Federal Privacy Legislation Should Be Context-Sensitive

By **Kirk Nahra and Lydia Lichlyter** (February 27, 2020)

Kirk Nahra

Lydia Lichlyter

Legislators in both houses of Congress are currently engaged in earnest and detailed discussions about the potential for passing comprehensive federal privacy legislation, which has never before existed in the United States.

Many of these proposals rely on the same framework that has become common in sectoral laws and international privacy regimes: provide consumers with notice of the business's data collection, use and sharing practices and give them choice about whether to consent to those practices.

This approach relies on a privacy notice made available by the relevant entity that describes how personal data is used and a consumer's ability to review, understand and agree to these activities. The specific way these elements — notice and choice — are provided varies widely from one context to another, but the basic structure is fairly consistent.

The problem is that, as many academics and advocates have pointed out, notice and choice is a fundamentally ineffective framework for giving people control over their personal information. It unnecessarily burdens consumers, proliferating paperwork that is largely useless to individuals. And it fails to stop conduct that actually harms consumers. We believe there is a better option.

Instead, Congress should adopt a context-sensitive approach, modeled off of laws like the Health Insurance Portability and Accountability Act.[1] Such an approach would have four major elements. First, there would be a framework to identify data collection, use and sharing practices that are clearly in line with the reasonable expectations of the consumer, in the context of their relationship with the business. These practices would be permitted without the need for specific consumer permission.[2]

Second, there would be a set of permitted purposes for which businesses could use personal information with an informal form of user consent. This could be obtained, by example, by giving the consumer a clear opportunity to object, where their consent could be inferred if they do not do so.[3] This category would include common practices that may be less obvious to consumers.

Third, there would be a set of practices that could only be engaged in if the business obtains formal consent, according to procedures established by law or regulation.[4]

And fourth, there would be a set of things that businesses may do in the interest of public policy purposes, such as the protection of public health and safety.[5]

Privacy policies would still be provided under this approach, as a source of information if consumers are interested, but they would no longer be depended upon as the primary protection for consumers. Congress also may wish to consider a fifth category — whether there are practices that are so inherently problematic that they should be banned in their entirety.

Relative to the existing notice-and-choice framework, this context-sensitive approach would more effectively provide consumers with choice and control over the use of their personal information.

Notice and choice is an ineffective framework for protecting consumers.

Whether they realize it or not, all American adults are probably familiar with the failings of notice and choice. Every one of us has been asked to click hundreds or thousands of checkboxes in our lives stating that we have read privacy policies — which, of course, we have not. Or we have used services that do not provide even a check box, based on a legally permitted assumption that a consumer who continues to use a service has read and agreed to the privacy policy.[6]

Even if these policies are clearly drafted, very few have the time to read them and consider carefully whether they approve of the company's data practices. And if they do, depending on the legal regime, they may have no choice but to accept the terms in full if they wish to use the product or service.

As privacy legislation has been crafted in different sectors and around the world, this process has not changed significantly. Often, the proposed solution to this problem is to add even more settings, disclosures and consent checkboxes.[7] Users may now have more opportunities to opt in or out of different practices, but the burden is still placed on them to do so. As the president of the Center for Democracy and Technology testified before the Senate in October 2018, this approach is "neither scalable [n]or practical for the individual."[8]

Particularly when notices can be dozens of pages of impenetrable legalese — often driven by a legal obligation to fully describe all potential or actual data sharing and collection activities — expecting users to read and understand the vast number of policies that apply to their online lives is unreasonable. Most companies take their obligations on consumer privacy seriously — whether by law or because of appropriate consumer best practices — and will engage in appropriate data-sharing practices consistent with consumer expectations.

Unscrupulous companies, however, have too much leeway to structure their notices and settings in the most inaccessible way possible, and manipulative design and choice architecture can be used to encourage users to do what the company wants or permit the company to engage in broad data sharing practices without a consumer's clear understanding.[9]

There is also frequently no restriction on what companies can do under most laws that rely on notice and choice, as long as it is disclosed. The most innocuous practice — say, sending a consumer's email address to a service provider to distribute a newsletter the consumer requested — often requires the same type of disclosure as much more insidious forms of data processing — such as selling profiles of consumer behavior for targeted marketing based on sensitive data.

This lack of proportionality makes it even more difficult for consumers to understand what practices they should be concerned about, which companies are acting responsibly, and where they should spend their limited attention resources to protect their privacy and control their data.

