could legally use this information without knowledge to the readers. While state initiatives and judicial practices have traditionally protected physical books, the uncertainty of laws protecting online data, as well as a heightened craving for vast quantities of data, have called into question the current state of privacy protections related to digital books.

State regulations can be an effective means by which to start a protective regime against third-party access to data related to digital readers. California's Reader Privacy Act, in particular, is the first step in tackling the issue of reader privacy in the digital landscape. Targeting digital books specifically to establish reader protections will assure the closure of the legal loopholes faced in the current privacy environment. Should more states follow California's lead in "experimenting" with digital reader privacy protections, the country may begin to develop a national policy in digital reader privacy that can result in federal laws and regulations. The current state of reader privacy in digital books remains in flux; however, California's Reader Privacy Act could be as revolutionary and influential to privacy protection as digital books are to the future of literary enjoyment.