What About Reader Privacy?

by Brandi Loveday-Chesley

EDITOR'S SUMMARY

Americans have long valued their freedom of speech and expression, but specific protection of reader privacy is a relatively new concept. Legal threats to reader privacy date to the 1950s with a resurgence of privacy invasion by the IRS and FBI in the 1970s, prompting 48 states to pass legislation extending confidentiality to readers. The PATRIOT Act of 2001 authorized the FBI to gain broad access to bookstore and library records for alleged terrorism investigations. Such information seeking threatens every reader's choice of reading materials where any trace, whether physical or digital, remains. Widespread use of computers to access data reflecting searches, downloads, cookies and other signs of reader habits and interests compounds the threat to personal privacy. Detailed records on electronic reader use stored in the cloud are accessible by authorities. It is crucial to recognize how invasions in the name of security threaten readers' personal privacy.

KEYWORDS

readers
personal information
privacy
usage records
computer security
government
intellectual freedom

Brandi Loveday-Chesley is an information technology specialist at New York State Insurance Fund, an officer of SIG/IFP, and a recipient of the ASIS&T New Leader Award. She can be reached at bloveday<at>gmail.com.

Reader privacy is a concept that most states (48 out of 50) have decided to protect with legislation targeted to engender and protect the freedom of speech held so dear by Americans [1]. So, how does reader privacy really affect freedom of speech and thought?

Reader privacy addresses the issue that readers should be free to read whatever materials they wish without fear of the government or another third party accessing that information. Protecting reader privacy fosters intelligent inquiry, research and freedom of expression. To allow the government, or any third party, access to a reader's records would constitute a serious invasion of privacy. Courts that protect reader privacy have allowed those who do not follow dominant political, social, scientific and economic thought to pursue their interests without fear of recrimination and the chilling effect that governmental intrusion can have on innovation and progress.

Brief History of Reader Privacy

While the constitution protects freedom of speech and expression, protecting reader privacy is relatively new. In the early 1950s the Supreme Court found it unconstitutional to convict a bookseller for refusing "...to provide the government with a list of individuals who had purchased political books." [1]

The 1970s saw attempted invasions of reader privacy by the IRS as well as the FBI. In 1973, 48 out of 50 states passed "confidentiality statutes to prevent such invasions of privacy." [2] The fight to protect readers' rights was brought to booksellers in 1998 when Kramerbooks & Afterwords and Barnes & Noble were served with subpoenas for records as part of an investigation regarding President Clinton. The publicity brought about by this attempt prompted other authoritative bodies such as the Denver Police

Department in 2000 to attempt to obtain detailed purchase records on suspects in criminal investigations [2].

The PATRIOT Act of 2001

In ensuing years federal and state courts have continued to protect a reader's right to privacy even in the face of the PATRIOT Act of 2001. This legislation contains a section (215) that "greatly amends and expands the scope of FISA," the Foreign Intelligence and Surveillance Act of 1978, "by granting the FBI the power to access and review any tangible thing, including bookstore and library records." [3] The PATRIOT Act allows FBI agents, under (unsubstantiated) claims of terrorism, to "state to a FISA court judge that the records requested are in connection with a terrorist investigation. The assertion alone is sufficient: the FISA judge has no authority to reject this application." [3]

An article published in *The New York Times* on December 12, 2002, recounts a national teleconference of thousands of librarians worried about the implications of the PATRIOT Act's sweeping ability to force libraries to surrender records of patrons. Despite the fact all speakers for the conference agreed that requests, accompanied by a legitimate court order, should be properly processed, they also admonished librarians to keep as few records as possible and the records they did keep were to be "promptly destroyed after use." [4]

According to the Electronic Frontier Foundation, in the years following September 11, 2001, the FBI sought patron information from more than 200 libraries [5]. One instance recounted by Joan Airoldi, director of the Whatcom County Library in Bellingham, Washington, tells us of the FBI's attempt to procure records of "persons who had borrowed the book *Bin Laden: The Man Who Declared War on America*, written by Yossef Bodansky." [6, p. 26] The FBI agent seeking information showed up at the library and initially requested records without a subpoena or a satisfactory explanation as to need. The request was passed to management, who then contacted counsel. The agent was subsequently contacted by library counsel to gather more information, at which time they learned of a handwritten note in the margin of the book (which was found to be an almost direct quote from Bin Laden during a 1998 interview); the agent was told that library records would not be released without a subpoena. The library received a grand jury subpoena, at which time the Board of Trustees decided to fight the subpoena.

