DOWN THE RABBIT HOLE: E-BOOKS AND USER PRIVACY IN THE 21ST CENTURY

ELIZABETH HENSLEE†

The rabbit-hole went straight on like a tunnel for some way, and then dipped suddenly down, so suddenly that Alice had not a moment to think about stopping herself before she found herself falling down a very deep well... There were doors all round the hall, but they were all locked; and when Alice had been all the way down one side and up the other, trying every door, she walked sadly down the middle, wondering how she was ever to get out again.¹

I. INTRODUCTION:

A. Wondering How We Are Ever To Get Out Again

When Amazon.com released the Kindle in 2007, the first lot sold out in five and a half hours, and remained out of stock for several months.² Since that time, e-readers and e-books have been embraced by the public offering light weight alternatives to tangible books (the first Kindle weighed 10.3 ounces) with seemingly limitless access to a virtual library.³ But, it appears, the e-reader public may have fallen down a “very deep well.”

In October of 2014, it was reported that Adobe was using their e-book software to spy on their users.⁴ Adobe gathered data on e-books in the user’s library—including pages that were read—and transmit-

† B.A., Emory University 2004; J.D., Florida A & M University College of Law, 2008; M.L.I.S., University of South Florida, 2015. Thank you to the faculty in the Masters in Library and Information Science program at the University of South Florida. Specifically, thank you to Professor Diane Austin for her all of her help and encouragement. Thank you to Dr. Kathleen de la Peña McCook for her guidance and support. I could not have done it without you. Finally, thank you to my husband, Bill Henslee, who constantly listened, calmed my nerves, and supported me even when I wanted to give up.

ted that data in unencrypted, plain text back to their servers. Adobe used this software in conjunction with Overdrive, a popular e-book lending system used with libraries. When confronted by the American Library Association, Adobe defended its system stating, "all data collection in Adobe Digital Editions is in line with the end user license agreement and the Adobe Privacy Policy." Overdrive, the e-book lending system used in many libraries, received publicity earlier in 2011 by contracting with Amazon.com and requiring users to register accounts to check out e-books formatted for a Kindle device. Amazon used this information the same way it treated information from retail sales, and used the data about user reading habits to market its own services and products. Further, all of this information can be sold to a third party in almost every jurisdiction in the United States.

In 2012, Google was sued under breach of contract and fraud claims by users of Android devices who downloaded at least one application through Google Play. Google Play is the primary source of Android applications, and also serves as the e-reader for Google Books. While the claim was dismissed on July 15, 2015 for failure to allege injury-in-fact, it remains evidence of consumers' fear of disclosing too much information through their web-browsing behavior. In this litigation, Google faced claims that its new privacy policy jeopardizes user privacy by exposing the names, email addresses, and geographic locations of users. The lawsuit was filed in 2012 as a result of Google changing its privacy policy to unify its user data through a variety of Google supported platforms like Google Play, Gmail, Google Maps, and YouTube. Effectively, users are concerned with the amount of personal information that Google can collect without express user consent.


11. Id. at *1.
The privacy issue with e-readers is not limited to vendors monitoring users' reading and online habits. In 2009, Amazon received attention when it remotely removed some digital copies of George Orwell's "1984," from users' Kindle devices when they realized that they did not possess a valid license for the work.12 Along with the digital copy of the book, readers lost their notations in the margins of the novel and any other work that had been saved on their electronic version of the book.13 This illustrated that not only is everything monitored via user sign-in, but third party vendors can and will remove anything they want from your e-reader. These actions by suppliers of e-books have created user awareness of potential privacy violations. This article will look at current federal privacy protection, state privacy protection, the American Library Association's stance on patron privacy, licensing and the privacy policies of vendors. Finally, this article will comment on the need for change to create meaningful digital privacy laws that protect users' privacy rights in an online environment.

II. FEDERAL PRIVACY PROTECTION:

"If everybody minded their own business . . . the world would go around a great deal faster than it does."14

The First Amendment's Free Speech Clause has been interpreted to protect private reading.15 "The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, [and among others] the right to read . . ."16 In 1965, when the Court struck down a statute that required post offices to refuse delivery to foreign-mailed communist propaganda unless the addressee specifically requested the material, Justice Brennan equated the right to free speech with the right to private reading. He stated:

It is true that the First Amendment contains no specific guarantee of access to publications. However, the protection of

---


13. Stone, supra note 12 ("Justin Gawronski, a 17-year-old from the Detroit area, was reading '1984' on his Kindle for a summer assignment and lost all his notes and annotations when the file vanished. They didn't just take a book back, they stole my work[,] he said").

14. Carroll, supra note 1, at 32.


the Bill of Rights goes beyond the specific guarantees to protect from congressional abridgment those equally fundamental personal rights necessary to make the express guarantees fully meaningful. I think the right to receive publications is such a fundamental right. The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers.\textsuperscript{17}

Supreme Court precedent also finds support for First Amendment protection of private reading in \textit{United States v. Rumley,}\textsuperscript{18} when the government sought to compel a bookstore owner to disclose the names of customers who had purchased political books.\textsuperscript{19} In a concurring opinion, Justice Douglas equated a publisher disclosing the identities of its customers to the "beginning of surveillance of the press."\textsuperscript{20} He further stated:

Then the spectre of a government agent will look over the shoulder of everyone who reads. The purchase of a book or pamphlet today may result in a subpoena tomorrow. Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular what the powers-that-be dislike. When the light of publicity may reach any student, any teacher, inquiry will be discouraged. The books and pamphlets that are critical of the administration, that preach an unpopular policy in domestic or foreign affairs, that are in disrepute in the orthodox school of thought will be suspect and subject to investigation. The press and its readers will pay a heavy price in harassment. But that will be minor in comparison with the menace of the shadow which government will cast over literature that does not follow the dominant party line.\textsuperscript{21}

Private reading promotes First Amendment values by advancing free expression, permitting access to controversial ideas, and promoting an individual's ability to develop private thoughts.\textsuperscript{22} Monitoring

\textsuperscript{17} Lamont, 381 U.S. at 308 (Brennan, J., concurring) (citations omitted).
\textsuperscript{18} 345 U.S. 41 (1953).
\textsuperscript{19} Rumley, 345 U.S. at 47-48.
\textsuperscript{20} Id. at 57 (Douglas, J., concurring).
\textsuperscript{21} Id. at 57-58.
individuals’ reading may deter them from reading controversial materials and may create a chilling effect detrimental to the preservation of First Amendment values. Further, surveillance of private reading causes concern that freedom of inquiry will be stifled. Freedom of inquiry is fundamental to the American democratic society, and surveillance of reading materials may quell participation in public debate and participation in self-governance.

III. STATE PRIVACY RIGHTS:

“You used to be much more . . . ‘muchier.’ You’ve lost your muchness.”

While private reading is an important aspect of a democratic society, it is not completely protected. It is protected through a patchwork of state laws applicable to libraries ensuring patron privacy. Forty-eight states and the District of Columbia have laws that protect the confidentiality of library records, and two states have opinions from their respective Attorney General’s Office protecting the confi-

Rev. 387, 419 (2008) [hereinafter Richards I] (“Intellectual exploration must be private insofar as the act of reading must be free from interference by outsiders, and also unwatched, lest the surveillance of others chill the development of new thoughts in the direction of the bland and the mainstream”); Marc Jonathan Blitz, Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and a First Amendment Theory for an Unaccompanied Right to Receive Information, 74 UMKC L. Rev. 799, 818 (2006) (“information-seeking by itself, even when unconnected to any specific willing speaker or any specific instance of speech, deserves to be valued and constitutionally-protected because of its crucial role in promoting core First Amendment values”).

23. Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1945-46 (2013) [hereinafter Richards II] (“Intellectual-privacy theory suggests that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy—protection from surveillance or interference—is necessary to promote this kind of intellectual freedom”).

24. Richards I, supra note 22, at 403-04 (“The knowledge that others are watching (or may be watching) tends the preference of the individual towards the bland and the mainstream. Thoroughgoing surveillance, whether by public or private actors, has a normalizing and stifling effect”).


State restrictions on public discourse can be inconsistent with democratic legitimacy in two distinct ways. To the extent that the state cuts off particular citizens from participation in public discourse, it pro tanto negates its claim to democratic legitimacy with respect to such citizens. To the extent that the state regulates public discourse so as to reflect the values and priorities of some vision of collective identity, it preempts the very democratic process by which collective identity is to be determined.

Id.

26. ALICE IN WONDERLAND (Walt Disney Pictures 2010).
dentiality of library records.27 The language and level of protection varies by state, but in almost every state, the statutes are specific to libraries and do not apply to third-party lenders that distribute e-books.28 As a result of the e-book, the state privacy laws have lost their “muchness.”

These safeguards are in place to protect citizens from their reading records being released. Until the advent of the e-book and e-reader, the only way an individual’s personal reading records were obtainable was through the public library system, which maintains a database of patron records. By protecting private reading within the safe haven of a library, people have traditionally been free to explore unpopular ideas, threats to social norms, and delve into the depths of their creativity without the fear of government surveillance.29 Under Blitz’s theory, libraries provide an important social function because they allow people the ability to explore more ideas, concepts, and theories through private reading than they could through action alone.30 This guarantee of privacy reduces the social cost associated with these intellectual endeavors.31

The purpose and practice of the state laws and policies in place to protect reader privacy are circumvented by the emergence of the e-book and e-reader. Simply put, the privacy laws do not attach to a virtual library the same way they attach to the physical library. Commercial e-book providers are third party vendors as opposed to libraries, and the statutes are specifically designed to apply to public libraries even though the contents of reading records would be similar. The distinction between the records, other than the possessor of the records, is that the records kept by e-book providers (Adobe, Amazon, Barnes & Noble, and Google) are much more detailed. These records include what was downloaded, the search to locate the download, how long a page was examined, and notations made in the margins.32

27. See infra Appendix A.
28. See infra Appendix A; see also Meredith Mays Espino, Sometimes I Feel Like Somebody’s Watching Me . . . Read? A Comment on the need for Heightened Privacy Rights for Consumers of Ebooks, 30 J. INFO. TECH. & PRIVACY L. 281, 293-95 (2013). The exceptions are California, which has specific legislation designed for e-books and Arizona and Missouri where the library statutes were amended to specifically include e-books and e-readers. CAL. CIV. CODE § 1798.90 (West 2012); ARIZ. REV. STAT. ANN. § 41-151.22 (2013); MO. REV. STAT. § 182.817 (2014).
29. See Ard, supra note 6, at 10-11; Blitz, supra note 22, at 820.
30. Blitz, supra note 22, at 820.
31. Id. “It is not only the book collection of a public library that frees individuals from reliance on their external community, but also its walls and privacy policies.” Id.
IV. THE LIBRARY AND PRIVACY RIGHTS:

"Who are YOU?" said the Caterpillar . . .

