Legal Landscape of Consumer/User Data Privacy and Current Policy Discussions

Krista L. Cox, Director of Public Policy Initiatives, Association of Research Libraries

Introduction

Privacy has long been deemed an essential right, but this right has been threatened by current practices in the digital era, in which vast swaths of data are collected from individuals each day. Although privacy is not directly mentioned in the United States Constitution, courts, including the Supreme Court of the United States, have recognized a right to privacy based on the First, Fourth, and Fourteenth Amendments. Additionally, numerous states explicitly provide for a right to privacy in their constitutions or through state laws. Privacy, which was famously defined as a right to be left alone,[1] relates to a number of areas of everyday life, including family, health, and—of particular importance to library—the ability to seek and impart information.

The American Library Association's (ALA) Library Bill of Rights explicitly recognizes that, "All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information."[2] In interpreting this right, ALA defines privacy in the library context as "the right to open inquiry without having the subject of one's interest examined or scrutinized by others." ALA widely applies the right to privacy to search records, reference questions, circulation records, and personally identifiable information about uses of services and materials. ALA also notes, "best

"Privacy, which was famously defined as a right to be left alone, relates to a number of areas of everyday life, including...the ability to seek and impart information."

practice leaves the user in control of as many choices as possible" and that libraries should refrain from sharing personally identifiable information with third parties or vendors without permission from the users.[3]

While patron privacy has long been a fundamental value to libraries, the digital world complicates traditional notions of privacy because of the vast amounts of data collected when users encounter technology. In the digital age, research libraries are tasked with addressing broader privacy concerns than in the analog world because they must account for more than the records libraries themselves create and keep, but also the personal data that may be collected by services, applications, and vendors that libraries work with. Indeed, this personal data can prove valuable for third-party vendors and services, but also for libraries seeking to enhance user experience. Libraries today must carefully consider how to balance core values of privacy—and the inherent trust that is placed in them by patrons—with improved delivery of service to their users.

"Libraries today must carefully consider how to balance core values of privacy...with improved delivery of service to their users."

As libraries evaluate best practices to protect patron privacy in the digital era and policy makers determine how to move forward with legislation to protect consumers, it is clear that there are no easy answers. All stakeholders and policy makers in the privacy debates must consider a range of complicated issues. Some of the biggest issues to consider in determining what elements should be included in a comprehensive, consumer privacy regime are:

- **How broadly should the law apply?** In order to avoid the current problems with the sectoral approach, a comprehensive solution must address broader privacy issues. Stakeholders in the privacy debate have differed as to whether federal privacy laws should apply solely to the technology sector or to all companies;

whether federal laws will only apply to companies of a certain size, in order to ensure that compliance costs are not overly burdensome for new entrants to the market; whether there should be carve outs for certain types of companies or data.

- **What types of data will the law apply to?** Policy makers must determine whether to create different classes of data or treat specific types of consumer data differently. While some advocate for "sensitive" data, such as medical data, to have heightened protections, others note that with interconnected systems and the ways data is shared today, such distinctions may be meaningless. Additionally, many advocates have raised concerns about the use of de-anonymized data, pointing to studies that have precisely identified individuals or connected users with personal information through aggregation of supposedly anonymous information.
- **What rights will be guaranteed?** From the outset, policy makers must determine which rights a federal bill will cover. While the right to information or transparency seems to be non-controversial, will consumers have rights to access, portability, correction, restriction, erasure, minimization, and objection? How broadly will these rights be framed and to what type of data will it apply? What exceptions might exist to these rights? From a library perspective, a right to erasure/deletion, which in the European Union (EU) is also framed as a right to be forgotten, raises particular concerns with respect to accurately preserving the cultural and historical record. The right to be forgotten has inherent tensions with the First Amendment rights under the United States Constitution and also raises ethical concerns. The right to delisting, meaning that it cannot be indexed in a search engine, is a related concern which alters accessibility and discoverability of the information.
- **What do meaningful notice, transparency, and consent mean?** While all stakeholders appear to agree that notice and

transparency are critical features of any privacy law, in order to make these elements meaningful, users must be able to easily access and understand what data is being collected and how it is being used prior to such collection. One issue that has been hotly debated is whether opt-out systems should satisfy consent requirements, or whether default opt-in provisions should be required. Another question is whether terms of service that are framed as a take-it-or-leave-it policy allow for meaningful consent.

