Insight

Opt-In Mandates Shouldn't Be Included In Privacy Laws

WILL RINEHART | NOVEMBER 8, 2018

Executive Summary

- Many in the United States are pushing for a comprehensive privacy regulation that requires websites to only gather data after individuals' opt-in, and they contend that an opt-in requirement will better educate people about what companies are doing with their data.
- An opt-in regime does not give users more information than an opt-out system.
- Research indicates that most people are aware that their data is being collected and processed, and take steps now to protect their privacy.
- An opt-in requirement would not fix the problem it is trying to solve while simultaneously imposing burdens on both users and companies.

Making the Case for Opt-in

With Congress likely to consider a comprehensive federal privacy law next year, some are pushing for an opt-in requirement for all forms of data collection, which would require that users affirmatively agree to data collection. Such a requirement could be modeled on Europe's General Data Protection Regulation (GDPR), which requires opt-in. California Representative Ro Khanna made opt-in a central feature of his Internet Bill of Rights, while Internet rights group Access Now made opt-in an explicit part of their guidelines for lawmakers for the adoption of a new U.S. privacy law.

Eric Null, senior policy counsel at the Open Technology Institute, has articulated one of the more prominent cases for an opt-in regime, saying, "The benefit of opt-in is making sure consumer data isn't used in ways they didn't know about, understand, or agree to. Opt-out assumes they know, when in reality we all know they don't. How do you solve that without opt-in?" The argument from knowledge—or lack thereof—is a primary part of the argument for an opt-in privacy regime. The choice, whatever it may be, should be supported by knowledge about the promises and pitfalls of the service. But because consumers don't have that knowledge, they cannot make a prudent decision. Until consumers know what they are agreeing to, the default must be no collection, many argue.

But does this argument for an opt-in privacy regime stand up to scrutiny? A brief survey of some basic data points indicates it might be overblown: Many people don't read the terms of service contracts yet agree to them anyway, and one study suggested that only about one in a thousand people click on a site's terms of service. Other research confirms this conclusion. An opt-in regime will not solve the knowledge problem. On the whole, people are aware of their privacy options, and they tend to weigh trade-offs when valuing their privacy.

The Privacy Paradox

Privacy preferences, like all preferences, tend to be formed at the moment when it is elicited, such as when a

surveyor asks a question or when a user has to choose among privacy settings. Biases affect all decisions, but they perhaps affect instantaneous decisions the most. A number of cognitive biases affect decisions regarding privacy, including the fact that the benefit of information collection is immediate, in that people get access to a service, while the costs of disclosing that information are delayed. This phenomenon, sometimes called "benefit immediacy," is a time-related bias. (It is worth noting that opt-in mandates don't solve this intertemporal problem.)

Due to the conflict between privacy attitudes and actual outcomes, some scholars worry about a privacy paradox. As one review of the literature described it, "while many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behavior, this rarely translates into actual protective behavior."

While the privacy paradox often animates calls for regulation, there isn't really a paradox when you dive deeper into privacy-related decision-making. Just because a person wants privacy doesn't preclude them from also wanting the services and convenience granted from data processing. In an ideal world, users would be able to consume both the service and privacy. But in the real world, users choose, in some instances privacy, and in other instances to share. Every introductory economics course uses the indifference curve to illustrate how consumption of one good is slowly traded off for the consumption of another. This fundamental insight doesn't stop because the good (e.g. privacy) is intangible.

A privacy paradox could reasonably exist if consumers don't think a trade-off is occurring. Pew found, for example, that "there are a variety of circumstances under which many Americans would share personal information or permit surveillance in return for getting something of perceived value." As those researchers found, many will willingly trade shopping histories for a discount card, but will not do the same when car insurance companies offer cheaper rates if a tracking device is installed. Acxiom and trade group Data & Marketing Association found in their own survey earlier this year that 58 percent of consumers will share personal data under the right circumstances.

In the most recent survey of its kind, economist Caleb Fuller found that nine out of ten people who use Google are aware of its business practice. Moreover, as users consume the service more, they are more aware of the information collection. For those that use Google about once a day, 78 percent are aware of information collection, but this number jumps up for those who use the site "dozens of times a day or more" to 93 percent. Fuller also found that, "of the 71% of all respondents who said they would prefer not to be tracked, a full 74% are unwilling to pay anything to retain their privacy."

An unwillingness to pay is a common finding and for good reason. Everyone would love to get something for nothing. Trade association NetChoice worked with Zogby Analytics to find that only 16 percent of people are willing to pay for online platform service. Strahilevitz and Kugler found that 65 percent of email users, even though they knew their email service scans emails to serve ads, wouldn't pay for alternative. As a result, instead of paying with money, people trade their data for access.