'I—I hardly know, sir, just at present—at least I know who I WAS when I got up this morning, but I think I must have been changed several times since then.'\textsuperscript{33}

The library has undergone many changes since its inception. Previously a brick and mortar institution with strong ties to its community, it has now made the transition to the digital world. Even though the shape and structure of the library has changed, the library has a very strong commitment to privacy regardless of format.

Privacy is of vital philosophical importance to the American library system. The American Library Association ("ALA") "strongly recommends" that libraries "formally adopt a policy that specifically recognizes its circulation records and other records identifying the names of library users to be confidential."\textsuperscript{34} In the ALA Code of Ethics, Article III states, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted."\textsuperscript{35} In Privacy: An Interpretation of the Library Bill of Rights, the ALA states, "[i]n a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others."\textsuperscript{36}

The Internet has transformed the way that individuals read. Digitized books and e-reading devices have become a dominant form of reading.\textsuperscript{37} These new digital resources bring with them new privacy concerns.\textsuperscript{38} "In the United States, the reading habits of those who read traditional paper-bound books are heavily protected, while readers of electronic books are given little to no privacy protection."\textsuperscript{39} As opposed to the physical-lending model where the library controls the patrons' records, with electronic books, the digital format is intermedi-

\textsuperscript{33} Carbull, supra note 1, at 23.
\textsuperscript{38} Theresa Chmara, Privacy and E-Books, Knowledge Quest, *64-67 (2012), http://www.ala.org/asl/ecollab/kq/v40n03.
\textsuperscript{39} Elmore, supra note 32, at 128 (footnote omitted).
ated by third parties. These third parties, or non-library actors, are not restricted by the same stringent privacy policies and have broad discretion with how they collect and exploit the records of patrons' activities. Unlike libraries that take administrative and technical precautions to disassociate the identities of patrons from their reading history, the third-party vendors store user information for extended periods of time and use it for marketing and financial gain. Effectively, because of the licenses with third-party vendors, the library privacy policy may not apply to e-books, and libraries that loan tablets or e-readers likely violate the ALA principles articulated above.

V. LICENSING:

"I can't explain myself . . . because I am not myself, you see?"

The e-book purchasing model is different than purchasing a physical book. When a user purchases an e-book from a retailer, the payment is for a license to read the book as opposed to ownership in a physical copy of the book. This license can be revoked, because it is only permission to use the intellectual property for a period of time. When an owner licenses its intellectual property, it is often coupled with a privacy policy dictating how one may appropriate or use the intellectual property. Each company that sells electronic books has a unique privacy policy that tells consumers how they may use the intellectual property and how their use of the property may be used by the company. Merchants have a financial interest in using a consumer's information. As Julie Cohen writes, "the new information age is turning out to be as much an age of information about readers as an age of information for readers." Companies generate and store this

40. Ard, supra note 6, at 3.
42. Ard, supra note 6, at 13. "In the information economy, the probative thoroughness of the data is what makes it commercially valuable." Id.
43. Chmara, supra note 38, at *66.
45. Ard, supra note 1, at 23.
47. Espino, supra note 46, at 283-84.
48. Julie E. Cohn, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, 28 CONN. L. REV. 981, 1013 (1996). "Reader profiles are valuable to marketers precisely because they disclose information about the reader's tastes, preferences, interests, and beliefs." Id.
49. Cohn, supra note 48, at 981.
data to put it to commercial use, either by improving personalized services to the consumer or by selling it to a third party for profit.50

The "privacy policies" of many e-book vendors protect the companies' interest and do not protect the readers' privacy. Some of the most popular vendor policies are discussed below.

VI. READERS: KINDLE, NOOK, AND IPAD:

A. Amazon and Kindle

Amazon collects data from consumers to "personalize and continually improve [the] Amazon experience."51 This consumer data comes in five types: (1) information that consumers give them; (2) automatic information (like "cookies"); (3) mobile information (like an individual's location and an individual's unique identifier on their mobile device) so they can provide location based services; (4) e-mail communications that include a confirmation when any email is opened by an individual from Amazon; and (5) information from other sources (examples include delivery and address information from Amazon carriers or other third parties, purchase information, page view information, and credit history). The information can be shared with affiliated businesses that Amazon does not control; third-party service providers; other businesses that use Amazon.com for promotional offers; business transfers; "when [Amazon.com] believe[s] release is appropriate to comply with the law; enforce or apply [Amazon.com's] Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon.com, [its] users, or others."52 Amazon currently tracks any searches, purchases, participant questionnaires, and communications with customer service.53 All Amazon "Instant Video" services, "Wish Lists," discussion boards, and reviews are also tracked by Amazon.54 Information such as name, address, phone numbers, credit card information, email addresses of friends, and people whom purchases have been shipped to are also tracked and stored.55

In terms of information gleaned from the Amazon Kindle, Amazon collects data on products viewed and/or searched for on the device and

50. Id.; Neil M. Richards, The Dangers of Surveillance, 126 HARY. L. REV. 1934, 1938 (2013). "[The Internet is] free on its face to use, but is in reality funded by billions of transactions where advertisements are individually targeted at Internet users based upon detailed profiles of their reading and consumer habits." Id.
52. Amazon.com Privacy Notice, supra note 51.
53. Id.
54. Id.
55. Id.
associates this information with the user’s Amazon account.\textsuperscript{56} Amazon also stores the last page read and may store annotations, highlights, and markings.\textsuperscript{57} Based on Amazon’s privacy policy, it can be inferred that a subpoena or other court order is not necessary for Amazon to share this information with law enforcement or other third parties if they deem it will “protect the rights, property, or safety of Amazon.com, [their] users, or others.”\textsuperscript{58} This allows Amazon.com and not a court of law to determine when and how much information about an individual is given to third parties when it is requested—a potentially dangerous situation for civil liberties.

\section*{B. Barnes & Noble and Nook}

Effective August 2, 2015, Barnes & Noble updated their privacy policy permitting them to collect personal information which includes: name, email address, billing address, shipping address, phone number, credit card number/bank information, date of birth, and other “persistent identifiers” which replaced the previously enumerated: “student/faculty identification number, financial aid number, driver license number, information about courses enrolled in or taught, program of study.”\textsuperscript{59} In addition to these types of “personal identifiers” Barnes & Noble automatically collects “usage information” including items browsed, “purchased, downloaded, read, watched, [or] accessed . . .”\textsuperscript{60} Further, the web server logs information such as the IP address, date, time of use, and the Apps and devices of the user including device registration, operating system, settings, usage, and downloads. They also collect a user’s geographical location.\textsuperscript{61} Barnes & Noble claims that this personal information is used to “provide you with a superior customer experience.”\textsuperscript{62} Barnes & Noble reserves the right to retrieve information about their customers from other third parties.\textsuperscript{63} Their policy specifically states that if their goods and services are accessed through a Microsoft account, then Microsoft “may share” the user’s personal information and the two companies will

\textsuperscript{57} \textit{Id.}
\textsuperscript{58} Amazon.com Privacy Notice, \textit{supra} note 51.
\textsuperscript{60} Barnes & Noble Privacy Policy, \textit{supra} note 59.
\textsuperscript{61} \textit{Id.}
\textsuperscript{62} \textit{Id.}
\textsuperscript{63} \textit{Id.}
share information about the user to provide “products and services . . . related to your Device.” Barnes & Noble specifically outlines in bold faced, capital letters that they “do[ ] not sell or rent your personal information to third parties.” Like Amazon, Barnes & Noble may release personal information to third parties “when [they] determine, in [their] judgment, that it is necessary to (a) comply with the law, regulation, legal process, or enforceable governmental request; (b) enforce or apply the terms of any of our policies or user agreements; or (c) protect the rights, property or safety of Barnes & Noble, our employees, our customers, users, or others.”

Like Amazon, this takes the decision of when and how to comply with a third party’s request for personal information away from a court of law and places it within Barnes & Noble’s discretion, which is a dangerous precedent.

C. Apple and iPad

Apple’s Privacy Policy was updated on September 17, 2014. Apple points out that a user is not “required to provide the personal information . . . but, if you chose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have.” Included in the personal information that Apple collects is: name, mailing address, phone number, email address, contact preferences, and credit card information. If users provide information about their friends, then Apple will also collect the information about those individuals. In addition to using the information to verify identity and communicate with customers, Apple may use the “information for internal purposes such as auditing, data analysis, and research to improve Apple’s products, services, and customer communications.” Apple also collects “non-personal information” that ironically tells more about a user than the “personal information” collected. The “non-personal information” includes: “occupation, language, zip code, area code, unique device identifier, referrer URL, location,” and time zone. Customer activities on Apple’s website, iCloud services, and iTunes are also collected and aggregated, or

64. Id.
66. Id.
67. Id.
68. Id. “When you share your content with family and friends using Apple products, send gift certificates and products, or invite others to participate in Apple services or forums, Apple may collect the information you provide about those people such as name, mailing address, email address, and phone number.” Id.
69. Id.
70. Id.
stored in the collective, for Apple’s use.\textsuperscript{71} Search queries are stored, and they “may” collect data about how the device and applications are used.\textsuperscript{72} Cookies (and other technologies that track a user’s Internet behavior “such as pixel tags and web beacons”) are used to “understand user behavior”—this is also considered non-personal information.\textsuperscript{73} Apple also discloses this data to third parties when they “determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.”\textsuperscript{74} The amount of time that the information is retained is vague under Apple’s policy. They state the information will be retained “for the period necessary to fulfill the purposes outlined[.]”\textsuperscript{75} These clauses are particularly troubling because the time Apple retains the information is unclear and the information can be distributed to a third party without the user’s consent as long as Apple deems it “appropriate.”\textsuperscript{76}

VII. DIGITAL BOOKS: ADOBE AND GOOGLE:

A. ADOBE

Adobe Digital Editions privacy policy states that they collect the following information about reader behavior: (1) the duration for which the book was read; (2) percentage of the e-book read; (3) information provided by e-book providers relating to the e-book the reader had purchased including, date of e-book purchased/downloaded, distributor ID and Adobe Content Server Operator URL, and the metadata of the book (title, author, language, publisher list price, and ISBN number).\textsuperscript{77} After it was exposed in October of 2014 that Adobe was sending the user data unencrypted and in plain text back to Adobe their policy was changed so that the information was sent “via secure transmission using HTTPS.”\textsuperscript{78} Adobe claims that they do not “share any personally identifiable information” but “may share anonymous aggregated information to eBook providers to enable billing under the applicable pricing model.”\textsuperscript{79} While Adobe has recently

\textsuperscript{71} Id.
\textsuperscript{72} Id.
\textsuperscript{73} Id. “We treat information collected by cookies and other technologies as non-personal information. However, to the extent that Internet Protocol (IP) addresses or similar identifiers are considered personal information by local law, we also treat these identifiers as personal information.” Id.
\textsuperscript{74} Id.
\textsuperscript{75} Id.
\textsuperscript{76} Id.
\textsuperscript{78} Id.
\textsuperscript{79} Id.
changed their policy to “secure” user data to ensure some form of user privacy, they are still using the data for marketing purposes to find out vast amounts about their customers and use that data for their own purposes. There is nothing that prevents them from selling this data to a third party.