- **Who will enforce the legislation and what remedies should be provided?** Most stakeholders agree that the Federal Trade Commission (FTC) is the most logical agency to enforce violations of a federal consumer privacy framework. Indeed, bills such as Senator Ron Wyden's draft (discussed more below), would provide for increased hiring at the FTC to investigate and enforce violations. The fines that the FTC could impose and whether criminal sanctions are appropriate are issues that policy makers will debate. Additionally, policy makers must determine whether to leave enforcement solely in the hands of government agencies, or whether to create a private right of action that allows citizens to bring companies to court for failure to comply with federal privacy laws.
- **What safe harbors should be granted to companies for complying with legislation?** Depending on the remedies provided in federal legislation, some stakeholders have noted that safe harbors may be necessary to provide assurances for companies that, as long as they comply with particular requirements, they will not face extensive penalties for security or other breaches.
- **Should the federal baseline be a floor or ceiling?** Preemption is another issue that policy makers must confront and determine whether any federal legislation should be a floor or a ceiling. If federal legislation serves as a ceiling, states would be prohibited

from enacting more stringent rules. Should federal legislation fail to provide meaningful data protection, states may wish to provide further privacy protections for their citizens. However, by allowing states to create stronger privacy rules, companies and organizations will continue to run into a patchwork system.

- **Will federal legislation provide incentives for privacy research and development?** Some advocates for a federal framework have urged for inclusion of incentives for cybersecurity research and development of new models to address privacy concerns. Some have noted that incentives for companies to proactively protect data and prevent security breaches will better serve consumers than systems that simply rely on notice or after-the-fact disclosures.

As will be discussed further below, there are no easy answers nor consensus around these issues. However, stakeholders and policy makers are determined to move discussions around privacy forward, with many holding an ultimate goal of creating new legislation in the United States in 2019.

Current Privacy Landscape in the United States

Federal Approach to Privacy

The legal privacy landscape in the United States currently can be described as a patchwork system, at best, that relies on sector-specific federal laws and widely divergent state legislation. The United States does not currently have a comprehensive consumer privacy law, meaning that different types of data are treated differently and there is no baseline standard for consumers to expect protection of personally identifiable information. Privacy laws currently existing at the federal level are sector-specific, such as the Health Insurance Portability and Accountability Act (HIPAA) covering protected health information, or the Family Education Rights and Privacy Act (FERPA) covering certain student records, or the Gramm-Leach-Bliley Act covering consumers' financial information. This sectoral approach, however,

creates compliance problems, with different classes of data and varying standards of privacy. It also results in gaps and inconsistencies regarding how the same data may be treated, depending on where it is shared or conveyed. Many policy makers have expressed an interest in addressing these gaps through enactment of comprehensive federal privacy legislation.

While there appears to be an increased interest and urgency in creating a federal standard, it should be noted that the FTC has repeatedly called on Congress to enact comprehensive privacy laws to protect consumers for nearly two decades.[4] The FTC has long advocated federal regulation, in part because the Fair Information Practice Principles (FIPPs) are principles and not enforceable as law, though the commission can police certain behavior deemed unfair or deceptive. While FIPPs provide an excellent starting point as guiding principles for companies engaged in data collection, compliance is largely voluntary. As a result, the United States has largely relied on market mechanisms to protect consumer privacy. In other words, the US has operated under the assumption that if consumers were unhappy about privacy policies or data collection practices, companies would be forced to change. Unfortunately, reliance on market corrections has not resulted in the changes that users would like, in part because privacy policies or terms of services are often hidden, not accessible until after signing up for the platform, or are lengthy and legalistic documents that do not plainly explain data collection practices. Users often do not fully understand what data is collected, how it is used, who else can view it, or whether they can opt-out.

> "The legal privacy landscape in the United States currently can be described as a patchwork system, at best, that relies on sector-specific federal laws and widely divergent state legislation."

