Wesley Teal

10 December 2012

A Moving Target: Privacy, Libraries, and Mobile Technology

The proliferation of mobile devices* among Americans is rapidly changing the ways in which individuals interact with information. Some of these changes, where they improve an individual's ability to engage in the local, national, and even international cultural and information landscapes, are beneficial. However, these benefits often come at the cost of an individual's right to privacy. Librarians as traditional curators of culture and information as well as protectors of privacy have an important role to play in aiding individuals, corporations, and government bodies in ensuring that the right to privacy is not sacrificed on the alter of mobile technology.

Why Privacy?

In a time when people regularly share the ins-and-outs of their daily lives on Facebook, Twitter, or their blogs, when people regularly google each other to see what they can learn, concern about privacy seem almost irrelevant. Indeed, there are more than a few people who believe that privacy is only important for those doing illicit activities. This sort of sentiment is reinforced by the 2009 statement of Google's then-CEO Eric Schmidt who said that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (Popkin, 2010, para. 7).

Such a lackadaisical approach to privacy, while not uncommon, is not necessarily well thought out. First, it assumes that all activities that are currently illegal or socially unacceptable are inherently wrong. Never

* For the purpose of this paper, the term mobile devices include smartphones, tablets, certain audio players like the iPod Touch, and e-readers. For the sake of scope, this paper excludes laptops, traditional cellphones, pagers, and other devices that, while mobile, don't necessarily to share all the privacy concerns and usage patterns of mobile devices as defined herein.

mind that our laws and social mores now allow for activities like abortion, interracial marriage, homosexuality, and women's suffrage, that were all once illegal, yet are all legal and, to varying degrees, acceptable in today's society. Never mind that there are still lesbian, gay, or transgendered individuals who wish to keep their sexual or gender identity private to preserve family relations, work situations, or to protect themselves from the kind of violent hate crimes that allegedly include the 2011 beating of a Kentucky man (Barrouquere, 2012) and the alleged forced captivity of a North Carolina man (Faith In America, 2012).

Second, such a dismissal of privacy assumes that a desire for privacy stems only from illicit behavior. Individuals avoiding a stalker, an abusive former partner, and those enrolled in witness protection programs all have legitimate reasons to seek privacy even when their own behavior is irreproachable. The same is true for those receiving medical or psychiatric care, children who wish to learn about or do something that, while legal, their parents would disapprove of, those seeking the perfect surprise gift for a loved one, and myriad other people who, for their own mundane reasons, prefer to keep their actions and thoughts to themselves. Likewise, publishing one's location, which is supported by social networking sites like Foursquare, Facebook, and Twitter, can be highly dangerous even for those unconcerned with privacy. Foursquare has been used as a stalking tool in at least one instance and burglars have used Facebook Places to find out when people were not in their homes (Cyrus and Baggett, 2012, p. 290).

Third, dismissing privacy as unimportant ignores the long-standing legal basis for a right to privacy. In 1890, attorneys Samuel D. Warren and Louis Brandeis, who would later serve on the Supreme Court, outlined the Common Law basis for a right to privacy in the *Harvard Law Review*. Warren and Brandeis (1890) cite a 1769 court case to establish that the "common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others" (p. 198). The legal protection of privacy, they note, had to that point been largely based on property rights arguments (p. 204) and on asserting the binding nature of implicit contracts (p. 207-210), but ultimately rests on a broader "right of the individual to be let alone" based on the principle of "inviolate personality" (p. 205).

In 1960, Prosser published a review of cases related to privacy since Warren and Brandeis's landmark argument. Prosser noted that from the 1890s until the 1930s, the existence of a right to privacy was alternately supported and dismissed in various court cases, but began to become a firm part of American law in the late 1930s (p. 385-386). Prosser also noted that the right to privacy in was formally recognized by 26 states and the District of Columbia and that only three states openly rejected the right by 1960 (p. 386-388). Prosser's review draws the conclusion that the right to privacy is individual, personal, and nontransferable (p. 408-409) based on an aggregate of four separate but related rights: the right to keep one's private life free of intrusion, the right to keep embarrassing private facts from public knowledge, the right not to be portrayed falsely in public, and right to protect one's name and likeness from unauthorized appropriation (p. 389).

The right to privacy has also been asserted to be a Constitutional right, stemming from the Bill of Rights, in a number of Supreme Court cases including *Griswold v. Connecticut* (1965), *Roe v. Wade* (1973), and *Lawrence v. Texas* (2003) (DeCew, 2012). Justice Douglas details the origin of the right to privacy in *Griswold v. Connecticut*, in which he echoes Prosser's assertion that the right to privacy is the sum of many elements

> Various [Constitutional] guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." (para. 12)

Thus, it can be seen that protecting the right to privacy is an important part of America's moral and legal framework. Yet with the rise of mobile devices, which have increased the ease at which personal data can be collected via the internet, privacy faces a broad new set of challenges. The question is how to balance the bright promise that mobile technology holds for communication and the exchange of information and culture with the need to protect privacy.