B. Google and Google Books

Google Play is a digital distribution platform developed by Google that is used as a digital media store offering music, magazines, books, movies, and television programs. Google Books is the world’s largest collection of e-books.80 Superficially, the Google Privacy Policy seems to be the most protective of user data. Google Play does not share personal information with third parties “except in narrow circumstances.”81 However, if a user is logged in and synchronizes Google Play with the account from the reseller or developer of the book, then Google will share information about all of the user’s library shelves, titles, annotations, and last five pages read with the reseller or developer.82 “The application developer’s or reseller’s treatment of that information (and any other information you submit to the reseller or application developer directly) will be governed by the application developer’s or reseller’s privacy policy, not [Google’s].”83 In addition, the information gathered by Google Play includes query terms, page requests, IP address, browser type, browser language, the date and time of request, and cookies that portray information about a user’s Internet behavior.84 The information is used to improve services, for security, and to look at aggregate user trends.85 Specific information about a user’s reading history, like a list of books purchased, are kept from credit card companies, but released to the rightsholders (licensors) of the books, and kept by Google for an undetermined amount of time.86 Google specifically addresses book privacy laws, they state:

Some jurisdictions have special “books laws” saying that this information is not available unless the person asking for it meets a special, high standard such as proving to a court

82. Id.
83. Id.
84. Id.
85. Id.
86. Id. “We limit the information (such as books titles) we provide to credit card companies, and enable you to delete purchased books from your Google Account. However, you will not be able to delete the record of your purchase transaction (including the title of the book) from your Checkout account history.” Id.
that there is a compelling need for the information, and that
this need outweighs the reader's interest in reading anony-
mously under the United States First Amendment or other
applicable laws. Where these "books laws" exist and apply to
books on Google Play, we will raise them. 87

While the knowledge of special "books laws" and awareness of
First Amendment considerations of "reading anonymously" is encour-
aging, Google is only responsible for what they do with the informa-
tion, they cannot control what other resellers or developers do with a
user's information. Unfortunately, they are contractually bound to
share the information with the other resellers or developers who may
sell, distribute, or release that information at their companies'
discretion.

VIII. CALL FOR CHANGE
A. FEDERAL READING PRIVACY LAW:

"I almost wish I hadn't gone down that rabbit-hole—and yet—

. . . ."88

Three states have enacted laws that are designed to protect the
privacy of digital records obtained through an e-reader or e-book ven-
dor. 89 California enacted the Reader Privacy Act 90 that protects read-
ing records from being accessed by government or third parties
without proper justification and transparency. 91 The California stat-
ute protects information about the books that Californians read,
browse, or purchase from electronic services or online booksellers.
Government entities must obtain a court order and give the book
seller or provider "reasonable notice of the proceeding to allow the pro-
vider the opportunity to appear and contest the issuance of the or-
der." 92 Civil actions must show that "the person or entity seeking
disclosure has a compelling interest" 93 and "that the personal infor-
mation sought cannot be obtained by the person or entity seeking dis-
closure through less intrusive means." 94

California's Reader Privacy Act served as a model for New
Jersey's Reader Privacy Act that was vetoed in 2014 by Governor

87. Id.
88. CARROLL, supra note 1, 17.
89. CAL. CIV. CODE § 1798.90 (West 2012); ARIZ. REV. STAT. ANN. § 41-151.22
(2013); MO. REV. STAT. § 182.817 (2014).
90. Id. CIV. CODE § 1798.90 (West 2012).
91. Id.
92. CAL. CIV. CODE § 1798.90(c)(1)(D).
93. CAL. CIV. CODE § 1798.90(c)(2)(B)(i).
94. CAL. CIV. CODE § 1798.90(c)(2)(B)(ii).
Chris Christie and has been reintroduced in the New Jersey Legisla-
ture.\textsuperscript{95} The New Jersey Reader Privacy Act contains similar language
requiring government entities to obtain a court order\textsuperscript{96} that may be
issued only if “probable cause exists to believe the personal informa-
tion requested is relevant and material to an ongoing criminal investi-
gation[,]”\textsuperscript{97} and that law enforcement has a “compelling interest”\textsuperscript{98}
and the “information cannot be obtained through [a] less intrusive
means.”\textsuperscript{99} Like the California Reader Privacy Act, the New Jersey
Reader Privacy Act requires that “the provider [have] the opportunity
to appear and contest the issuance of the order.”\textsuperscript{100} The same lan-
guage is used for civil actions.\textsuperscript{101}

Arizona revised their state privacy statute in 2013 to read that “a
library or library system supported by public monies shall not allow
disclosure of any record or other information, including e-books, that
identifies a user of library services as requesting or obtaining specific
materials or services or as otherwise using the library.”\textsuperscript{102}

Additionally, in 2014 Missouri amended their state statute to de-
fine “digital resource or material” and “e-book” and added them to the
enumerated list of protected items in the definition of “library mate-
rial” that a patron may use, borrow, or request.\textsuperscript{103} The Missouri stat-
ute also provides that any “third party contracted by a library that
receives, transmits, maintains, or stores library records” shall not re-
lease or disclose a library record or portion of a library record except to
the person identified in the record by a court order.\textsuperscript{104}

Nevada and Minnesota do not specifically protect online reading
records, but prohibit internet service providers (“ISPs”) from releasing
customers’ private information unless the customer gives permission
to disclose that information.\textsuperscript{105} Both Minnesota and Nevada prohibit
disclosure of personally identifying information, but Minnesota goes a
step further and requires ISPs to get permission from subscribers
before disclosing information about the subscriber’s online user
behavior.

The difficulty with these state privacy laws is that they only apply
to the residents of those states. In addition, they are superseded by

\textsuperscript{96} Id.
\textsuperscript{97} Id.
\textsuperscript{98} Id.
\textsuperscript{99} Id.
\textsuperscript{100} Id.
\textsuperscript{101} Id.
\textsuperscript{103} Mo. Rev. Stat. § 182.815 (2014).
\textsuperscript{104} Mo. Rev. Stat. § 182.817 (2014).
the Patriot Act and Freedom Act of 2015, which means that the protections do not apply to the federal government.\textsuperscript{106} Broad protection is necessary, and a federal "Electronic Consumer Privacy Act" should be implemented to ensure protection of digital reading records.

There is already some form of federal protection to electronic records created by the Electronic Communications Privacy Act ("ECPA")\textsuperscript{107} and federal protection of video tape rental records contained in the Video Privacy Protection Act ("VPPA").\textsuperscript{108} These two acts provide the structure for a comprehensive federal statute that protects electronic records that disclose Internet search histories or other electronic information that portrays a detailed picture of Internet user behavior.

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The ECPA\textsuperscript{109} contains three titles: Title I, the Wiretap Act,\textsuperscript{110} Title II, the Stored Communications Act,\textsuperscript{111} and Title III, the Pen Register Statute.\textsuperscript{112} Enacted in 1986, the ECPA was a response to technological change.\textsuperscript{113} Similar to the disparity between the privacy protections of traditional print sources in a library and the lack of protection for electronic readers, the ECPA was passed to increase protection of electronic mail.\textsuperscript{114} When the ECPA was passed, there were


Just a few years ago, our nation's communications networks, while extensive, were relatively simple in form. The mails, the telegraph systems, the telephone, and radio communications each played a role; but those roles were distinct from one another, and not too hard to understand. Those simple days are gone forever. Today's systems of electronic communication envelop our society in an invisible web, complex in structure and pervasive in scope. We entrust, each day, to that network of electrons a wide spectrum of information, from the latest stock quotations to our most personal revelations. But the uneasy realization is growing that someone else may be listening. Modern technology, which has given us these dazzling new means of communications, has also opened up opportunities for new and more intrusive forms of snooping.

\textit{Id.}

\textsuperscript{114} S. REP. No. 99-541 at 1, reprinted in 1986 U.S.C.C.A.N. 3555, 3555
prohibitions in place to protect oral and wire communications, but there was no protection for electronic communications.115 Under the Wire and Electronic Communications Interception and Interception of Oral Communications Act of 1968, “oral” and “wire” communications were protected.116 Electronic mail was neither an “oral communication,” nor could it be subject to “aural acquisition,” which placed it outside of protected activity. The purpose of the ECPA was “to protect against the unauthorized interception of electronic communications.”117

In context of the ECPA, the Wiretap Act and the Stored Communications Act are applicable to ISPs. The Wiretap Act applies to the interception of “wire, oral, and electronic communications.”118 The Stored Communications Act applies to “stored wire and electronic communications and transactional records.”119 The ECPA creates multiple levels of protection for different forms of electronic communication. The Wiretap Act requires information about electronic communication (e-mail) requested by law enforcement to have a probable-cause-based warrant.120 However, e-mail and data held by ISPs under the Stored Communications Act are treated under a separate standard, only requiring the “conduct be authorized by the person or

---


_id_.

115. Wire and Electronic Communications Interception and Interception of Oral Communications, Pub. L. No. 90-351, 82 Stat. 197 (1968) (current version at 18 U.S.C. §§ 2510-2522 (2012)). The original act was passed to satisfy the procedural and substantive requirements articulated by the Supreme Court in two cases: Katz v. United States, 389 U.S. 347, 353 (1967) (holding that wiretapping a private conversation in a phone booth was a search under the Fourth Amendment), and Berger v. New York, 388 U.S. 41, 63 (1967) (finding unconstitutional a state statute which authorized eavesdropping based on an ex parte order of the Court).