Many academics agree that notice and choice has failed. Professor Woodrow Hartzog, for

example, has called it "irreparably broken," because the control it promises users is "an illusion" and the "dizzying array of switches, delete buttons, and privacy settings" is "overwhelming."[10] As professor Fred Cate has written, "As theoretically appealing as this [notice and choice]approach may be, it has proven unsuccessful in practice."[11]

A context-sensitive approach would better protect consumers.

Instead, in crafting comprehensive federal privacy legislation, Congress should take an approach inspired by laws like HIPAA that takes into account the context in which a consumer interacts with a business. Certain practices that align with a consumer's reasonable expectations should be permitted without burdensome notice and consent requirements that waste the consumer's time and attention.

This approach mirrors a consumer's expectations and permits normal activity to proceed efficiently. Other practices that are reasonable, but less expected, should be permitted with an informal form of consent — perhaps a simple switch or yes/no pop-up.[12]

Where companies engage in practices that consumers are likely to find truly surprising or potentially alarming, or even just unusual — practices that are outside the norms of what a reasonable consumer would expect — there should be a well-defined consent procedure that ensures these out-of-the-norm practices are truly consensual.[13] Consumers should have a clear choice here, but one that is specific and focused and where the burden is on the entity, rather than the consumer.

For these situations, typically, if the consumer does not agree, the business cannot go forward. This approach provides consumer choice — but in a manageable and appropriate way, limited to these unusual data-sharing practices. In the HIPAA framework, for example, there often are situations where this unusual data-sharing practice is desired by the consumer for the consumer's own interest, such as when a consumer needs to provide medical records to a future employer or a life insurer.

There may even be limited cases in which Congress or regulators should consider banning some types of practices outright, if they pose risks to others beyond the consumer, or if they pose a high risk of harm that is impossible for the consumer to foresee.[14]

The core of this approach should be dependence on consumers' reasonable expectations in a given context. While notice and choice theoretically respects the possibility that every consumer wishes to precisely tailor the use of their data to a set of unique preferences, the truth is that most people have fairly similar expectations for how their data should be used.[15] Similarly, most businesses operating in similar circumstances generally have a set of baseline practices that are common for the industry.

In the health care industry that is regulated by HIPAA, these are "treatment, payment and health care operations" uses and disclosures. In financial services, the Gramm-Leach-Bliley Act focuses on certain disclosures to nonaffiliated third parties as atypical disclosures. In retail, while there are no clear legal requirements, consumers would expect to obtain (or return) their purchases in a seamless manner and receive information about new products and services offered by companies that they have shopped with in the past.

While there is no harm in providing the opportunity for consumers to make idiosyncratic choices if they wish to, demanding that they do so to exercise any form of control is unrealistic and unnecessary.

Perhaps most importantly, a context-sensitive approach would shift the burden of protecting privacy from consumers to businesses. As professor Hartzog testified before the Senate in February 2019, "People will always know less than companies regarding the wisdom of a decision" about data collection practices.[16]

Instead of deluging individuals with notices and settings and expecting them to take the time to read and analyze them, businesses would have to take on the responsibility of determining which choices are truly important for the consumer to make or where the law would require an additional form of consumer permission.

They would then be required to present those choices clearly, so that the consumer can focus their attention on making the decisions that really matter to them.[17] Moreover, for these out-of-the-norm disclosures, these businesses would typically be permitted neither to force an agreement by the consumer to these additional disclosures, nor to proceed in the absence of specific consumer permission.

Though this approach would shift responsibility to businesses, it would also be likely to lighten their overall compliance burden. By limiting requirements to obtain consent to only the circumstances that vary from consumers' reasonable expectations, businesses are left free to focus their resources on the most important issues and can proceed with these normal operations more efficiently to the general benefit of both consumers and companies.

And by tying the amount of work a business must do to comply with the law to the degree to which their practice departs from normal expected behavior, Congress would essentially be taxing data practices that pose a higher risk of being unexpected or undesirable to the average consumer. Over time, businesses would be likely to shift away from these practices whenever possible.

The context-sensitive approach would also be flexible over time. Because it is tied to consumers' reasonable expectations, the law would be able to adapt as those expectations change. If, as suggested, businesses shift away from certain practices to avoid compliance requirements, consumers would adjust to expect more privacy-protective behavior, and a virtuous cycle would be created.