The Promises of Mobile Technology

In the era of mobile technology the ability to access and share information, knowingly or not, has become almost effortless. With an iPhone or similar smartphone, one can call friends, family, and colleagues, surf the web, take photographs, get directions, read a book, and post on social networking sites, all while carrying-on all one's day-to-day activities. GPS-enabled devices (most smartphones) allow users to pinpoint their location and get accurate directions even when they have no idea where they are. E-readers allow individuals to carry around large libraries in their pockets and to purchase books or check them out from a library anywhere internet access is available. This unprecedented ease of access to information and communications technology has created an environment where seemingly limitless knowledge is available instantaneously.

The Risks of Mobile Technology

Unfortunately, instant information is not only available *to* end users, it is also available *from* them. The same technology that allows GPS devices and Google Maps to identify a person's location and give that person meaningful directions also allows for a person's every move to be easily tracked. With the ability to purchase and download books anytime, anywhere on an e-reader, also comes the detailed monitoring of a person's reading behavior. According to the *Wall Street Journal*, all major e-readers (Kindle, Nook, Kobo, and even iPad apps) track a wide array of users reading habits and report those habits back to the manufacturer (Alter, 2012). With an estimated 40 million e-readers and 65 million tablets in the United States alone (Alter, 2012) the amount of data that is being gathered and stored is staggering. The Electronic Frontier Foundation (2012) also notes that most e-book and e-reader services not only mine their users for information, but are also free to distribute the collected information with other companies without getting their users' consent.

Geo-location presents another problem for user privacy. Apple changed its privacy policy in 2010 to enable it to share personal location information with other companies. Although Apple claimed the data would be anonymous it would lack direct control over how information was used after it had been shared and it has been previously shown that individuals can be identified through large behavioral data sets like the one Apple is collecting (Cyrus and Baggett, 2012, 290-291). In 2006, AOL released a large set of search queries grouped by individual searcher. After public outcry about the level of personal detail revealed by the search queries of “anonymous” individuals, AOL recalled the dataset while still asserting that the release of information “'wasn't a violation of the AOL privacy policy” (Hansell, 2006). When Netflix released a similar dataset in the same year, academic researchers were able to identify several Netflix users by correlating the dataset with other publicly available information mere weeks after the data’s release (Wicker, 2012, p. 65). Additionally, using mobile apps to check in at locations can open one up to being easily stalked or to notifying criminals of when one is away from home. Such problems have occurred: a woman calling herself Sylvia told *The Guardian UK* how she was stalked via Foursquare and industrious burglars in Nashua, New Hampshire, broke into more than 50 homes they knew to be empty thanks to Facebook Places, and stole more than $100,000 worth of goods (Cyrus and Baggett, 2012, p. 290).

Further trouble can arise when a person installs malicious software that surreptitiously collects personal data without a user's knowledge. A number of these applications have been found both on Android devices and Apple's mobile devices (Cyrus and Baggett, 2012, p. 290). *USA Today* reported that in December, 2011, F-Secure, an anti-virus company, had found 1,639 malicious apps for Android devices (Acohido, 2012). Unlike Android apps, apps on Apple’s iOS devices must undergo an audit before being distributed, but in July, 2012, an app that harvested information from people’s address books for spammers was found in the Apple App Store (Kingsley-Hughes, 2012).

The ease at which individuals, companies, and organizations can engage in data collection becomes increasingly worrisome when people like former CEO and current Executive Chairman of Google, the internet giant behind the popular Android mobile operating system, declare that anyone who wants to keep an activity private should simply cease doing it (Popkin, 2010, para. 7). Such statements suggest that Google, or at least Schmidt, feels entitled to know anything and everything they can learn about a person. The anti-privacy stance that seems prevalent among companies and organizations that gather data is all the more reason for working hard to ensure patron privacy.

What Libraries Can Do

The potential value and potential risks of mobile technology place libraries and librarians in an awkward position. On the one hand, mobile devices, particularly e-readers, provide a new way for libraries to engage with and serve their communities. On the other hand, libraries have traditionally served as protectors of patron privacy. Indeed, the *Code of Ethics of the American Library Association* declares “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” (ALA, 2012). The inherent lack of privacy in the use of e-books threatens to undermine the credibility of libraries if they provide e-books without being clear to their patrons about the sorts of information that will be gathered if they choose to check out an e-book.