116. 18 U.S.C. § 2510(4) (defining “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”).


119. _Id_.

120. See 18 U.S.C. § 2516 (2012) (authorizing a Federal judge of competent jurisdiction to authorize interception of wire, oral, or electronic communications that must be in conformity with § 2518—effectively creating a probable cause based warrant requirement).
entity providing a wire or electronic service.”\textsuperscript{121} This gives ISPs considerable flexibility when email or data is in storage.\textsuperscript{122}

There are multiple problems with the treatment of electronic communications under the ECPA. When it was created in 1986, there was no vision of the current level of electronic communication and electronic storage.\textsuperscript{123} The use of electronic mail was primitive, used primarily by businesses and academics, and the average American home had not yet embraced electronic mail or electronic data storage.\textsuperscript{124} The exceptions for electronic storage were, and continue to be, based on that primitive technology. This creates problems for electronic privacy protection in two basic ways: (1) exceptions for the ISPs, and (2) automatically generated information that is not considered “content.”

1. Exceptions for ISPs

Under the ECPA, there are two prominent exceptions for ISPs. The first exception is consent\textsuperscript{125} through the privacy policies and terms of service agreements for ISPs.\textsuperscript{126} This exception is the one most commonly used with electronic readers, because through the privacy policies of electronic book providers, users are allowing their information to be intercepted and stored.\textsuperscript{127} The second exception is

\begin{itemize}
\item \textsuperscript{121} \citenum{f121}
\item \textsuperscript{122} \citenum{f122}
\item \textsuperscript{123} \citenum{f123}
\item \textsuperscript{124} \citenum{f124}
\item \textsuperscript{125} \citenum{f125}
\item \textsuperscript{126} \citenum{f126}
\item \textsuperscript{127} \citenum{f127}
\end{itemize}

---

\textsuperscript{121} 18 U.S.C. § 2701(c)(1) (2012).

\textsuperscript{122} For a detailed description of the levels of protection, see Deirdre Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 GEO. WASH. L. REV. 1557 (2004) (outlining the history of the ECPA, breaking down the structure of the ECPA, and following the ECPA to the difficulties with privacy expectations in electronic records using remote storage); see also Bruce E. Boyden, Can a Computer Intercept Your Email?, 34 CARDOZO L. REV. 669, 669 (2012) (arguing that “automated processing that leaves no record of the contents of a communication does not violate the ECPA, because it does not ‘intercept’ that communication within the meaning of the Act”).

\textsuperscript{123} Electronic Communications Privacy: Hearing on S. 1667, supra note 113.

\textsuperscript{124} Id.: There are currently several hundred million messages sent annually, and this figure will grow into the tens of billions in less than a decade. It is reasonable to assume that during the next decade electronic mail will become a regular part of the communications mix that a substantial number of Americans use in the workplace and increasingly at home as well.


\textsuperscript{127} Electronic Communications Privacy Act, 18 U.S.C. § 2511(2)(d) (no liability “where one of the parties to the communication has given prior consent to such interception”). Courts have interpreted this to excuse ISP providers from liability under the
information stored through the “ordinary course of its business” for an ISP. Under the “ordinary course of business” exception, ISPs and vendors must show that the interception of the information facilitated the communication service or that it was incidental to the functioning of the provided communication service. This permits ISPs to contract with advertising companies to conduct research on what online advertising will most likely engage the user as long the ISP's access is no different than the access it would have in the ordinary course of providing internet services.

2. Automatically Generated Content

In addition, the Wiretap Act has not been found to create a privacy interest in automatically generated information (like geolocation). Automatically generated information is not “content” defined by the Wiretap Act. This information can contain “the source desti-

ECPA for turning over information to third parties as long as the users' consent to the terms and conditions in the click through license. See Valentine v. WideOpen W. Fin., LLC, 288 F.R.D. 407, 412 (N.D. Ill. 2012) (noting that "consent is an exception to ECPA liability"); Kirch v. Embarq Mgmt. Co., No. 10–2047–JAR, 2011 WL 3651359, at *7 (D. Kan. Aug. 19, 2011) (explaining that language contained in the ISP's privacy policies and terms of service agreements excluded the conduct from the "category of 'unlawful interceptions'").

128. The Electronic Communications Privacy Act, 18 U.S.C. § 2510(5)(a), exempts from the definition of "device":

any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigatory or law enforcement officer in the ordinary course of his duties[.]

Id.

129. See Kirch, 2011 WL 3651359, at *9 (noting that data that was intercepted only incidental to its provision of internet service fell under the 18 U.S.C. § 2510(5)(a)(ii) exception).

130. See id. (holding that the ISP was exempted under the ECPA for activities conducted in ordinary course of business when it contracted with an advertising company to generate optimized advertisement).

131. The Northern District of California found that users of iPhones did not have a privacy interest in geolocation data that was automatically generated by the technology. In re iPhone Application Litigation, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) (discussing "content" in the context of the Wiretap Act: "[T]he Court concludes under the current version of the statute, personally identifiable information that is automatically generated by the communication but does not compromise the substance, purport, or meaning of that communication is not covered by the Wiretap Act.")

132. United States v. Reed, 575 F.3d 900, 916 (9th Cir. 2009) (finding that the "source, destination, duration, and time of a call" were not "content" for the purposes of the Wiretap Act, because they contain "no 'information concerning the substance, purport or meaning of [the] communication'") (quoting 18 U.S.C. § 2510(5)).
nation, duration, and time” of a phone call. Troublingly, through the Stored Communications Act, the ECPA has not been held to create a reasonable expectation of privacy in an individual’s name, address, social security number, credit card number, or details about one’s Internet connection. While the ECPA was a response to technological change, the technology has continued to proliferate making the Act outdated. It no longer protects the information it was designed to protect.

C. Video Privacy Protection Act

Additional inspiration can be found in the VPPA. The Video Privacy Protection Act makes a provider civilly liable for “knowingly disclose[ing] to any person, personally identifiable information concerning any consumer.” The VPPA also requires that the rental industry delete personally identifiable information “as soon as practicable” to ensure customer privacy. Redbox was recently sued under this statute for allowing call center employees to access customer rental records and the court noted:

When the law was passed, Congress assuredly had a brick-and-mortar video rental store in mind. The “ordinary course” of that rental store’s business would have included typical interactions between a customer and the store clerk, who in many cases would have accessed an individual customer’s rental history, address, and other personal information during the checkout process. And if that customer experienced technical problems with his rented VHS upon his return home from the store, he would have called the store to complain or seek a refund. He also would have called to complain if the store overcharged his credit card. All of these interactions, occurring within the store’s ordinary course of business, constitute that customer’s “request processing” and

133. Reed, 575 F.3d at 916.

For Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection. The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information.

Id.

135. See Electronic Communications Privacy: Hearing on S. 1667, supra note 113 (“But the uneasy realization is growing that someone else may be listening. Modern technology, which has given us these dazzling new means of communications, has also opened up opportunities for new and more intrusive forms of snooping.”)

“order fulfillment,” if ordinary meaning is assigned to those terms. Accordingly, plaintiffs’ attempt to carve out customer service from a video rental company’s “ordinary course of business” is unpersuasive. Congress, of course, did not draft the VPPA only with automated video rental kiosks in mind, and so it defies logic to construe the statute’s terms as if it had.\footnote{Sterk v. Redbox Automated Retail, LLC., 770 F.3d 618, 625 (7th Cir. 2014).}

The purpose of the legislation was to protect video tape rental records that could be used to ascertain the private viewing behaviors of citizens.\footnote{S. Rep. No. 100-599, at 1 (1988), reprinted in 1988 U.S.C.C.A.N. 4342, 4342-1.} The limitations of the statute are further illustrated by a recent 2014 case, \textit{In re Nickelodeon Consumer Privacy Litigation},\footnote{No. 12-07829, 2014 WL 3012873 (D.N.J. July 2, 2014).} where children under the age of thirteen created user profiles on Nickelodeon themed websites and their online record was disseminated to Google who collected and compiled the information.\footnote{In re Nickelodeon Consumer Privacy Litigation, No. 12-0789, 2014 WL 3012873, at *1 (D.N.J. July 2, 2014).} In addition:

The fruits of Google’s data tracking include “the URLs . . . visited by the Plaintiffs, the Plaintiffs’ respective IP addresses and each Plaintiff’s [sic] browser setting, unique device identifier, operating system, screen resolution, browser version, detailed video viewing histories and the details of their Internet communications with” the Viacom sites. Google’s cookies also assign to each Plaintiff a “unique numeric or alphanumerical identifier” that becomes “connected to” the information Viacom discloses to Google about that Plaintiff—namely, the username, gender, birthdate, IP address, etc. The information is used by Google for the same reason that Viacom uses it “to sell targeted advertising” based upon Plaintiffs’ “individualized web usage, including videos requested and obtained.”\footnote{\textit{Nickelodeon}, 2014 WL 3012873, at *2 (internal citations omitted).}

In this case, the court found that the data described above was “simply not information that, without more, identifies a person—an actual, specific human being—as having rented, streamed, or downloaded a given video, especially given the absence of factual allegations regarding how (and if) Plaintiffs’ unique usernames were linked to their actual names.”\footnote{Id. at *11.}

Despite the limitations of the VPPA, the type of privacy protected by the VPPA is the type of privacy that is being invaded when reading records or Internet use behavior is tracked and stored by suppliers. While the courts have failed to extend the VPPA to these types of records, the intent behind the legislation is to “help[ ] define the right
of privacy by prohibiting unauthorized disclosure of personal information.]^{145} As the Senate Report notes, "[Privacy] is not a conservative or a liberal or moderate issue. It is an issue that goes to the deepest yearnings of all Americans that we are free and we cherish our freedom and we want our freedom. We want to be left alone."^{146} This type of information is personal in nature and is information about an individual's behavior that usually occurs within the confines of the home.

The Senate Report to the VPPA acknowledged a nexus "between what one views and what one reads."^{147} It is time to combine the privacy state statutes, the type of privacy protected by the VPPA, and the concept of electronic privacy in the ECPA to protect digital personal information. Under this type of statute, potentially any personally identifiable electronic information conveyed in the ordinary course of business in an online environment could become protected. Personal electronic information includes name, address, social security number, credit card number, or anything else that identifies a person by name. It should also include the type of information that the terms of service consider "nonpersonal" information such as: occupation, language, zip code, area code, unique device identifier, referrer URL, location, and time zone.^{148} New legislation should be drafted to create a reasonable privacy interest in personal information, as well as the nonpersonal information that identifies user behavior and is compiled in the ordinary course of business of ISPs.

