Research

Preventing Privacy Policy From Becoming a Series of Unfortunate Events

JENNIFER HUDDLESTON, MERCATUS CENTER | JANUARY 14, 2019

It seems that every day new headlines are calling our attention to the "growing problem" of data privacy. From the Equifax breach to a series of Facebook scandals to new laws in Europe and California, there seems to be a growing chorus advocating that "something must be done." Unfortunately, these calls often neglect the full spillover effects of increasing compliance burdens on innovation and free speech. Further, they also often neglect the existing tools available both to consumers and the government regarding data privacy.

THE PRESENT POSITION OF PUBLIC POLICY ON PRIVACY

To begin, let's examine the current privacy laws in the United States. Contrary to what critics may claim, the United States is not completely a "Wild West" when it comes to data privacy. The lack of comprehensive privacy policy rather has recognized that choices regarding privacy and transactions involving data primarily exist as an individual preference between consumers and companies. Nevertheless, there are still specific rules when necessary to stop harm or protect those individuals or data that are particularly vulnerable and/or significantly more likely to result in real, cognizable harm if breached.

For example, Congress recognized that children under the age of 13 needed special protections regarding data collection. The Children's Online Privacy Protection Act (COPPA) requires verifiable parental consent for the collection of personal information collected online and is enforced and interpreted by the Federal Trade Commission (FTC). Other laws have carved out additional data privacy protections for particularly sensitive information such as medical, financial, and credit data held by certain entities, as well as information that is more likely to reveal information an individual would likely consider not to be public such as data gathered while driving and personal video rental history. Rather than taking a restrictive but comprehensive approach to data privacy that might have prevented many of the most popular uses of the Internet, such as tailored song recommendations or social media, these laws have served to carve out particular types of data that would most likely result in real, cognizable harm to individuals if a breach were to occur.

But actions not covered by these narrow categories are not entirely without recourse either. If the privacy harm in question is harming consumer welfare, the FTC has broad authority to go after the companies using its unfair and deceptive practices authority. As Neil Chilson points out, in this role the FTC has brought privacy actions against companies regarding data privacy "where consumers are substantially injured, could not reasonably avoid the injury, and this injury isn't outweighed by benefits to consumers or competition." This approach focused on consumer welfare has tended to preserve a broad array of options to reflect individual preferences regarding data privacy and allow individual consumers and companies to select standards that fit these preferences. Many states have given similar broad authority to their consumer protection authorities that would allow them to go after bad actors if there was harm to consumer welfare. The consumer welfare standard used by the FTC limits the ability of this broad power to be abused for just a sense of "creepiness" and rather limits

its pursuit of such incidents ideally to only those where harm has occurred or is most likely to occur.

It is important to remember that most if not all of these interactions are voluntary and in exchange for services and not mandated by government authorities.

PRIVACY PARADOX PROBLEMS

When news of a data breach or a perceived abuse breaks, there is an uptick in popular concern about the state of online privacy. This interest, however, appears to be immediate reactions to specific events and not an actual desire for change or willingness to make tradeoffs. For example, a 2018 NetChoice survey found less than 1 percent of younger adults and teenagers chose to leave a platform over changes in a privacy policy.

Much of this type of data has been labeled the "privacy paradox." The privacy paradox is the distinction between expressed and revealed preferences for data privacy online. Individuals may state that they value data privacy, but their actions and further preferences reveal that they are willing tolerate little that would decrease efficiency or increase costs to achieve it. Many complain or are unwilling to deal with privacy measures that would increase friction of usage or change the user experience and even fewer are willing to pay for actual measures. It is important to note that in many cases additional products and solutions are available to those whose expressed preferences for data privacy do align with such willingness to take action.

Furthermore, many consumers willingly participate in the data-driven marketplace and appreciate its benefits. For example, a 2017 Accenture study found the majority of consumers would be willing to share financial data in exchange for service benefits such as investment advice, insurance, and banking. When surveyed, few adults say that concerns about privacy are significant enough to make them willing to pay for access to online platforms rather than exchange data for a free, ad-supported version. Policymakers should carefully consider that in choosing to prioritize privacy over consumer preferences they may be making choices that consumers aren't actually looking for. As Chris Koopman points out, "In truth, it seems that consumers have a pretty good idea that their personal information is being collected but seem to value it less than what they're getting in exchange from the platforms."