In the instance of Whatcom County Library, the grand jury subpoena was quashed on the grounds of First Amendment rights and no substantial connection between a grand jury proceeding and the information requested as well as "libraries have the right to disseminate information freely, confidentially, and without the chilling effect of disclosure." [6, p. 26] This library system's story only became public because it was a grand jury subpoena and not a PATRIOT Act subpoena. The grand jury subpoena did not include a gag order, but the PATRIOT Act's provisions include automatic gag orders for all parties involved. Another provision of the PATRIOT Act removes the right of any party to challenge a PATRIOT Act subpoena in court. "Had the FBI secured a Section 215 order (of the PATRIOT Act) from the Foreign Intelligence Surveillance Court, the search would have gone forward and nobody – not even the patrons whose records had been examined – would have known it happened." [7] This particular library system's initial policy for keeping patron records was a maximum of 30 days. Since this incident, they have changed that policy to seven days.

Technology's Effect on Reader Privacy

The introduction and use of computers and associated technologies has allowed the government to keep exceptionally detailed records about businesses and persons; computers also now house thousands of pieces of data that can be easily compromised or accessed if proper steps are not taken to protect them. The widespread use of this and similar technology has allowed users to keep bank statements, purchase receipts, digital journals, photos and more on personal and business computers. The browsers we use (such as Internet Explorer, Firefox and Chrome) to access the Internet can also tell authorities or a third party about user interests by examining the history of searches and the cookies stored on computers by websites.

Bit by bit (pun intended) our lives and even our personalities can be pieced together by those with the inclination to do so. All of these details

The breadcrumbs we leave behind in the digital world can paint a very accurate and detailed picture of who we are, who we were, who we want to be, our health issues, political affiliations and personal interests.

can also be misinterpreted and misconstrued by those same parties. The breadcrumbs we leave behind in the digital world can paint a very accurate and detailed picture of who we are, who we were, who we want to be, our health issues, political affiliations and personal interests.

The advances in technology regarding electronic readers (e-readers from this point forward) bring to the forefront the legislative need to update reader privacy laws to reflect the impact that technology has on record keeping and the possibility of these records being used improperly. Computer technology allows physical bookstores, libraries and Internet-based stores to store more information than before the so-called *digital age*. Digital books are becoming more commonplace as e-readers become more affordable. According to Cindy Cohn, legal director of the Electronic Frontier Foundation, "[d]igital books are now outselling paperbacks on Amazon.com, readers are turning to online services like Google Books, and analysts expect that over 18 million e-readers will be sold in 2012." [8] These digital devices, half the weight of a hard cover book, allow users to carry hundreds of books, complete with marginal notes wherever they may go.

Amazon's Kindle allows users to write notes in the margins of their purchased books. These notes are also stored in Amazon's cloud computing environment along with records of purchases and detailed browsing histories that can include how long a page was viewed. Kindle also allows users to highlight passages of interest for their own notes or to share with friends via Twitter or Facebook. This information can be considered sensitive due to the fact it can give insight into the reader's interests, which some members of society (and the government) may not approve of. One example mentioned in much of the literature reviewed was the instance of the McCarthy hearings of the 1950s. "Sensitive reader information can and does come under fire. During the McCarthy hearings, Americans were questioned about whether or not they had read Marx or Lenin." [5]

Another service related to electronic books and readers is Google Books. Google Books allows users to purchase titles that can be accessed on multiple mobile devices. Purchases are stored in the digital cloud, which according to Google Books' overview has an unlimited amount of storage space. [9] According to the objection filed by Privacy Authors and Publishers to the original settlement in The Authors Guild vs. Google, Google has "no limitations on collection and use of reader information and no privacy standards for retention, modification, deletion or disclosure of that information to third parties or the government. Without those limitations, an unprecedented quantity of information about readers' activities will be and indeed already is being collected. Google Book Search can link a reader to every book searched for, browsed, purchased and read. It even tracks which particular pages the user reads and for how long." [p.10, 2]