Under this type of legislation, a provider of Internet services (whether that be e-books or web browsing) could not disclose personal or nonpersonal information that identifies an individual's online behavior without express consent from the user. In addition, like the VPPA, the statute should require information retained in normal electronic business transactions to be deleted "as soon as practicable" to ensure customer privacy, and all information relayed back to a company about users of their Internet behavior should be encrypted to prevent the type of data breach that occurred with Adobe in October of 2014 discussed in the Introduction.

IX. CONCLUSION

"Begin at the beginning . . . and go on till you come to the end: then stop."^{149}

---

145. S. REP. No. 100-599 at 6.
146. Id. (citations omitted).
147. Id. at 8.
148. See infra Appendix B for suggested language for this type of bill.
149. CARROLL, supra note 1, at 70.
The Video Privacy Protection Act was a reaction to the video tape rental records of a Supreme Court nominee, Robert H. Bork, being published. The Washington City Paper, a weekly Washington paper, published a list of 146 films his family had rented from a video store.150 His nomination was rejected by the Senate. In 1987, during the Hearings on Nomination of Robert H. Bork to be an Associate Justice of the Supreme Court of the United States, Senator Leahy stated:

It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. . . . [I]n an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. . . . I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.151

The warning is insightful and more applicable today than it was in 1987. The challenges to user's privacy cannot be answered by pre-existing statutes that were designed before the Internet changed the delivery and format of goods and services. User privacy should be protected with the same safeguards available to the pre-networked world. Privacy should attach to personal information disclosed to an internet service provider and to online vendors who require user accounts to access digital information. In addition, privacy should attach to records that disclose an intimate record of online user behavior. While the majority of these records are deemed "nonpersonal information" they disclose much more intimate information about an individual than the personal information. The aggregate data could potentially show if a person has marital problems, depression, difficulty with their job, sexual fetishes, etc. These types of Internet searches, records of digital books, and online products purchased can disclose an incredible amount of details about a person that the person may not realize. These records should have their own protection that requires encryption and a limitation of use beyond marketing by the provider. The information should be explicitly protected to preserve online privacy and prevent the information from being used for a different purpose without the user's consent.

151. Id. at 5-6.
### APPENDIX A:

**State Laws Protecting Confidentiality of Library Records**

<table>
<thead>
<tr>
<th>Alabama, Ala. Code §§ 41-8-9, 41-8-10 (1975). Definitions; Confidentiality of registration records:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definitions:</strong></td>
</tr>
<tr>
<td>As used in Section 41-8-10, the term &quot;registration records&quot; includes any information which a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term &quot;circulation records&quot; includes all information which identifies the patrons utilizing particular books and any other library materials in any medium or format.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ala. Code § 41-8-9 (1975). Confidentiality of registration records:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration, etc., records of public libraries to be confidential; right of parents to inspect records:</strong></td>
</tr>
<tr>
<td>It is recognized that public library use by an individual should be of confidential nature. Any other provision of general, special or local law, rule or regulation to the contrary notwithstanding, the registration and circulation records and information concerning the use of the public, public school, college and university libraries of this state shall be confidential. Registration and circulation records shall not be open for inspection by, or otherwise available to, any agency or individual except for the following entities: (a) the library which manages the records; (b) the state education department for a library under its jurisdiction when it is necessary to assure the proper operation of such library; or (c) the state Public Library Service for a library under its jurisdiction when it is necessary to assure the proper operation of such library. Aggregate statistics shown from registration and circulation records, with all personal identification removed, may be released or used by a library for research and planning purposes. Provided however, any parent of a minor child shall have the right to inspect the registration and circulation records of any school or public library that pertain to his or her child.</td>
</tr>
</tbody>
</table>

| Ala. Code § 41-8-10 (1975). |

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(a) Except as provided in (b) of this section, the names, addresses, or other personal identifying information of people who have used materials made available to the public by a library shall be kept confidential, except upon court order, and are not subject to inspection under AS 40.25.110 or 40.25.120. This section applies to libraries operated by the state, a municipality, or a public school, including the University of</strong></td>
</tr>
</tbody>
</table>
Alaska.
(b) Records of a public elementary or secondary school library identifying a minor child shall be made available on request to a parent or guardian of that child.

Id.


§ 41-151.22. Privacy of user records; violation; classification; definition
A. Except as provided in subsection B of this section, a library or library system supported by public monies shall not allow disclosure of any record or other information, including e-books, that identifies a user of library services as requesting or obtaining specific materials or services or as otherwise using the library.
B. Records may be disclosed:
1. If necessary for the reasonable operation of the library.
2. On written consent of the user.
3. On receipt of a court order.
4. If required by law.
C. Any person who knowingly discloses any record or other information in violation of this section is guilty of a class 3 misdemeanor.
D. For the purposes of this section, “e-book” means a book composed in or converted to digital format for display on a computer screen or handheld device.

Id.

Definitions:

(a) “Confidential library records” means documents or information in any format retained in a library that identify a patron as having requested, used, or obtained specific materials, including, but not limited to, circulation of library books, materials, computer database searches, interlibrary loan transactions, reference queries, patent searches, requests for photocopies of library materials, title reserve requests, or the use of audiovisual materials, films, or records; and
(b) “Patron” means any individual who requests, uses, or receives services, books or other materials from a library.

Penalty:

(a) Any person who knowingly violates any of the provisions of this subchapter shall be guilty of a misdemeanor and shall be punished by a fine of not more than two hundred dollars ($200)
or thirty (30) days in jail, or both, or a sentence of appropriate public service or education, or both.
(b) No liability shall result from any lawful disclosure permitted by this subchapter.
(c) No action may be brought under this subchapter unless the action is begun within two (2) years from the date of the act complained of or the date of discovery.

Disclosure Prohibited:

(a) Library records which contain names or other personally identifying details regarding the patrons of public, school, academic, and special libraries and library systems supported in whole or in part by public funds shall be confidential and shall not be disclosed except as permitted by this subchapter.
(b) Public libraries shall use an automated or Gaylord-type circulation system that does not identify a patron with circulated materials after materials are returned.


California, Cal. Gov't Code § 6267 (West 2011). Registration and circulation records of library supported by public funds.

All patron use records of any library which is in whole or in part supported by public funds shall remain confidential and shall not be disclosed by a public agency, or private actor that maintains or stores patron use records on behalf of a public agency, to any person, local agency, or state agency except as follows:
(a) By a person acting within the scope of his or her duties within the administration of the library.
(b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records.
(c) By order of the appropriate superior court.

As used in this section, the term "patron use records" includes the following:
(1) Any written or electronic record, that is used to identify the patron, including, but not limited to, a patron's name, address, telephone number, or e-mail address, that a library patron provides in order to become eligible to borrow or use books and other materials.
(2) Any written record or electronic transaction that identifies a patron's borrowing information or use of library information resources, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries.
This section shall not apply to statistical reports of patron use nor to records of fines collected by the library.
Id.


(1) Except as set forth in subsection (2) of this section, a publicly-supported library shall not disclose any record or other information that identifies a person as having requested or obtained specific materials or service or as otherwise having used the library.

(2) Records may be disclosed in the following instances:

   (a) When necessary for the reasonable operation of the library;

   (b) Upon written consent of the user;

   (c) Pursuant to subpoena, upon court order, or where otherwise required by law;

   (d) To a custodial parent or legal guardian who has access to a minor's library card or its authorization number for the purpose of accessing by electronic means library records of the minor.

(3) Any library official, employee, or volunteer who discloses information in violation of this section commits a class 2 petty offense and, upon conviction thereof, shall be punished by a fine of not more than three hundred dollars.

Id.


(a) The libraries established under the provisions of this chapter, and any free public library receiving a state appropriation, shall annually make a report to the State Library Board.

(b) (1) Notwithstanding section 1-210, records maintained by libraries that can be used to identify any library user, or link any user to a library transaction, regardless of format, shall be kept confidential, except that the records may be disclosed to officers, employees and agents of the library, as necessary for operation of the library.

   (2) Information contained in such records shall not be released to any third party, except (A) pursuant to a court order, or (B) with the written permission of the library user whose personal information is contained in the records.

(3) For purposes of this subsection, "library" includes any library regularly open to the public, whether public or private, maintained by any industrial, commercial or other group or association, or by any governmental agency, but does not include libraries maintained by schools and institutions of higher education.

(4) No provision of this subsection shall be construed to prevent a library from publishing or making available to the public statistical reports regarding library registration and use of
library materials, if such reports do not contain personally identifying information.

Id.


Any records of a public library which contain the identity of a user and the books, documents, films, recordings or other property of the library which a patron has used[.]

Id.


Confidentiality of circulation records.
(a) Circulation records maintained by the public library in the District of Columbia which can be used to identify a library patron who has requested, used, or borrowed identified library materials from the public library and the specific material that patron has requested, used, or borrowed from the public library, shall be kept confidential, except that the records may be disclosed to officers, employees, and agents of the public library to the extent necessary for the proper operation of the public library.
(b)(1) Circulation records shall not be disclosed by any officer, employee, or agent of the public library to a 3rd party or parties, except with the written permission of the affected library patron or as the result of a court order.

Id.

**Florida, Fla. Stat. § 257.261 (2003).**

Library registration and circulation records
(1) All registration and circulation records of every public library, except statistical reports of registration and circulation, are confidential and exempt from the provisions of s. 119.07(1) and from s. 24(a) of Art. I of the State Constitution.
(2) As used in this section, the term “registration records” includes any information that a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term “circulation records” includes all information that identifies the patrons who borrow particular books and other materials.
(3)(a) Except in accordance with a proper judicial order, a person may not make known in any manner any information contained in records made confidential and exempt by this section, except as otherwise provided in this section.

Id.

Confidential nature of library records.
(a) Circulation and similar records of a library which identify the user of library materials shall not be public records but shall be confidential and may not be disclosed except:
(1) To members of the library staff in the ordinary course of business;
(2) Upon written consent of the user of the library materials or the user's parents or guardian if the user is a minor or ward; or
(3) Upon appropriate court order or subpoena.
(b) Any disclosure authorized by subsection (a) of this Code section or any unauthorized disclosure of materials made confidential by that subsection (a) of this Code section shall not in any way destroy the confidential nature of that material, except for the purpose for which an authorized disclosure is made. A person disclosing material as authorized by subsection (a) of this Code section shall not be liable therefor.