Despite the risk to privacy posed by e-readers and other mobile devices used in conjunction with library services, there is a surprising paucity of material published on the subject in library-centric publications. Discussion of privacy issues surrounding e-readers makes up only a small percentage of the discourse on e-books and e-readers, particularly in formal publications. Discussions of privacy concerns with other mobile devices in the context of library services are even more rare. However, there are some in the library and information science field that are trying to establish best practices in regard to e-readers and mobile devices.

To deal with the particular challenges mobile technologies present to libraries, an important first step is to ensure that one's library has an established privacy policy that presents a well thought-out and systematic approach to privacy in all areas of the library's service, including the use of mobile devices with regard to library services. Deborah Caldwell-Stone (2012) advocates such an approach, saying that librarians need to ensure their professional standards and policies are up-to-date and address new technologies and digital content (p. 61). Theresa Chmara (2012) stresses the importance of consulting with legal council in drafting a comprehensive privacy policy for libraries (p. 64). Caldwell-Stone (2012) further suggests that librarians create new guidelines, FAQs, and tool kits that will allow not only themselves, but also other librarians to better assess and understand the privacy implications of different technologies and the privacy policies of vendors (p. 61). Implicit in this suggestion is the importance of maintaining open communication between librarians as they navigate the new and evolving world of mobile technology.

In addition to establishing coherent and comprehensive policies in one’s own library, its important to be involved in the broader policy discussion. Cyrus and Baggett (2012) suggest librarians need to stay informed about the trends in mobile technologies and their implications for privacy and about state and federal legislation regarding privacy or mobile devices (p. 292-293). Such trend monitoring, they note, has become much easier thanks to internet technologies like (mobile-friendly) RSS feeds and Twitter (p. 293). By keeping abreast of technological and political trends, librarians will be better able to act as advocates for their patrons. Informed librarians with strong standards will be better able to, as Caldwell-Stone (2012) suggests, perform a “thorough examination of technologies, platforms, and agreements that control the delivery of digital content to identify problematic features” and work with vendors, as well as legislators and regulators, to make sure that technologies and laws property protect the privacy of mobile device users (p. 61). Chmara (2012) suggests libraries write their privacy policies into vendor contracts (p. 65). Cyrus and Baggett (2012) also note that advocacy needs to take place not just with vendors and higher government, but within libraries, within cities, and at the state level (p. 294). By working with organizations like the American Civil Liberties Union and the Electronic Frontier Foundation that have an interest in protecting privacy and/or in the social implications of new technology, librarians may be able to amplify their advocacy.

Another important way librarians can continue to protect patron privacy is through patron service and education. On the service side, Cyrus and Baggett (2012) suggest assisting patrons in configuring the privacy settings on their devices and on social networking sites (p. 294). On the education side, librarians have a number of means open to them. The simplest, is signage, either traditional or via digital displays, to keep patrons aware of privacy concerns (p. 293). Incorporating privacy content or discussions into existing educational programming on technology or even creating educational programming specifically about privacy are other options (p. 294). Additionally, participating in the ALA’s Choose Privacy Week and making mobile and e-book privacy a prominent part of that week’s programming is another way for librarians to make sure their patrons are well informed.

Another solution to patron privacy may come from Jamie LaRue and the Douglas County (Colo.) Libraries. In an effort to deal with the rising costs of e-books, the Douglas County Libraries now insist on buying actual copies of e-books, not simply paying to access them through a third party, as has been the norm (LaRue, 2012). Although LaRue’s experiment is not necessarily aimed at protecting patron privacy, by cutting out third-party content control in favor of self-distributing e-books (as libraries have always done with non-electronic media), libraries can reclaim control over their collections. Additionally, LaRue's experiment utilizes the Adobe Content Server (LaRue, 2012, para. 5) which doesn't record user information (EFF, 2012). This control can potentially be used to ensure that companies other than e-reader providers cannot easily track a patron's reading habits. By having access to the e-book files, some intrepid librarian-programmer may eventually be able to attach a bit of code to each file that interferes with e-reader tracking software.

Sarah Houghton has put the most extreme solution forward to the problems surrounding e-books in particular in her blog *Librarian in Black*. Houghton (2012) likens e-books to a bad boyfriend and declares that she intends to cease her library's contract with e-book distributor Overdrive as soon as legally allowed by their contract. Houghton acknowledges that her patrons want e-books but counters

> does that mean that we trade away our core values and ethics to provide *anything*, under *any* terms? Does it mean that we spend our residents' limited tax dollars on sub-par products with sub-par usage terms and no ownership or longevity guarantees? Or is the fact that people want eBooks from their libraries and we can't get them going to turn out to be enough reason to stop the madness and engage in a massive national boycott of the societal conflagration that we are faced with for the future of digital information? (para. 13)

If the only option for libraries interested in providing mobile services and e-books is to surrender their patrons' right to privacy in exchange for expensive, unreliable service, canceling all such services may be the best option available for some libraries. As suggested in Houghton's blog, withdrawing from the e-book world entirely will likely be most effective in conjunction with broader boycott and advocacy campaigns.