In 2012, the Obama Administration released its report, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*,[5] largely based on

FIPPs. The purported intention behind the report's release was to call on Congress to enact the Consumer Privacy Bill of Rights contained within the paper into legislation. President Obama noted in the report:

> Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times....
>
> One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.[6]

Ultimately, Congress did not act on the Obama Administration's report and the United States still lacks comprehensive consumer privacy protections.

The FTC does oversee internet privacy through its authority over "unfair or deceptive acts or practices in or affecting commerce."[7] These FTC cases generally result in a settlement with the companies due to the lack of authority to impose civil penalties unless the company has violated an existing FTC order.

State Approach to Privacy

While states each have their own privacy laws, these laws are often older, do not address the swaths of data that exist in the digital age, or are limited in scope. Like the federal approach, where states have enacted laws addressing privacy in the digital environment, they are generally narrowly focused and target discrete populations or are sector-specific. For example, California and Delaware have

specific laws aimed at protecting the privacy of minors.[8] Many states, including Arizona, California, Delaware, and Missouri have specific laws governing e-reader privacy, which vary from protecting library patron records to more generally applying to all e-book browsing, including from commercial bookstores.[9] Several states, including California, Connecticut, Delaware, Minnesota, Nevada, and Oregon, also address privacy policies for websites or for personal information held by internet service providers. All states now have some form of data breach notification laws, and some states have amended these rules in recent months. While these states have addressed important issues related to online privacy, with the exception of California's recently enacted privacy legislation, these laws do not comprehensively address consumer data collected during the everyday course of using online services, platforms, and applications.

> "While states each have their own privacy laws, these laws are often older, do not address the swaths of data that exist in the digital age, or are limited in scope."

More recently, attention to comprehensive consumer privacy has increased as a result of the European Union's General Data Protection Regulation (GDPR) (discussed in greater detail below). Soon after GDPR went into force, California quickly enacted the California Consumer Privacy Act of 2018 (CCPA).[10] This bill, scheduled to go into effect in 2020, purports to follow GDPR in many respects, but is narrower in scope than its EU counterpart and has come under a wave of criticism from nearly all stakeholders involved. CCPA focuses on the collection of data and—in contrast to GDPR—limits its application only to certain companies: those with gross revenue exceeding $25 million, or that sell data on more than 50,000 consumers each year, or derive 50% or more of their revenue from selling personal data. Ultimately, many criticized the rush to enact the legislation, with virtually no time for close analysis or meaningful debate.

From a consumer advocacy perspective, CCPA has been criticized as a weakened version of GDPR, heavily relying on notice provisions, rather than requiring consumers to opt-in to data collection and processing; for providing only limited availability to data portability; for including at least a limited right to deletion or right to be forgotten; for applying only to a specific definition of "businesses"; and, in some respects, for lacking appropriate enforcement mechanisms. On the other hand, some have criticized CCPA as overly expansive in its application by eliminating the distinction between sensitive and non-sensitive personal information or by requiring high costs for compliance, thereby disadvantaging smaller technology companies.

While other states do not have comprehensive consumer privacy legislation in place, several are reportedly considering it.[11] Washington State, for example, is currently considering the Washington Privacy Act.[12] This bill would apply to personally identifiable data, but largely excludes de-identified data. It includes provisions on the right to access, the right to delete and the right to opt-out. It also specifically governs facial recognition technology. The Washington Privacy Act, as currently drafted, would empower the state Attorney General's office to enforce its provisions, but would not create a private right of action for consumers. Regardless of the provisions that might be included if the Washington Privacy Act becomes law, it is clear that there would be stark differences between this bill and CCPA, as well as GDPR. Other state legislation is also likely to have small and large differences, resulting once again in a patchwork of state provisions governing different aspects of consumer data, with different standards of protection.

International Privacy Developments

Consumer data privacy has been a topic of active discussion internationally, as well. Most notably, in 2018, the EU's General Data Protection Regulation (GDPR) went into effect and has resulted in a domino effect in terms of compliance by private businesses as well as new legislation in other countries.