Other research indicates that users do take steps to manage their online privacy. A comScore study on cookies found that about three in every ten Internet users delete their cookies every month, a small but powerful sign of interest in privacy. At least a quarter of all U.S. Internet users employ ad blocking technology. Those aged 18 to 45 are far more engaged in protecting their privacy: Forty five percent of this group enable two-step verification, nearly one-third have created another email account dedicated for services, and 17 percent have signed up with security companies to protect their information. Teens use coded language on platforms such as Facebook to maintain privacy from their parents who also might be on the site. While some might claim that

people don't know about privacy protection or their setting, three out of four Facebook users are aware of their privacy settings, and even more know how to change their privacy settings, nearly eight in ten.

In other words, requiring an opt-in regime would not help the vast majority of online users, and would only make their online experience more burdensome with minimal added value.

Valuing Privacy

Privacy researchers Alessandro Acquisti, Curtis Taylor, and Liad Wagman recently brought attention to the issue of knowledge in privacy decision-making by noting that the "individuals' awareness of privacy challenges, solutions, and trade-offs cast doubts over the ability of market outcomes to accurately capture and reveal, by themselves, individuals' true privacy valuations." Yet, the totality of evidence suggest that privacy is central to a complex set of decisions. Because opt-in regimes won't solve the problem of knowledge, they aren't likely to lead to an optimal level of privacy protection when balanced against the costs.

Research indicates that the value of privacy varies depending on the context. For example, one group of researchers found that the vast majority of customers will buy from a more privacy-invasive firm that was selling DVDs if they offered only a slightly lower price. In repeated interactions, this firm got both a larger market share and higher revenue than competitors without data collection. Similarly, professors Christian Happ, André Melzer, and Georges Steffgen found that a over a third of people will readily give up their personal passwords for a bar of chocolate. As one seminal study noted, "most subjects happily accepted to sell their personal information even for just 25 cents." Using differentiated smartphone apps, economists were able to estimate that consumers were willing to pay a one-time fee of $2.28 to conceal their browser history, $4.05 to conceal their list of contacts, $1.19 to conceal their location, $1.75 to conceal their phone's identification number, and $3.58 to conceal the contents of their text messages. The average consumer was also willing to pay $2.12 to eliminate advertising. Sometimes, consumers are willing to a pay a higher price to purchase goods from more privacy-protective merchants. Context matters.

The individuals in these studies were doing cost-benefit analyses, yet the results often indicate that people don't value their privacy as much as advocates of an opt-in regime contend. Further, showing users the long-term risks involved in sharing information oftentimes doesn't matter that much for their end choices. Law professors Adam Chilton and Omri Ben-Shahar tested these assumptions within an experiment by simplifying privacy policies and laying out the potential long-term costs of information collection. They found that these kinds of information changes did little to shift the users' comprehension of the disclosure, the willingness to share personal information, or expectations about their rights.

Similar research only confirms Chilton and Ben-Shahar's result. As Adjerid, Acquisti, Brandimarte, and Loewenstein explained after testing privacy disclosure, "the ability of even improved transparency solutions or additional control tools to better align consumer attitudes towards privacy with actual behavior and reduce regret from oversharing is ultimately questionable." Ironically, related research indicates that giving users an increased feeling of control over the publication of their data often results in increased and riskier disclosures.

What's more, it doesn't seem as though strong regulations have done anything to make people feel as though they are getting a better deal with Internet companies. Calls for opt-in regulations assume that changing the defaults will help to align privacy preferences with outcomes. But as Daniel Castro and Alan McQuinn point out, "European trust in the Internet remained flat from 2009 through 2017, despite the European Union strengthening its ePrivacy regulations in 2009 (implementation of which occurred over the subsequent few

years) and significantly changing its privacy rules, such as the court decision that established the right to be forgotten in 2014."

If the move towards an opt-in data regime rests on an information deficit, policy makers might want to consider less onerous options that achieve the same outcomes.

The True Effect of Opt-In

Opt-out and opt-in mandates don't differ in their choices or in the kind of information that consumers can access. Rather, what is truly at stake in the opt-in versus opt-out debate then is where the default should be. Data collection is a default yes in the case of a privacy opt-out, while the default becomes no for an opt-in regime. As Obama's chief regulatory czar wrote, "setting default options, and other similar seemingly trivial menu-changing strategies, can have huge effect on outcomes."

The likely outcome of an opt-in regime is not more knowledge, however. Many people already understand that their data is being gathered, and often people don't take the time to dig deep into companies' privacy policies anyway. The most likely outcomes of an opt-in privacy regime affect innovation and jobs, as such a policy is burdensome, especially for smaller companies. It is on the basis of these negative outcomes that an opt-in mandate should not be pursued.

For a larger consideration of these and other issues around a comprehensive privacy law, read this regulatory comment.