For reasons like these, the Consumer Bill of Rights released by the Administration of then President Barack Obama in 2012 included respect for context as one of its core rights, stating that "Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."

The Consumer Bill of Rights report notes that companies should be able to infer consent for data practices that are "common to many contexts and integral to companies' operations," such as product and service fulfillment, fraud prevention and standard first-party marketing practices. But for practices that are less consistent with the original context of collection, heightened transparency and choice are required.[18]

Conclusion

Some may be reluctant to consider the approach we are proposing because it seems new. The notice-and-choice approach has so thoroughly pervaded the conversation around privacy legislation that it now appears to be the inevitable bedrock of any comprehensive federal law. This is despite the fact that many — industry, academia and privacy advocates included — recognize its many significant shortcomings.

A context-sensitive approach provides an alternative and one with a foundation in existing law and commonsense ideas for how people should be able to expect companies to behave.

The most extensive current regulatory scheme utilizing this approach involves the privacy and security rules under HIPAA. Under HIPAA, covered entities are permitted by law to engage in typical uses and disclosures with presumed consent. There also are defined public policy purposes where disclosure is permitted with other safeguards.

In general, beyond these categories, a consumer authorization is needed before a use or disclosure is permitted outside these common categories. This history has worked well for both consumers and the health care industry and has permitted appropriate data sharing for a range of typical purposes that benefit both consumers and the industry, as well as the public at large.

By placing the burden on companies to disclose which choices matter most and focusing consumers' attention on them, we can give people real control over the way their data is used online. This context-specific approach will benefit both consumers and industry and provide a more effective and efficient overall approach to managing consumers' choices in connection with their privacy.

Kirk Nahra is a partner and co-chair of the cybersecurity and privacy practice, and Lydia Lichlyter is an associate at WilmerHale.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See Off. for Civ. Rts., U.S. Dep't of Health & Hum. Servs., Summary of the HIPAA Privacy Rule (May 2003), available at https://www.hhs.gov/sites/default/files/privacysummary.pdf?language=es.

[2] This category is analogous to HIPAA's permitted uses and disclosures for treatment, payment, and health care operations or uses and disclosures that are incidental to an otherwise permitted use or disclosure. See id.

[3] The HIPAA analogue for this category would be uses and disclosures that are permitted with an opportunity to agree or object, which includes uses and disclosures such as notification to an individual's family of their general health condition. See id.

[4] This category is analogous to HIPAA's rules for authorized uses and disclosures, which provide specific requirements for how formal authorization must be obtained. See id.

[5] Under the HIPAA Privacy Rule, the analogous category includes uses and disclosures for twelve "national priority purposes," including law enforcement purposes, public health activities, and research. See id.

[6] A 2016 study found that 74% of participants skipped even opening a privacy policy before joining a fictitious social networking site. Those who opened the policy spent an average of less than 90 seconds reading the policy before agreeing to it at a 97% rate.

Jonathan A. Obar & Anne Oeldorf-Hirsch, The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services, TPRC 44: The 44th Research Conf. on Comm'n, Info. & Internet Pol'y (June 1, 2018), available at https://ssrn.com/abstract=2757465 or http://dx.doi.org/10.2139/ssrn.2757465.

[7] One report found that when websites rewrote their privacy policies to accommodate GDPR requirements, they increased in length over 25% on average. Rob Sobers, The Average Reading Level of a Privacy Policy, Varonis (July 11, 2018), available at https://www.varonis.com/blog/gdpr-privacy-policy/. And a Wall Street Journal reporter who printed out the privacy policies of 35 commonly used apps found that they spanned a football field. Joanna Stern, Those Privacy Policies Flooding Your Inbox? Print Them Out and They Span a Football Field, Wall Street Journal (May 17, 2018), available at https://www.wsj.com/articles/privacy-policies-flooding-your-inbox-how-to-cut-through-the-gibberish-1526565342.

[8] Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act: Hearing Before the S. Comm. on Commerce, Sci., & Transp., 115th Cong. 5 (2018) (statement of Nuala O'Connor, President & CEO, Center for Democracy & Technology), available at https://cdt.org/wp-content/uploads/2018/10/2018-10-09-FINAL-Nuala-OConnor-Written-Testimony-Senate-Commerce.pdf.