Id.


In Hawaii, the protection does not stem from a state statute, but from an interpretation of state law by the Department of the Attorney General, Office of Information Practices, State of Hawaii. Office of Information Practices, Opinion Letter No. 90-30, October 23, 1990 states:

Unlike the majority of states, Hawaii does not have a specific statute which prohibits public access to public library circulation records. Accordingly, resolution of the question presented must be determined with reference to the provisions of the UIPA.

The UIPA does not require agencies to disclose “[g]overnment records which, if disclosed, would constitute a clearly unwarranted invasion of personal privacy.” Haw. Rev. Stat. § 92F-13(1) (Supp. 1989). In order for this exception to apply to a particular government record, it must be a record in which an individual has a significant privacy interest. Based upon attorney general opinions from several other states, and a decision of the Supreme Court of Hawaii, we conclude that individuals have a significant privacy interest in information, such as Library circulation records, which reveals their thoughts, associations, or beliefs.

Furthermore, under the UIPA's balancing test set forth at section 92F-14(a), Hawaii Revised Statutes, we conclude that an individual's privacy interest in Library circulation records is
not outweighed by the public interest in disclosure. The public disclosure of Library circulation records would reveal little about “the discussions, deliberations, decisions, and action of government agencies.” See Haw. Rev. Stat. § 92F-2 (Supp. 1989). Indeed, the public disclosure of Library circulation records would reveal little more than the fact that the Library permitted materials to be borrowed. Accordingly, we conclude that generally, the public disclosure of Library circulation records would “constitute a clearly unwarranted invasion of personal privacy” under the UIPA.

*Id.*


The following records are exempt from disclosure:

1. Records, maps or other records identifying the location of archaeological or geophysical sites or endangered species, if not already known to the general public.
2. Archaeological and geologic records concerning exploratory drilling, logging, mining and other excavation, when such records are required to be filed by statute for the time provided by statute.
3. The records of a library which, when examined alone, or when examined with other public records, would reveal the identity of the library patron checking out, requesting, or using an item from a library.
4. The material of a library, museum or archive that has been contributed by a private person, to the extent of any limitation that is a condition of the contribution.
5. Test questions, scoring keys, and other data used to administer a licensing examination, employment, academic or other examination or testing procedure before the examination is given if the examination is to be used again. Records establishing procedures for and instructing persons administering, grading or evaluating an examination or testing procedure are included in this exemption, to the extent that disclosure would create a risk that the result might be affected.

*Id.*


§ 1. (a) The registration and circulation records of a library are confidential information. No person shall publish or make any information contained in such records available to the public

(b) This Section does not prevent a library from publishing or making available to the public reasonable statistical reports regarding library registration and book circulation where those
reports are presented so that no individual is identified therein.

(c) For the purpose of this Section, (i) "library" means any public library or library of an educational, historical or eleemosynary institution, organization or society; (ii) "registration records" includes any information a library requires a person to provide in order for that person to become eligible to borrow books and other materials and (iii) "circulation records" includes all information identifying the individual borrowing particular books or materials.

_id_.

**Indiana, Ind. Code § 5-14-3-4 (2015).**

Sec. 4 (a) The following public records are excepted from section 3 [IC 5-14-3-3] of this chapter and may not be disclosed by a public agency, unless access to the records is specifically required by a state or federal statute or is ordered by a court under the rules of discovery:

(1) Those declared confidential by state statute.
(2) Those declared confidential by rule adopted by a public agency under specific authority to classify public records as confidential granted to the public agency by statute.

(b) Except as otherwise provided by subsection (a), the following public records shall be excepted from section 3 of this chapter at the discretion of a public agency.

(16) Library or archival records:
(A) which can be used to identify any library patron; or
(B) deposited with or acquired by a library upon a condition that the records be disclosed only:
(i) to qualified researchers;
(ii) after the passing of a period of years that is specified in the documents under which the deposit or acquisition is made; or
(iii) after the death of persons specified at the time of the acquisition or deposit.

_id_.

**Iowa, Iowa Code § 22.7 (2015).**

Confidential records
The following public records shall be kept confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release such information:

13. The records of a library which, by themselves or when examined with other public records, would reveal the identity of the library patron checking out or requesting an item or information from the library. The records shall be released to a criminal or juvenile justice agency only pursuant to an
investigation of a particular person or organization suspected of committing a known crime. The records shall be released only upon a judicial determination that a rational connection exists between the requested release of information and a legitimate end and that the need for the information is cogent and compelling.

14. The material of a library, museum or archive which has been contributed by a private person to the extent of any limitation that is a condition of the contribution.

Id.


Certain records not required to be open; separation of open and closed information required; statistics and records over 70 years old open

(a) Except to the extent disclosure is otherwise required by law, a public agency shall not be required to disclose:

(7) Library, archive and museum materials contributed by private persons, to the extent of any limitations imposed as conditions of the contribution.

(23) Library patron and circulation records which pertain to identifiable individuals.

Id.


In Kentucky, the protection is derived from an interpretation of a state statute from the Office of the Attorney General. The pertinent language includes:

The main thrust of OAG 81-159 and of this opinion is that no person can demand as a matter of right to inspect the circulation records of any type of library—school, public, academic or special—under the Open Records Law.

Id.


Registration records and other records of use maintained by libraries

A. Notwithstanding any provisions of this Chapter or any other law to the contrary, records of any library which is in whole or in part supported by public funds, including the records of public, academic, school, and special libraries, and the State Library of Louisiana, indicating which of its documents or other materials, regardless of format, have been loaned to or used by an identifiable individual or group of individuals may not be
disclosed except to a parent or custodian of a minor child seeking access to that child's records, to persons acting within the scope of their duties in the administration of the library, to persons authorized in writing by the individual or group of individuals to inspect such records, or by order of a court of law. B. Notwithstanding any provisions of this Chapter or any other law to the contrary, records of any such library which are maintained for purposes of registration or for determining eligibility for the use of library services may not be disclosed except as provided in Subsection A of this Section.

**Id.**

**Maine, Me. Rev. Stat. tit. 27, § 121 (2013).**

Confidentiality of library records

Records maintained by any public library . . . the Maine State Library, the Law and Legislative Reference Library and libraries of the University of Maine System, Maine Community College System and the Maine Maritime Academy that contain information relating to the identity of a library patron relative to the patron's use of books or other materials at the library are confidential. Those records may only be released with the express written permission of the patron involved or as the result of a court order.

**Id.**

**Maryland, Md. Code Ann., SG, § 4-308 (West 2014).** Specific records. Inspection of a public record, as provided in this section.

In general (1) Subject to subsection (b) of this section, a custodian shall prohibit inspection, use, or disclosure of a circulation record of a public library or other item, collection, or grouping of information about an individual that: (i) is maintained by a library; (ii) contains an individual's name or the identifying number, symbol, or other identifying particular assigned to the individual; and (iii) identifies the use a patron makes of that library's materials, services, or facilities.

**Id.**

**Massachusetts, Mass. Gen. Laws ch. 78, § 7 (1988).**

A town may establish and maintain public libraries for its inhabitants under regulations prescribed by the city council or by the town, and may receive, hold and manage any gift, bequest or devise therefor. The city council of a city or the selectmen of a town may place in such library the books, reports and laws which may be received from the commonwealth. That part of the records of a public library which reveals the identity and intellectual pursuits of a person using such library shall not be a public record as defined by clause Twenty-sixth of
section seven of chapter four. Library authorities may disclose or exchange information relating to library users for the purposes of inter-library cooperation and coordination, including but not limited to, the purposes of facilitating the sharing of resources among library jurisdictions as authorized by clause (1) of section nineteen E or enforcing the provisions of sections ninety-nine and one hundred of chapter two hundred and sixty-six.

_id_.

**Michigan, Mich. Comp. Laws § 397.603 (1996).** Library record not subject to disclosure requirements.

Sec. 3. (1) Except as provided in subsection (2), a library record is not subject to the disclosure requirements of the freedom of information act, Act No. 442 of the Public Acts of 1976, being sections 15.231 to 15.246 of the Michigan Compiled Laws.

(2) Unless ordered by a court after giving the affected library notice of the request and an opportunity to be heard on the request, a library or an employee or agent of a library shall not release or disclose a library record or portion of a library record to a person without the written consent of the person liable for payment for or return of the materials identified in that library record.

(3) The procedure and form of giving written consent described in subsection (2) may be determined by the library.

(4) A library may appear and be represented by counsel at a hearing described in subsection (2).

_id_.

**Minnesota, Minn. Stat. § 13.40 (2007).**

Library and historical data.

Subd. 2. Private data; library borrowers. (a) Except as provided in paragraph (b), the following data maintained by a library are private data on individuals and may not be disclosed for other than library purposes except pursuant to a court order:

(1) data that link a library patron’s name with materials requested or borrowed by the patron or that link a patron’s name with a specific subject about which the patron has requested information or materials; or

(2) data in applications for borrower cards, other than the name of the borrower.

(b) A library may release reserved materials to a family member or other person who resides with a library patron and who is picking up the material on behalf of the patron. A patron may request that reserved materials be released only to the patron.
Id.


Records maintained by any library funded in whole or in part by public funds, which contain information relating to the identity of a library user, relative to the user's use of books or other materials at the library, shall be confidential. Such records may only be released with the express written permission of the respective library user or as the result of a court order.

Id.

**Missouri, Mo. Rev. Stat. § 182.815 (2014).** Definitions:

As used in this section and section 182.817, the following terms shall mean:

1. "Digital resource or material", any E-book, digital periodical, digital thesis, digital dissertation, digital report, application, website, database, or other data available in digital format from a library for display on a computer screen or handheld device;
2. "E-book", any book composed or converted to digital format for display on a computer screen or handheld device;
3. "Library", any library established by the state or any political subdivision of the state, or combination thereof, by any community college district, or by any college or university, and any private library open to the public;
4. "Library material", any book, E-book, digital resource or material, document, film, record, art work, or other library property which a patron may use, borrow or request;
5. "Library record", any document, record, or other method of storing information retained, received or generated by a library that identifies a person or persons as having requested, used, or borrowed library material, and all other records identifying the names of library users. The term "library record" does not include nonidentifying material that may be retained for the purpose of studying or evaluating the circulation of library material in general.

Id.


1. Notwithstanding the provisions of any other law to the contrary, no library, employee or agent of a library, or third party contracted by a library that receives, transmits, maintains, or stores library records shall release or disclose a library record or portion of a library record to any person or persons except:

   1) In response to a written request of the person identified in that record, according to procedures and forms giving written
consent as determined by the library; or
(2) In response to an order issued by a court of competent jurisdiction upon a finding that the disclosure of such record is necessary to protect the public safety or to prosecute a crime.