Although GDPR applies to EU citizens and residents, it affects companies and organizations worldwide both because of ties to those in the EU, as well as the practical difficulties in handling EU personal data differently from personal data collected in other parts of the world. GDPR grants individuals six specific rights with respect to their data:

1. Information and access (the right to know that their personal data is being processed and have access to this data free of charge)
2. Data portability (data collected under certain circumstances must be provided "in a structured, commonly used, and machine-readable form"
3. Rectification (ability to correct inaccurate personal data or to complete information)
4. Erasure (also known as the "right to be forgotten," applicable only under certain circumstances)
5. Restriction (individuals may restrict data controller from processing data further under certain circumstances)
6. Objection (the right to object to processing of one's data)

Significantly, GDPR requires explicit consent from the user for collection and processing of data in an opt-in system, rather than simply allowing individuals to opt-out. As Anne T. Gilliland notes, the enactment of GDPR matters to companies and libraries worldwide: "Because of their various ties to Europe and EU citizens, such as exchange programs, study abroad opportunities, visiting scholars, and satellite campuses in other countries, universities and research libraries are among the organizations that now must come to terms with the GDPR's requirements."[13]

As a result of GDPR, other countries, such as Canada, Argentina, Brazil, Israel, and Japan, have enacted similar privacy legislation that is at least compatible with the EU's approach.[14] Canada, for example, updated

the Personal Information Protection and Electronic Documents Act (PIPEDA), which has governed data privacy since 2000.[15] While the updates included amendments regarding data security breaches, Canada is considering more sweeping changes. The Standing Committee on Access to Information, Privacy and Ethics published the report, "Addressing Digital Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process" recommending additional amendments to PIPEDA, in line with GDPR.[16] In 2018, the Canadian government held national digital and data consultations, including roundtables in Ottawa, Vancouver, Calgary, Regina, Winnipeg, Waterloo, Toronto, Ottawa, Montreal, Quebec, Fredericton, Charlottetown, Halifax, St. John's, and Whitehorse, in addition to a roundtable in Silicon Valley in the United States.[17] However, legislation has not yet been introduced in Canada to create a GDPR-like law.

> "In 2018, the EU's General Data Protection Regulation (GDPR) went into effect and has resulted in a domino effect in terms of compliance by private businesses as well as new legislation in other countries."

Because companies, even those based outside the EU, may interact with those in the EU and must comply with GDPR, it is easier to take a uniform approach to data collection. As the months following GDPR's effective date demonstrate, one natural result has been an effort in several countries to update their own privacy laws to ensure a compatible standard. The growing number of countries adopting GDPR-like laws places the United States as an outlier because of the lack of comprehensive, uniform privacy laws. Without comprehensive federal legislation, the United States risks losing credibility and leadership on the issue of privacy.

On the Horizon in the United States

The interest in protecting consumer privacy in the United States likely stems from a number of events. First, as a practical matter, the notice-and-consent regime that has formed the basis for many services

and platforms is proving inadequate in a growing digital economy. It is less realistic or rational to place the burden on consumers to read through every, generally lengthy, terms-of-service statement and then opt-out of data collection services, when so many services that are central to today's communications and interactions grow. Second, the rising number of data breaches at companies holding millions—sometimes billions—of users' information, including Equifax, Yahoo, and Uber, among others, has given rise to concerns about the security or vulnerability of personal information and the amount of data collected and retained by services. Third, a growing concern that personal data is used for political purposes emerged after news broke that Cambridge Analytica mined the data of millions of Facebook accounts, without the users' consent, using the data for political purposes, such as to support the campaigns of President Trump and Senator Ted Cruz. Fourth, as noted above, the European Union's data protection law resulted in a number of companies, including those in the United States, being forced to comply with these rules. Policy makers, advocates, and consumers have objected to what has often resulted in a two-tiered system, where United States–based companies provide greater privacy protections to those in Europe than to those domestically. With a growing number of states interested in a GDPR-like system, the concern of a patchwork system with potentially conflicting laws grows. Strong, comprehensive legislation at the federal level could address these concerns.

> With a growing number of states interested in a GDPR-like system, the concern of a patchwork system with potentially conflicting laws grows. Strong, comprehensive legislation at the federal level could address these concerns.