[9] As Professor Hartzog has written, "Entities inescapably engineer their technologies to produce particular results. People's choices are constrained by the design of the tools they use. Companies decide the kind of boxes people get to check, the buttons that they press, switches they activate and deactivate, and other settings they get to fiddle with." Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Commerce, Sci., & Transp., 116th Cong. 3–4 (2019) (statement of Woodrow Hartzog, Professor of Law & Computer Science, Northeastern University), available at https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53. Much has been written about these techniques, sometimes called "dark patterns" or "persuasive design," though opinions differ about the prevalence of the practices and their risks. For example, witnesses at a recent Senate hearing titled "Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms" debated the issue. Witness statements and a video of the hearing are available at https://www.commerce.senate.gov/2019/6/optimizing-for-engagement-understanding-the-use-of-persuasive-technology-on-internet-platforms.

[10] Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Commerce, Sci., & Transp., 116th Cong. 3–4 (2019) (statement of Woodrow Hartzog, Professor of Law & Computer Science, Northeastern University), available at https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53.

[11] Fred H. Cate, The Failure of Fair Information Practice Principles, in Consumer Protection in the Age of the 'Information Economy' (2006), available at https://www.huntonak.com/images/content/3/7/v3/3754/Failure-of-Fair-Information-Practice-Principles.pdf.

[12] In the HIPAA context, "Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object." In emergency situations or when the individual is otherwise unavailable, covered entities may exercise their professional judgment to make uses or

disclosures that are in the best interests of the individual. Off. for Civ. Rts., U.S. Dep't of Health & Hum. Servs., Summary of the HIPAA Privacy Rule (May 2003), available at https://www.hhs.gov/sites/default/files/privacysummary.pdf?language=es.

[13] Under HIPAA, authorizations must: (1) be in writing, (2) use plain language, and (3) contain specific information, including the information to be disclosed or used and the person(s) disclosing and receiving the information. Id.

[14] For example, some advocates have suggested prohibiting secondary uses of biometric or health information without an affirmative request from the consumer. See, e.g., Protecting Consumer Privacy in the Era of Big Data: Hearing Before the Subcomm. on Consumer Protection & Commerce of the H. Comm. on Energy & Commerce, 116th Cong. 9 (2019) (statement of Nuala O'Connor, President & CEO, Center for Democracy & Technology), available at https://cdt.org/wp-content/uploads/2019/02/Testimony-Nuala-OConnor-02262019.pdf.

[15] Researchers from the University of California, Berkeley conducted a series of surveys between 2009 and 2013 about Americans' privacy knowledge and preferences. Their results show widespread consensus among consumers on many topics. For example, over 85% of survey respondents said that advertisers should not be able to keep information about consumers' internet activity for more than a few months, and over 80% said that they would not allow a social networking app to collect their contact list in order to suggest more friends. Chris Jay Hoofnagle & Jennifer M. Urban, Alan Westin's Privacy Homo Economicus 49 Wake Forest L. Rev. 261 (May 19, 2014), available at https://ssrn.com/abstract=2434800.

[16] Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Commerce, Sci., & Transp., 116th Cong. 3–4 (2019) (statement of Woodrow Hartzog, Professor of Law & Computer Science, Northeastern University), available at https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53.

[17] As Professor Hartzog put it: "Even if a company achieves the platonic ideal of how to give data subjects' notice and choice, it wouldn't solve people's limited bandwidth dilemma. People only have twenty four hours in a day and every service they use wants them to make choices about how they can handle their data. Meaningful individual control over one data flow between a person and a data collector won't change the fact that the data ecosystem is vast." Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Commerce, Sci., & Transp., 116th Cong. 3–4 (2019) (statement of Woodrow Hartzog, Professor of Law & Computer Science, Northeastern University), available at https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53. Instead, support is growing for a perspective that respects the limited resources individuals have to deploy, relying on company's to act as trustworthy stewards of data. See, e.g., Cameron Kerry, Why protecting privacy is a losing game today—and how to change the game, Brookings (July 12, 2018), available at https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/; Jack M. Balkin & Jonathan Zittrain, A Grand Bargain to Make Tech Companies Trustworthy, The Atlantic (Oct. 3, 2016), available at https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.

[18] The Consumer Bill of Rights lists several factors that should be taken into account when evaluating context, including the age and sophistication of the relevant consumers,

the terms governing the company-to-consumer relationship, and research and feedback regarding consumers' attitudes and understandings. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, White House (Feb. 2012), available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf; see also Cameron Kerry, Why protecting privacy is a losing game today—and how to change the game, Brookings (July 12, 2018), available at https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.