Id.


Nondisclosure of library records
(1) No person may release or disclose a library record or portion of a library record to any person except in response to:
(a) a written request of the person identified in that record, according to procedures and forms giving written consent as determined by the library; or
(b) an order issued by a court of competent jurisdiction, upon a finding that the disclosure of such record is necessary because the merits of public disclosure clearly exceed the demand for individual privacy.

Id.


Records which may be withheld from the public; enumerated
The following records, unless publicly disclosed in an open court, open administrative proceeding, or open meeting or disclosed by a public entity pursuant to its duties, may be withheld from the public by the lawful custodian of the records:
(1) Personal information in records regarding a student, prospective student, or former student of any educational institution or exempt school that has effectuated and election not to meet state approval or accreditation requirements pursuant to section 79-1601 when such records are maintained by the possession of a public entity, other than routine directory information specified and made public consistent with 20 U.S.C. 1232g, as such section existed on February 1, 2013, and regulations adopted thereunder;

....
(11) Records or portions of records kept by a publicly funded library which, when examined with or without other records, reveal the identity of any library patron using the library's materials or services ....

Id.


Confidentiality of records of library which identify user with property used
Any records of a public library or other library which contain the identity of a user and the books, documents, films, recordings or other property of the library which were used are
confidential and not public books or records within the meaning of NRS 239.010. Such records may be disclosed only in response to an order issued by a court upon a finding that the disclosure of such records is necessary to protect the public safety or to prosecute a crime.

*Id.*


Library User Records; Confidentiality.

I. Library records which contain the names or other personal identifying information regarding the users of public or other than public libraries shall be confidential and shall not be disclosed except as provided in paragraph II. Such records include, but are not limited to, library, information system, and archival records related to the circulation and use of library materials or services . . . .

II. Records described in paragraph I may be disclosed to the extent necessary for the proper operation of such libraries and shall be disclosed upon request by or consent of the user or pursuant to subpoena, court order, or where otherwise required by statute.

III. Nothing in this section shall be construed to prohibit any library from releasing statistical information and other data regarding the circulation or use of library materials provided, however, that the identity of the users of such library materials shall be considered confidential and shall not be disclosed to the general public except as provided in paragraph II.

*Id.*


Confidentiality.

Library records which contain the names or other personally identifying details regarding the users of libraries are confidential and shall not be disclosed except in the following circumstances:

a. The records are necessary for the proper operation of the library;

b. Disclosure is requested by the user; or

c. Disclosure is required pursuant to a subpoena issued by a court or court order.

*Id.*


Library Privacy Act.

Short title
This act [18-9-1 to 18-9-6 NMSA 1978] may be cited as the “Library Privacy Act”. Id.


Purpose
The purpose of the Library Privacy Act [18-9-1 to 18-9-6 NMSA 1978] is to preserve the intellectual freedom guaranteed by Sections 4 and 17 of Article 2 of the constitution of New Mexico by providing privacy for users of the public libraries of the state with respect to the library materials that they wish to use.

Id.


Definitions
As used in the Library Privacy Act [18-9-1 to 18-9-6 NMSA 1978]:
A. “library” includes any library receiving public funds, any library that is a state agency and any library established by the state, an instrumentality of the state, a local government, district or authority, whether or not that library is regularly open to the public; and
B. “patron record” means any document, record or other method of storing information retained by a library that identifies, or when combined with other available information identifies, a person as a patron of the library or that indicates use or request of materials from the library. “Patron record” includes patron registration information and circulation information that identifies specific patrons.

Id.


Release of patron records prohibited
Patron records shall not be disclosed or released to any person not a member of the library staff in the performance of his duties, except upon written consent of the person identified in the record, or except upon court order issued to the library. The library shall have the right to be represented by counsel at any hearing on disclosure or release of its patron records.

Id.


Exceptions
The prohibition on the release or disclosure of patron records in Section 4 [18-9-4 NMSA 1978] of the Library Privacy Act shall not apply to overdue notices or to the release or disclosure by school libraries to the legal guardian of the patron records of unemancipated minors or legally incapacitated persons.
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Library records</td>
</tr>
<tr>
<td>Library records, which contain names or other</td>
</tr>
<tr>
<td>personally identifying details regarding the</td>
</tr>
<tr>
<td>users of public, free association, school,</td>
</tr>
<tr>
<td>college and university libraries and library</td>
</tr>
<tr>
<td>systems of this state, including but not</td>
</tr>
<tr>
<td>limited to records related to the circulation</td>
</tr>
<tr>
<td>of library materials, computer database</td>
</tr>
<tr>
<td>searches, interlibrary loan transactions,</td>
</tr>
<tr>
<td>reference queries, requests for photocopies</td>
</tr>
<tr>
<td>of library materials, title reserve requests,</td>
</tr>
<tr>
<td>or the use of audio-visual materials, films</td>
</tr>
<tr>
<td>or records, shall be confidential and shall</td>
</tr>
<tr>
<td>not be disclosed except that such records may</td>
</tr>
<tr>
<td>be disclosed to the extent necessary for the</td>
</tr>
<tr>
<td>proper operation of such library and shall be</td>
</tr>
<tr>
<td>disclosed upon request or consent of the user</td>
</tr>
<tr>
<td>or pursuant to subpoena, court order or where</td>
</tr>
<tr>
<td>otherwise required by statute.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality of library user records</td>
</tr>
<tr>
<td>(a) Disclosure. — A library shall not disclose</td>
</tr>
<tr>
<td>any library record that identifies a person</td>
</tr>
<tr>
<td>as having requested or obtained specific</td>
</tr>
<tr>
<td>materials, information, or services, or as</td>
</tr>
<tr>
<td>otherwise having used the library, except as</td>
</tr>
<tr>
<td>provided for in subsection (b).</td>
</tr>
<tr>
<td>(b) Exceptions. — Library records may be</td>
</tr>
<tr>
<td>disclosed in the following instances:</td>
</tr>
<tr>
<td>(1) When necessary for the reasonable operation</td>
</tr>
<tr>
<td>of the library;</td>
</tr>
<tr>
<td>(2) Upon written consent of the user; or</td>
</tr>
<tr>
<td>(3) Pursuant to subpoena, court order, or</td>
</tr>
<tr>
<td>where otherwise required by law.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Library records—Open records exception</td>
</tr>
<tr>
<td>Any record maintained or received by a library</td>
</tr>
<tr>
<td>receiving public funds, which provides a</td>
</tr>
<tr>
<td>library patron’s name or information</td>
</tr>
<tr>
<td>sufficient to identify a patron together with</td>
</tr>
<tr>
<td>the subject about which the patron requested</td>
</tr>
<tr>
<td>information, is considered private and</td>
</tr>
<tr>
<td>excepted from the public records disclosure</td>
</tr>
<tr>
<td>requirements of section 44-04-18. These records</td>
</tr>
<tr>
<td>may be released when required pursuant to a</td>
</tr>
<tr>
<td>court order or a subpoena.</td>
</tr>
</tbody>
</table>

| Ohio, OHIO REV. CODE ANN. § 149.432 (West 2004). Release of |
| library record or patron information.               |

| (A) As used in this section:                        |
| (1) “Library” means a library that is open to the  |
| public, |
including any of the following:
(a) A library that is maintained and regulated under section 715.13 of the Revised Code;
(b) A library that is created, maintained, and regulated under Chapter 3375. of the Revised Code;
(c) A library that is created and maintained by a public or private school, college, university, or other educational institution;
(d) A library that is created and maintained by a historical or charitable organization, institution, association, or society.
“Library” includes the members of the governing body and the employees of a library.

(2) “Library record” means a record in any form that is maintained by a library and that contains any of the following types of information:
(a) Information that the library requires an individual to provide in order to be eligible to use library services or borrow materials;
(b) Information that identifies an individual as having requested or obtained specific materials or materials on a particular subject;
(c) Information that is provided by an individual to assist a library staff member to answer a specific question or provide information on a particular subject.
“Library record” does not include information that does not identify any individual and that is retained for the purpose of studying or evaluating the use of a library and its materials and services.

(3) Subject to division (B)(5) of this section, “patron information” means personally identifiable information about an individual who has used any library service or borrowed any library materials.
(B) A library shall not release any library record or disclose any patron information . . . .

Id.


Disclosure of records
A. Any library which is in whole or in part supported by public funds including but not limited to public, academic, school or special libraries, and having records indicating which of its documents or other materials, regardless of format, have been loaned to or used by an identifiable individual or group shall not disclose such records to any person except to:
1. Persons acting within the scope of their duties in the administration of the library;
2. Persons authorized to inspect such records, in writing, by the individual or group; or
3. By order of a court of law.
B. The requirements of this section shall not prohibit middle and elementary school libraries from maintaining a system of records that identifies the individual or group to whom library materials have been loaned even if such system permits a determination, independent of any disclosure of such information by the library, that documents or materials have been loaned to an individual or group.

**Id.**

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The following public records are exempt from disclosure under ORS 192.410 to 192.505:</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>(23) The records of a library, including:</td>
</tr>
<tr>
<td>(a) Circulation records, showing use of specific library material by a named person;</td>
</tr>
<tr>
<td>(b) The name of a library patron together with the address or telephone number of the patron;</td>
</tr>
<tr>
<td>(c) The electronic mail address of the patron.</td>
</tr>
</tbody>
</table>

**Id.**

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Records of the following institutions which relate to the circulation of library materials and contain the names or other personally identifying information of users of the materials shall be confidential and may not be made available to anyone except by a court order in a criminal proceeding:</td>
</tr>
<tr>
<td>(1) The State Library.</td>
</tr>
<tr>
<td>(2) A local library established or maintained under the provisions of this chapter.</td>
</tr>
<tr>
<td>(3) A library of a university, college or educational institution chartered by the Commonwealth.</td>
</tr>
<tr>
<td>(4) The library of a public school.</td>
</tr>
<tr>
<td>(5) A library established and maintained under a law of this Commonwealth.</td>
</tr>
<tr>
<td>(6) A branch reading room, deposit station or agency operated in connection with a library described in this section.</td>
</tr>
</tbody>
</table>

**Id.**

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As used in this chapter:</td>
</tr>
<tr>
<td>(1) “Agency” or “public body” means any executive, legislative, judicial, regulatory, or administrative body of the state, or any</td>
</tr>
</tbody>
</table>
political subdivision thereof; including, but not limited to, any department, division, agency, commission, board, office, bureau, authority, any school, fire, or water district, or other agency of Rhode Island state or local government which exercises governmental functions, any authority as defined in § 42-35-1(b), or any other public or private agency, person, partnership, corporation, or business entity acting on behalf of and/or in place of any public agency.