Conclusion

The rate at which the public now creates data bits for marketers, businesses and government agencies to follow is exponential when compared to the years before widespread computer use and the Internet. User names, log-in IDs, passwords, cookies, IP address tracking, click-tracking and a myriad of other items used by technology could easily be used to piece together an accurate picture of our personal lives, health concerns and interests. The rate at which the public uses material available online, such as journals, magazines, newspapers, research papers and books, begs to be addressed in legislation when such information can be used to infiltrate and ruin the lives of law-abiding citizens.

Intellectual freedom is a right to freedom of thought and expression of thought. It fosters innovation and ingenuity and accounts for our democracy, our technical advances and our current way of life. To ignore the fact that digital/electronic services offering sales of books or lending options need

the same protections as brick and mortar libraries is to invite the government into the private lives of every citizen who has ever made an online purchase of any book, electronic or not. As seen in the case of Whatcom Library, no thought other than terrorism was given as to why a book may have been checked out. For all anyone in that case knew, the person that wrote in the margin or checked out that book may have been interested in the psychology of Bin Laden for a research paper for a high school class. While some people may think this is fear-mongering all its own, we can thank our own government for such thoughts and feelings. They use the same tactics every day to chill the public's outcry in regard to rights being slowly eroded. For those that claim disinterest or lack of concern for the digital reader, I would ask that they purchase a few books on Al Qaeda, Bin Laden or any other terrorist organization to see if it piques the interest of the FBI and the Department of Homeland Security or the NSA. Do we really want to wait until it is too late to protect our innovative, free thinkers who can change the world for the better in the name of security? ■

Resources Mentioned in the Article

[1] Ozer, N. (March 2010). *Digital books: A new chapter in reader privacy.* ACLU of Northern California. Retrieved from www.aclunc.org/issues/technology/asset_upload_file295_9047.pdf

[2] Campaign for Reader Privacy. (2005). *A brief history of library and bookstore surveillance before 9/11.* Retrieved from www.readerprivacy.org/info.jsp?id=5

[3] Campaign for Reader Privacy. (2005) *How Section 215 threatens reader privacy.* Retrieved from www.readerprivacy.org/info.jsp?id=2

[4] Clymer, A. (December 2, 2002).Threats and responses: Privacy; Librarians get advice on handling government requests for information on readers." *The New York Times.* Retrieved from www.nytimes.com/2002/12/12/us/threats-responses-privacy-librarians-get-advice-handling-government-requests-for.html

[5] Electronic Frontier Foundation. (March 30, 2011). Reader Privacy Act introduced to upgrade book privacy for the digital era [press release]. Retrieved from www.eff.org/press/archives/2011/03/30

[6] Airoldi, Joan. (2006). Case study: A grand jury subpoena in the PATRIOT Act era - One library's lesson." *Library Administration & Management, 20*(1), 26-29. Retrieved from https://journals.tdl.org/llm/index.php/llm/issue/view/101

[7] Campaign for Reader Privacy. (2005). *What we know about bookstore and library searches since 9/11.* Retrieved from www.readerprivacy.org/info.jsp?id=4

[8] Electronic Frontier Foundation. (April 5, 2011). *Letter [to the Honorable Leland Yee] in support of SB 602 (Yee), The Reader Privacy Act.* Retrieved from www.eff.org/files/filenode/sb602/SB602EFFsupportletter.pdf

[9] Google, Inc. (n.d.). *Google Books: Overview.* Google.com. Retrieved from books.google.com/help/ebooks/overview.html

[10] Privacy Authors and Publishers' Objection to Proposed Settlement at 2, The Authors Guild, Inc., v. Google, Inc., No. 05 CV 8136-DC (S.D.N.Y. Filed Sept. 9, 2009); Fairness Hearing Transcript at 60, The Authors Guild v. Google, No. 05 CV 8136-DC. Retrieved from www.thepublicindex.org/wp-content/uploads/sites/19/docs/letters/privacy_authors.pdf