United States Congress

Comprehensive federal privacy legislation is likely to be a priority for the United States Congress in 2019. Congress has held multiple hearings on the topic of consumer privacy and policy makers released discussion drafts and bills on this issue in the last Congress. The

attention to federal privacy legislation will undoubtedly continue as this issue has the support of Congressional leadership. The Senate Commerce Committee chair Roger Wicker (R-MS) has expressed support for enacting a federal privacy law in 2019; ranking member Maria Cantwell (D-WA) has similarly been engaged on privacy issues and has supported legislation to protect privacy rights of consumers. House Committee on Energy and Commerce chair Frank Pallone (D-NJ) noted support for comprehensive federal legislation; ranking member Greg Walden (R-OR) pointed out last year that state privacy legislation "has heightened calls for federal privacy legislation" and encouraged the technology industry to come to a unified position.[18]

A wide range of stakeholders, including businesses, consumers, academics, and advocates support efforts to enact federal privacy legislation, though the right approach to federal privacy laws and nuances to a federal framework is contentious. Nevertheless, given the urgency in addressing data privacy and security with strong bipartisan support, privacy legislation could be enacted this year. Indeed, as Senator John Thune (R-SD) noted as chair of the Senate Commerce Committee in the last Congress, legislative efforts abroad and in the states "have all combined to put the issue of consumer data privacy squarely on Congress's doorstep. The question is no longer **whether** we need a federal law to protect consumers' privacy. The question is **what** shape it should take."[19] (emphasis added)

"A wide range of stakeholders, including businesses, consumers, academics, and advocates support efforts to enact federal privacy legislation."

Beginning in late 2018, numerous bills and discussion drafts—from members of Congress, businesses, and advocates—were introduced. Below are some of the most prominent drafts, which could potentially provide the starting point for discussions. In general, these proposals would shift the burden away from the current model, which requires consumers to proactively manage their data to a system that would

place the burden on companies to ensure meaningful consent and protections. Virtually all discussions assume FTC enforcement and oversight.

Senator Ron Wyden (D-OR), who has long been an advocate for privacy, released a discussion draft of the Consumer Data Protection Act, which would "create radical transparency into how corporations use and share their data...".[20] Wyden's bill would give consumers the power to control the sharing of their data and allow companies to charge consumers who want to use their services but opt-out of data collection and processing. Wyden's bill envisions harsh penalties, including steep fines and potential prison terms for violations of the act. However, the bill's scope is limited to larger companies or ones engaged in particularly high volumes of data collection.

Senator Brian Schatz (D-HI) released his own draft bill, the Data Care Act,[21] also in fall 2018, which garnered co-sponsorship of 14 other Democratic Senators.[22] The key elements of the Data Care Act would impose duties of care, loyalty, and confidentiality on companies; for example, the bill would prohibit companies from using data that would result in reasonably foreseeable physical or financial harm to the individual.

More recently, on April 12, 2019, Senator Edward Markey (D-MA), a member of the Senate Commerce, Science, and Transportation Committee, introduced a comprehensive privacy bill. In addition to providing the rights to notice and control, the Privacy Bill of Rights Act would: explicitly prohibit companies from using personal information in discriminatory ways (such as targeted advertisements related to housing), limit the information that companies can collect to only what is needed to provide the requested services, and allow for suits by state attorneys general and a private right of action by individuals. The bill also prohibits both "take-it-or-leave-it" policies and financial incentives (such as a discount for services) in exchange for opt-in approval of the use and sharing of personal information.

While these bills put forth by Wyden, Schatz, and Markey received much attention, other drafts have also been circulated, such as the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act introduced by Senators Markey and Richard Blumenthal (D-CT), and the Social Media Privacy Protection and Consumer Rights Act by Senators Amy Klobuchar (D-MN) and John Neely Kennedy (R-LA).

In addition to bills by members of Congress, a number of companies, associations, consumer advocacy groups, academics, and other stakeholders have discussed various principles and elements that should be included in federal privacy legislation.

Significantly, in late 2018, Intel Corporation released draft privacy legislation and allowed for interactive, public comment.[23] In welcoming public engagement and comment, Intel made clear that its draft is a work in progress and it has already gone through at least one revision. In the initial draft, Intel intentionally did not adopt CCPA's data minimization model and would provide for federal preemption of state laws. It provides for significant criminal fines and potential for jail time, as well as civil penalties. Intel's initial draft would apply to companies that collect data of more than 5,000 people and appears to introduce a privacy-by-design element, in prohibiting companies from collecting data beyond the companies' purpose. In this way, companies would not be able to collect vast swaths of data with an unknown purpose, the practice many technology companies have engaged in to date.