(2) "Chief administrative officer" means the highest authority of the public body.

(3) "Public business" means any matter over which the public body has supervision, control, jurisdiction, or advisory power.

(4) "Public record" or "public records" shall mean all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, computer stored data (including electronic mail messages, except specifically for any electronic mail messages of or to elected officials with or relating to those they represent and correspondence of or to elected officials in their official capacities) or other material regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. For the purposes of this chapter, the following records shall not be deemed public:

. . .

(U) Library records which by themselves or when examined with other public records, would reveal the identity of the library user requesting, checking out, or using any library materials.

*Id.*

**South Carolina, S.C. Code Ann. § 60-4-10 (1985).**

Records identifying library patrons as confidential information; disclosure.

Records related to registration and circulation of library materials which contain names or other personally identifying details regarding the users of public, private, school, college, technical college, university, and state institutional libraries and library systems, supported in whole or in part by public funds or expending public funds, are confidential information. Records which by themselves or when examined with other public records would reveal the identity of the library patron checking out or requesting an item from the library or using other library services are confidential information.

The confidential records do not include nonidentifying administrative and statistical reports of registration and circulation.

The confidential records may not be disclosed except to persons
acting within the scope of their duties in the administration of the library or library system or persons authorized by the library patron to inspect his records, or in accordance with proper judicial order upon a finding that the disclosure of the records is necessary to protect public safety, to prosecute a crime, or upon showing of good cause before the presiding Judge in a civil matter.

Id.

Confidential library records.

All public library records containing personally identifiable information are confidential. Any information contained in public library records may not be released except by court order or upon request of a parent of a child who is under eighteen years of age. As used in this section, “personally identifiable” means any information a library maintains that would identify a patron. Acts by library officers or employees in maintaining a check out system are not violations of this section.

Id.

Confidentiality of library records.

10-8-101. Definitions
As used in this chapter, unless the context otherwise requires:
(1) “Library” means:
(A) A library that is open to the public and established or operated by:
(i) The state, a county, city, town, school district or any other political subdivision of the state;
(ii) A combination of governmental units or authorities;
(iii) A university or community college; or
(B) Any private library that is open to the public; and
(2) “Library record” means a document, record, or other method of storing information retained by a library that identifies a person as having requested or obtained specific information or materials from such library. “Library record” does not include nonidentifying material that may be retained for the purpose of studying or evaluating the circulation of library materials in general.


10-8-102. Disclosure prohibited; Exceptions
(a) Except as provided in subsection (b), no employee of a library shall disclose any library record that identifies a person as having requested or obtained specific materials, information, or services or as having otherwise used such library. Such library records shall be considered an exception to § 10-7-503.
(b) Library records may be disclosed under the following circumstances:
   (1) Upon the written consent of the library user;
   (2) Pursuant to the order of a court of competent jurisdiction; or
   (3) When used to seek reimbursement for or the return of lost, stolen, misplaced or otherwise overdue library materials.


10-8-103. Applicability
   This chapter shall apply to libraries included within the provisions of chapters 1 and 3-5 of this title.


Information excepted from required disclosure.

   (a) A record of a library or library system, supported in whole or in part by public funds, that identifies or serves to identify a person who requested, obtained, or used a library material or service is excepted from the requirements of Section 552.021 unless the record is disclosed:
   (1) because the library or library system determines that disclosure is reasonably necessary for the operation of the library or library system and the record is not confidential under other state or federal law;
   (2) under Section 552.023; or
   (3) to a law enforcement agency or a prosecutor under a court order or subpoena obtained after a showing to a district court that:
   (A) disclosure of the record is necessary to protect the public safety; or
   (B) the record is evidence of an offense or constitutes evidence that a particular person committed an offense.
   (b) A record of a library or library system that is excepted from required disclosure under this section is confidential.

Id.


Private records
   The following records are private: records of publicly funded libraries that when examined alone or with other records identify a patron[.]

Id.


Definitions; public agency; public records or documents
   (a) As used in this subchapter:

   (2) "Public agency" or "agency" means any agency, board,
department, commission, committee, branch, instrumentality, or authority of the state or any agency, board, committee, department, branch, instrumentality, commission, or authority of any political subdivision of the State.

(b) As used in this subchapter, “public record” or “public document” means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of public agency business. Individual salaries and benefits of and salary schedules relating to elected or appointed officials and employees of public agencies shall not be exempt from public inspection and copying.

(c) The following public records are exempt from public inspection and copying:

... (19) records relating to the identity of library patrons or the identity of library patrons in regard to library patron registration records and patron transaction records in accordance with 22 V.S.A. chapter 4.

Id.

**Virginia, Va. Code Ann. § 2.2-3705.7 (2014).**

Exclusions to application of chapter [Ch. 37. Virginia Freedom of Information Act] ... The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

... .

3. Library records that can be used to identify both (i) any library patron who has borrowed material from a library and (ii) the material such patron borrowed.

Id.


Any library record, the primary purpose of which is to maintain control of library materials, or to gain access to information, that discloses or could be used to disclose the identity of a library user is exempt from disclosure under this chapter.

Id.

**West Virginia, W. Va. Code § 10-1-22 (1990).**

Confidential nature of certain library records

(a) Circulation and similar records of any public library in this state which identify the user of library materials are not public records but shall be confidential and may not be disclosed except:

(1) To members of the library staff in the ordinary course of
business;
(2) Upon written consent of the user of the library materials or
the user’s parents or guardian if the user is a minor or ward; or
(3) Upon appropriate court order or subpoena.
(b) Any disclosure authorized by subsection (a) of this section or
any unauthorized disclosure of materials made confidential by
that subsection (a) does not in any way destroy the confidential
nature of that material, except for the purpose for which an
authorized disclosure is made. A person disclosing material as
authorized by subsection (a) of this section is not liable therefor.

Id.


Public library records.
(1b) In this section:
(a) “Custodial parent” includes any parent other than a parent
who has been denied periods of physical placement with a child
under s. 767.24 (4)

(1m) Records of any library which is in whole or in part
supported by public funds, including the records of a public
library system, indicating the identity of any individual who
borrows or uses the library’s documents or other materials,
resources, or services may not be disclosed except by court order
or to persons acting within the scope of their duties in the
administration of the library or library system, to persons
authorized by the individual to inspect such records, to
custodial parents or guardians of children under the age of 16
under sub. (4), or to libraries as authorized under subs. (2) and
(3).

(2) A library supported in whole or in part by public funds may
disclose an individual’s identity to another library for the
purpose of borrowing materials for the individual only if the
library to which the individual’s identity is being disclosed
meets at least one of the following requirements:
(a) The library is supported in whole or in part by public funds.
(b) The library has a written policy prohibiting the disclosure of
the identity of the individual except as authorized under sub.
(3).
(c) The library agrees not to disclose the identity of the
individual except as authorized under sub. (3).
(3) A library to which an individual’s identity is disclosed under
sub. (2) and that is not supported in whole or in part by public
funds may disclose that individual’s identity to another library
for the purpose of borrowing materials for that individual only
if the library to which the identity is being disclosed meets at
least one of the requirements specified under sub. (2) (a) to (c)
(4) Upon the request of a custodial parent or guardian of a child
who is under the age of 16, a library supported in whole or part by public funds shall disclose to the custodial parent or guardian all library records relating to the use of the library's documents or other materials, resources, or services by that child.

_Id._


Right of inspection; grounds for denial; access of news media; order permitting or restricting disclosure; exceptions
The custodian shall deny the right of inspection of the following records, unless otherwise provided by law: Library patron transaction and registration records except as required for administration of the library or except as requested by a custodial parent or guardian to inspect the records of his minor child[.]
APPENDIX B
WRONGFUL DISCLOSURE OF PERSONALLY IDENTIFIABLE ELECTRONIC RECORDS:

(a) DEFINITIONS. — For purposes of this section —
(1) the term 'consumer' means any user, purchaser, or subscriber of goods, or subscriber of services from an Internet service provider or third party vendor that distributes Internet media;
(2) the term 'ordinary course of business' means information gathered by a supplier of electronic services about a consumer in a standard business transaction or receipt of service;
(3) the term 'personally identifiable information' includes information which identifies a personal or nonpersonal information of a person having requested or obtained specific materials or services from a digital service provider;
(4) the term 'personal information' means information that personally identifies the user such as name, email address, information in a user profile, and billing information;
(5) the term 'nonpersonal information' means information gathered from technology placed on a website for the purposes of tracking activity such as pixel tags, cookies, server logs (web requests, Internet Protocol address, browser type, browser language, and the date and time of request), and unique device identifiers;
(6) the term 'digital service provider' means any person engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of Internet services such as the licensing and delivery of electronic books, electronic videos, and electronic games or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) ELECTRONIC RECORDS. —
(1) A digital service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).
(2) A digital service provider may disclose personally identifiable information concerning any consumer —
(A) to the consumer;
(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;
(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;
(D) to any person if the disclosure is solely of the names and addresses of consumers and if —
(i) the digital service provider has provided the consumer with the opportunity in a clear and conspicuous manner, to prohibit such disclosure; and
(ii) the disclosure does not identify the title, description, or subject matter of any electronic services provided; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;
(E) to any person if the disclosure is incident to the ordinary course of business of the digital service provider; or
(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if —
(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and
(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.
If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the digital service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) CIVIL ACTION. —
(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.
(2) The court may award —
(A) actual damages, but not less than liquidated damages in an amount of $2,500;
(B) punitive damages;
(C) reasonable attorneys’ fees and other litigation costs reasonably incurred; and
(D) such other preliminary and equitable relief as the court determines to be appropriate.
(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) PERSONALLY IDENTIFIABLE INFORMATION. — Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) DESTRUCTION OF OLD RECORDS. — A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) ENCRYPTION OF RECORDS TRANSMITTED. — A person subject to this section shall encrypt personally identifiable information when that information is transmitted back to a digital service provider to protect users from unauthorized access, unauthorized alteration, or unauthorized disclosure of the personally identifiable information;

(g) PREEMPTION. — The provisions of this section preempt only the provisions of State or local law that requires disclosure prohibited by this section.