THE RISK OF A PRIVACY PATCHWORK PROBLEM

Perhaps the more pressing privacy public policy problem is not the lack of privacy regulation, but the potential pitfalls of the growing patchwork of policies aimed at privacy issues. The United States has traditionally embraced a permissionless approach to the Internet, including privacy policies, and has allowed individual online communities and individual users to develop their own preferences via a system of notice and choice. Any legislative intervention into the existing paradigm should be as narrowly tailored as possible to preserve allowing consumers a wide array of options to select personal preferences, and only intervening when consumer welfare is being harmed. Data do not obey borders, and increasingly state and global regulations risk changing the innovation-friendly framework that allowed the Internet to succeed and creating a quagmire of conflicting regulations.

Notably, the European Union (EU) has taken a very different approach to data privacy, first in establishing a "right to be forgotten" and more recently through the General Data Privacy Regulation (GDPR). These requirements have come at substantial costs to the firms operating in both the financial expenses of compliance as well as hiring additional employees to focus on the issue and dedicating time to insuring compliance rather

than innovation. In some cases, faced with such burdens, small- and mid-size firms have chosen to exit the market rather than undertake the compliance burden and costs. As a result, the largest market players that could afford to comply, such as Google, have increased their market share and consumers have fewer choices.

GDPR and privacy laws do not just impact those traditional data collectors such as social media and search engines, but also many online entities like personal blogs or small businesses that do not have large compliance teams at their disposal. Several U.S. newspapers are still not available in the EU due to not being GDPR compliant, and other websites and services from video games to a church website collecting prayer requests have geofenced EU users or stopped offering certain features. Even large tech companies may be rethinking potentially beneficial additions in light of these new standards. For example, GDPR likely prevented Facebook from launching a suicide prevention alert in Europe.

Given the amount of time and money many American tech companies invested into GDPR compliance, there is concern that it — rather than the more permissionless American approach — could emerge as a global default. GDPR style laws value privacy over innovation and put privacy choices in the hands of regulators rather than individual consumers. A shift to such a default could prevent the development of better options including those focused on data privacy due to the increased cost of compliance and the regulatory burdens. As a result, small players may never be able to grow big enough to offer alternatives to current giants.

Not only internationally are new laws such as the GDPR creating a complicated and potentially innovation-limiting framework for data privacy, domestically state laws are creating problems for data privacy policy. Notably the California Consumer Privacy Act (CCPA) was passed in August 2018 and would create a wide variety of requirements that would increase compliance costs and dissuade new innovators online in a very short period of time. While it may be an option to segment off and provide different defaults and services to comply with GDPR, the burden of doing so on a state-by-state level would not be sustainable. Additionally, the California law's definition of covered entities could be interpreted broadly enough to cover any data if the company has even a single California resident access the website — whether from California or elsewhere. Others may see this as a way to follow suit creating a problem in which it is difficult if not impossible to launch a universal product available in all communities. New York City recently stated in a comment filing that it intended to similarly pass its own data privacy law regardless of if a federal regulation occurred. Much like the GDPR, these state and local laws may further consolidate business in the large players who can afford to devote resources to complying with them and — because of the relatively lower number of users at which such requirements kick in — discourage current small players from trying to grow large enough to challenge existing giants. As a result, such state laws would deter innovation and competition.

With the rise of the Internet as a tool for commerce and the borderless nature of data flows, it seems the dormant commerce clause would likely render state or local privacy laws such as the CCPA unconstitutional. Similar issues are arising in the courts regarding state-level net neutrality laws. Yet because of the length of time it would take businesses to engage in necessary steps for compliance and the funds that would need to be allocated to such, some degree of damage could be done even if such laws are later struck down by the courts. If such laws were not struck down, it could create a scenario of conflicting requirements or one where the most restrictive approaches or largest states win for fear of noncompliance or losing the most lucrative markets.