Conclusion

In a world where tracking personal behavior seems to be getting easier by the day, privacy is more important than ever. Libraries and librarians have traditionally been guardians of privacy, but the rising popularity of e-books and other e-content threaten to make libraries just another data farm pumping patron information into far away servers. Ultimately, libraries that offer e-books or other mobile services without making sure such services don’t violate patrons’ privacy betray their patrons and the ALA *Code of Ethics*. They cast aside their traditional role as protectors of privacy and become participants in its destruction. Therefor it is necessary to approach mobile technology with a sober, informed caution. E-books and other mobile devices offer many new ways for libraries and patrons to engage with each other, and with the informational and cultural resources libraries provide. It is up to librarians to ensure that the price paid for such benefits doesn’t include our patrons’ personal information. Or their trust.

References

Acohido, B. (2012, March 4). Poison text messages and malicious mobile apps on the rise. *USA Today*. Retrieved from http://usatoday30.usatoday.com/tech/news/story/2012-03-05/mobile-security-threats/53357486/1

Alter, A. (2012, July 19). Your E-Book Is Reading You. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052702304870304577490950051438304.html

American Library Association (2008, January 22). Code of Ethics of the American Library Association. *American Library Association.* Retrieved from http://www.ala.org/advocacy/proethics/codeofethics/codeethics

Barrouquere, B. (2012, October 20). Witness: Pair plotted to kill gay man in Kentucky. *San Francisco Chronicle*. Retrieved from http://www.sfgate.com/news/crime/article/Opening-arguments-begin-in-hate-crime-trial-3959083.php

Caldwell-Stone, D. (2012, May). A Digital Dilemma: E-books and Users' Rights. *American Libraries 43(5/6)*, 60-61.

Chmara, T. (2012, January). Privacy and E-Books. *Knowledge Quest 40(3)*, 62-65.

Cyrus, J. W. W. and Baggett, M. P. (2012). Mobile Technology: Implications for Privacy and Librarianship. *Reference Librarian 53(3)*, 284-296).

DeCew, J. (2012). "Privacy." *Stanford Encyclopedia of Philosophy*. Retrieved from http://plato.stanford.edu/entries/privacy/

Electronic Frontier Foundation (2012). E-Reader Privacy Chart, 2012 Edition. Retrieved from https://www.eff.org/pages/reader-privacy-chart-2012

Faith in America (2012). Faith in America seeks hate crimes investigation into allegations made against N.C. church. Retrieved from http://us2.campaign-archive2.com/?u=e2bbf638ef2297cb0709a63be&id=c24f30906f

Griswold v. Connecticut, 381 U.S. 479 (1965). Retrieved from Cornell University Law School, Legal Information Institute website: http://www.law.cornell.edu/supct/html/historics/USSC_CR_0381_0479_ZO.html

Hansell, S. (2006, August 8). AOL Removes Search Data On Vast Group Of Web Users. *New York Times.* Retrieved from http://query.nytimes.com/gst/fullpage.html?res=9504E5D81E3FF93BA3575BC0A9609C8B63&smid=pl-share

Houghton, S. (2012, August 1). I'm breaking up with eBooks (and you can too) [Web log entry]. Retrieved from http://librarianinblack.net/librarianinblack/2012/08/ebookssuckitude.html

Kingsley-Hughes, A. (2012, July 6). First iOS malware hits App Store. *Forbes*. Retrieved from http://www.forbes.com/sites/adriankingsleyhughes/2012/07/06/first-ios-malware-hits-app-store/

LaRue, J. (2012, January 17). Dear Publishing Partner [Web log entry]. Retrieved from http://jaslarue.blogspot.com/2012/01/dear-publishing-partner.html

Popkin, H. A. S. (2010). Privacy is dead on Facebook. Get over it. *Technotica on NBCNews.com.* Retrieved from http://www.msnbc.msn.com/id/34825225/ns/technology_and_scie nce-tech_and_gadgets/t/privacy-dead-facebook-get-over-it/#.UIQZDBimWog

Prosser, W. L. (1960, August). Privacy. *California Law Review, 48(3)*, 384-423.

Warren, S. D. and Brandeis, L. D. (1890, December 15). *Harvard Law Review*, *4(5)*, 193-220.

Wicker, S. B. (2012, August). The Loss of Location Privacy in the Cellular Age. *Communications of the ACM, 55(8)*, 60-68. doi:10.1145/2240236.2240255