The Center for Democracy and Technology (CDT) released a draft federal privacy bill in December 2018.[24] CDT's bill grants consumers several rights, including the right to access and correction, data portability, and deletion. Some of these rights apply only to certain types of data; the right to correction, for example, would apply only when used for eligibility determinations for credit, insurance, housing, employment, educational opportunity, or health information. CDT's bill also explicitly addresses biometric information—including location data—limiting when it could be collected. The bill also provides a list

of unfair data uses and specifically addresses issues related to targeting based on data collection, that could result in civil rights violations and discrimination. It does not, however, provide users with the right to object, instead relying on users to agree to terms of service or walk away. It also provides significant exceptions to the provisions, which raises concerns that these exceptions could be exploited by companies. Like other bills, CDT's envisions that the FTC would have a role in enforcing the legislation and provides federal preemption of state laws.

Most recently, in February 2019, the US Chamber of Commerce released model privacy legislation, entitled the Federal Consumer Privacy Act.[25] The Chamber of Commerce model legislation focuses heavily on notice and transparency and would allow consumers to opt-out of data sharing and permit a right to deletion, subject to some exceptions. Like other models, the Chamber of Commerce's draft would empower the FTC to enforce these rules. It would also preempt state laws on data privacy, instead favoring a uniform piece of legislation across the United States. Most companies, such as those working with the Chamber of Commerce, have advocated for a uniform standard, rather than requiring compliance with a patchwork of state regulations.

> "More than 200 individuals, organizations, and companies, including ARL, submitted comments to the NTIA, largely focusing on the importance of strong transparency and meaningful consent, making opt-in the default position."

In addition to efforts in Congress to create a federal legislative solution, the National Telecommunications and Information Administration (NTIA), on behalf of the Department of Commerce, has also noted interest in a federal privacy framework. In September 2018, NTIA published a request for comment in a number of areas related to federal privacy regulations: "NTIA is seeking public comments on a proposed approach to this task that lays out a set of user-centric privacy outcomes that underpin the protections that should be produced by

any Federal actions on consumer-privacy policy, and a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections."[26] The request for comment sought feedback in a number of areas including transparency of collection, use and sharing of personal information; user control over personal information, reasonable minimization of collection, use, storage and sharing; security safeguards to protect data; user access and ability to correct personal data; risk management; and accountability.[27] The NTIA's notice clearly envisions federal preemption of state privacy laws and FTC enforcement.

More than 200 individuals, organizations, and companies, including ARL, submitted comments to the NTIA,[28] largely focusing on the importance of strong transparency and meaningful consent, making opt-in the default position. ARL's comments also note that a right to deletion implicates freedom of expression and the importance of preserving the cultural record and therefore such a right must be carefully considered and likely requires a highly nuanced approach.[29] The NTIA noted in its request for comment that other agencies are working on similar efforts, including the National Institute of Standards and Technology's voluntary privacy framework and the International Trade Administration's effort to increase global regulatory harmony on privacy.

Congress will continue working on a federal data privacy framework in the United States in 2019. Both Houses of Congress have explored various aspects of data privacy. The House of Representatives Committee on Energy and Commerce held a hearing on "Protecting Consumer Privacy in the Era of Big Data" on February 26, 2019.[30] One day later, the Senate Committee on Commerce, Science, and Transportation convened a hearing on "Policy Principles for a Federal Data Privacy Framework in the United States."[31] In announcing the hearing, Chairman Wicker noted, "It is this committee's responsibility and obligation to develop a federal privacy standard to protect consumers without stifling innovation, investment or competition. As we continue to examine this critically important issue, I hope this

first hearing will offer valuable insights that will help set the stage for meaningful bipartisan legislation,"[32] indicating that additional hearings should follow, with the intention of a bipartisan effort to enact privacy legislation. Several additional hearings in Congress and the FTC have been held.

As the numerous hearings and bills, as well as the NTIA's request for comment illustrate, legislating in this area will require thoughtful debate and, ultimately, a nuanced approach in many areas. While all of the discussion drafts and comments have been criticized by various stakeholders, elements of any of the drafts could find their way into federal privacy legislation.