While the California law is the most expansive, it is not the first state to carve out specific privacy regulations for its citizens, although prior attempts have been much more limited in both the data and entities covered. Perhaps the other most relevant example of such deviations from the general notice-and-choice process is Illinois' Biometric Information Privacy Act (BIPA). But even this relatively specific policy had consequences that prevented Illinois residents from using certain services. For example, many Illinoisans were surprised to

find they could not use Google's Arts & Culture app due to the law. Social media companies such as Facebook that use facial recognition to help users identify themselves or friends in photos have found themselves subject to class action lawsuits and hefty fines under the law. Offline it could prevent the use of biometric security because of consent requirements such as the recent lawsuit involving Six Flags amusement park and its collection of annual passholders' fingerprints. If left unchecked, such litigation could redefine harm so broadly as to undermine the sharing of information at the heart of many online communities or limit the technologies that companies are able to offer consumers. Texas and Washington passed similar but less restrictive laws regarding biometric data, and as a result have not experienced the same degree of loss of opportunity.

State data breach laws provide an example of what a 50-state patchwork could look like and even this relatively narrow privacy issue shows the potential compliance quagmire that could emerge if state policies pollute the current privacy frameworks. These laws vary in the amount of time in which users whose data have been breached must be notified and even what data are covered. As a result, nationwide companies may find the most restrictive laws to be de facto national regulations rather than risk noncompliance and must determine how best to deal with seemingly contradictory requirements.

It quickly becomes apparent that state governments are not the proper actor for data privacy policymaking, and if any reforms are necessary they must occur at the federal level. Recent actions suggest that when they are not preempted from doing so, states may try to pursue regulatory actions that could eliminate certain consumer choices and, potentially, fundamentally change the Internet.

PREEMPTION AND POTENTIAL PRIVACY PUBLIC POLICY SOLUTIONS

Perhaps the most obvious solution to this perplexing problem is federal preemption that retains the current framework of notice-and-choice for most privacy issues, continues case-by-case examination of consumer harms, and resolves current and potential data-privacy public policy patchworks caused by state and local interventions.

The United States has recognized since the mid-1990s that the Internet is an important tool for innovation, communication, and commerce. Now over 20 years after this initial framework, this overall permissionless framework that allowed the Internet to evolve faces significant challenges from a variety of policies on the state and federal level.

Policymakers should carefully consider the tradeoffs associated with any data privacy policies and if such actions will eliminate benefits and increase the burdens to providing consumers better and more innovative choices. One way to prevent or eliminate the growing patchwork problem would be to expressly preempt state laws regarding data. This move would prevent laws such as the CCPA from becoming de facto national regulations for millions and likely undo existing patchwork problems related to conflicting data breach laws or policies such as the BIPA.

Preemption of state policies that would disrupt the current system would not mean that a federal policy such as a U.S. GDPR is necessary. Such preemption could provide the opportunity to reiterate the U.S. emphasis on a permissionless approach to Internet policy, including notice-and-choice regarding data privacy and delegation of authority on a case-by-case basis regarding consumer harm to the FTC. Any policy should maintain the current neutrality in the U.S. system, which allows new entrants to emerge that may offer consumers more and better

options and allows individuals to make choices regarding data privacy that reflect their own preferences.

Perhaps the best policy solution is not to change policy regarding data privacy at all, but rather for the government to increase efforts regarding consumer education around privacy choices and to continue to have the FTC examine the specifics of instances where consumer welfare is truly harmed. The government's role as educator in such debates regarding possible data privacy solutions is often neglected. By informing consumers of steps to take if they seek to improve data privacy and what options are available to them in the case of specific harms, the government can empower individual citizens and their families to make the choices that are right for them and would also encourage new products to enter the market and provide consumers the options they desire.

THE TRUE PRIVACY PROBLEM

The presumption that data privacy is broken is based on individual incidents such as breaches rather than real harm to consumers or competition. This presumption could lead to tradeoffs that impact innovation and remove choices that consumers enjoy and value above their privacy. Many of the proposed solutions do not align either with consumer actions, expressed choices, or the reality of innovation. Perhaps the real privacy problem is knowing how not to start down a slippery slope that could lead to diminishing or dismantling many of the technologies that have revolutionized our lives, and that could prevent future innovation that brings even more benefits.