The Upshot

Any legislation in the United States would likely require libraries to evaluate their contracts with vendors and services, their own privacy policies, and data collection policies to which they agree. For example, while libraries may rely on outside services as platforms, libraries must fully understand what these services collect and why, as well as how this is communicated to patrons. Additionally, while research libraries are committed to improving user experience, they must consider what collection of data is appropriate and how to improve informed consent. Should some form of a right to deletion/right to be forgotten be included, libraries must determine how to balance these rules with the First Amendment or how to use any exceptions to such a right to preserve cultural heritage. Many of the issues a research library might face are ethical ones that depend on best practices, but could potentially fall under federal laws depending on how broadly or comprehensively a legislative solution is framed.

"Any legislation in the United States would likely require libraries to evaluate their contracts with vendors and services, their own privacy policies, and data collection policies to which they agree."

Similarly, although Canada is much further along than the United States in comprehensive, national legislation protecting data privacy, it is clear that Canada is considering additional amendments to its laws. Canadian research libraries should watch for updates from the Canadian government's 2018 roundtables and potential amendments to its laws to determine whether changes to their privacy policies are legally necessary.

Endnotes

1. Samuel D. Warren and Louis D. Brandeis published an article, "The Right to Privacy," in the *Harvard Law Review* 4, no. 5 (December 15, 1890): 193–220, in which they urged for a "right to privacy" or "right to be let alone." This article proved to be highly influential and a right to privacy was subsequently adopted in court decisions.

2. "Library Bill of Rights," American Library Association, last amended January 29, 2019, http://www.ala.org/advocacy/intfreedom/librarybill.

3. "Privacy: An Interpretation of the Library Bill of Rights," American Library Association, amended July 1, 2014, http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

4. See, for example, Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000), 36–38, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

5. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

6. The White House, *Consumer Data Privacy.*

7. Section 5 of the Federal Trade Commission Act of 1914.

8. Privacy Rights for California Minors in the Digital World, California Business and Professions Code, Section 22580, http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=22580&lawCode=BPC; Online and Personal Privacy Protection, Delaware Commerce and Trade Code, Chapter 12C, http://delcode.delaware.gov/title6/c012c/index.shtml.

9. See Privacy of User Records: Violation, Classification, Definition, Arizona Revised Statutes, Section 41-151.22, https://www.azleg.gov/ars/41/00151-22.htm; Reader Privacy Act, California Civil Code, Section 1798.90, http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.90.&lawCode=CIV; Online and Personal Privacy Protection, Delaware Commerce and Trade Code, Chapter 12C, http://delcode.delaware.gov/title6/c012c/index.shtml; Disclosure of Library Records: Definitions, Missouri Revised Statutes, Section 182.815, https://law.justia.com/codes/missouri/2011/titlexi/chapter182/section182815/.

10. California Consumer Privacy Act of 2018, Assembly Bill No. 375, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

11. Rhode Island, for example, is considering a bill on data protection. See "Rhode Island Lawmaker Proposes Data Transparency And Protection Act," *Daily Dashboard*, International Association of Privacy Professionals, January 25, 2018, https://iapp.org/news/a/ri-state-representative-proposes-data-transparency-and-protection-act/.

12. Washington Privacy Act, Senate Bill 5376, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376.pdf.

13. Anne T. Gilliland, *Issue Brief: The General Data Protection Regulation: What Does It Mean for Libraries Worldwide?* (Washington, DC: Association of Research Libraries, May 2018), https://www.arl.org/storage/documents/IssueBrief_GDPR_May2018.pdf.

14. See, for example, King & Spalding, "Canada to Update Data Law to GDPR Standard as a Minimum," *JD Supra*, June 29, 2018, https://

www.jdsupra.com/legalnews/canada-to-update-data-law-to-gdpr-16052/; Angelica Mari, "Brazil Moves Forward with Online Data Protection Efforts," *ZDNet*, July 5, 2018, https://www.zdnet.com/article/brazil-moves-forward-with-online-data-protection-efforts/.

15. Prior to these updates, the Standing Committee on Access to Information, Privacy and Ethics held hearings on PIPEDA. The Canadian Association of Research Libraries (CARL) testified, addressing concerns regarding the right to be forgotten: "CARL Appearance before the ETHI Committee Hearing on the Personal Information Protection and Electronic Documents Act (PIPEDA)," June 1, 2017, http://www.carl-abrc.ca/wp-content/uploads/2017/11/CARLOpening-Statement-to-ETHI-on-RTBF-version-31-05-17-bilingual.pdf.

16. Standing Committee on Access to Information, Privacy and Ethics, *Addressing Digital Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process: Report of the Standing Committee* (Ottawa, Ontario: House of Commons, June 2018), https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf.

17. "National Digital and Data Consultations," Government of Canada, accessed April 2, 2019, https://www.ic.gc.ca/eic/site/084.nsf/eng/home.

18. John D. McKinnon and Marc Vartabedian, "Tech Firms, Embattled over Privacy, Warm to Federal Regulation," *Wall Street Journal*, August 6, 2018, https://www.wsj.com/articles/tech-firms-embattled-over-privacy-warm-to-federal-regulation-1533547800.

19. John Thune's opening remarks presented in "Thune Leads Hearing Examining Safeguards for Consumer Data Privacy," press release, September 26, 2018, https://www.thune.senate.gov/public/index.cfm/2018/9/thune-leads-hearing-examining-safeguards-for-consumer-data-privacy.

20. Ron Wyden United States Senator for Oregon, "Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy," press release, November 1, 2018, https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.

21. McKinnon and Vartabedian, "Tech Firms, Embattled over Privacy."

22. Co-sponsors include Senators Maggie Hassan (D-NH), Michael Bennet (D-CO), Tammy Duckworth (D-IL), Amy Klobuchar (D-MN), Patty Murray (D-WA), Cory Booker (D-NJ), Catherine Cortez Masto (D-NV), Martin Heinrich (D-NM), Ed Markey (D-MA), Sherrod Brown (D-OH), Tammy Baldwin (D-WI), Doug Jones (D-AL), Joe Manchin (D-WV), and Dick Durbin (D-IL).

23. "Legislation," Intel Corporation, accessed April 2, 2019, https://usprivacybill.intel.com/legislation/.

24. *CDT's Federal Baseline Privacy Legislation Discussion Draft*, Center for Democracy and Technology, December 13, 2018, https://cdt.org/insight/cdts-federal-baseline-privacy-legislation-discussion-draft/.

25. Federal Consumer Privacy Act (draft), US Chamber of Commerce, accessed April 2, 2019, https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

26. National Telecommunications and Information Administration, Request for Comments on Developing the Administration's Approach to Consumer Privacy, September 25, 2018, https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

27. National Telecommunications and Information Administration, "NTIA Seeks Comment on New Approach to Consumer Data Privacy," press release, September 25, 2018, https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy.

28. NTIA released the comments responding to its request for comments. See "Comments on Developing the Administration's Approach to Consumer Privacy," NTIA website, November 13, 2018, https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy.

29. Association of Research Libraries comment on "Developing the Administration's Approach to Consumer Privacy," Docket No. 180821780-8780-01, accessed April 2, 2019, https://www.ntia.doc.gov/files/ntia/publications/ntia_privacy_220ct2018.pdf.

30. "Hearing on 'Protecting Consumer Privacy in the Era of Big Data,'" US House of Representatives Committee on Energy and Commerce, February 26, 2019, https://energycommerce.house.gov/committee-activity/hearings/hearing-on-protecting-consumer-privacy-in-the-era-of-big-data.

31. "Policy Principles for a Federal Data Privacy Framework in the United States," hearing announcement and webcast, US Senate Committee on Commerce, Science, and Transportation, February 27, 2019, https://www.commerce.senate.gov/public/index.cfm/hearings?ID=CBA2CD07-4CC7-4474-8B6E-513FED77073D.

32. "Policy Principles for a Federal Data Privacy Framework," US Senate Committee on Commerce, Science, and Transportation.

To cite this article: Krista L. Cox. "Legal Landscape of Consumer/User Data Privacy and Current Policy Discussions." *Research Library Issues*, no. 297 (2019): 15–37. https://doi.org/10.29242/rli.297.3.