Comments on Developing the Administration's Approach to Consumer Privacy
NTIA Docket No. 180821780-8780-01
By Will Rinehart[1]

Executive Summary

Among the most controversial parts of the European General Data Protection Regulation (GDPR) is the shift of the entire Internet ecosystem toward an opt-in system where users have to say yes to every instance of data collection. Yet, the requirement that all data collectors abide by an opt-in mandate has been gaining support among policymakers and advocates here in the United States. As talks over a comprehensive federal privacy law have become more serious, policymakers should be aware of several facts:

- Privacy is a multifaceted term, and yet, consumers tend to be more concerned about fraudulent activity such as identity theft rather than control over data;
- Advocates frame opt-in mandates as fundamental for consumer choice, yet changing a privacy regime to opt-in doesn't change the choices available to a consumer;
- Evidence suggests that users of online platforms are aware of their privacy settings and take steps to secure their data; and finally
- Privacy laws impose large costs on innovation and the online information ecosystem.

Introduction, or When to Regulate

At the very core, opt-in mandates are meant to solve an informational market failure, proponents contend.[2] That failure occurs because consumers' choices are biased, as they aren't aware of the risks involved in disclosing information. In this sense, an informational market failure is similar to a typical market failure in that there exists, in principle, a trade that could occur between market participants that would make at least one participant better off. Yet, that trade does not occur.

The informational market failure is the first part of a three-part test that should be used for all new regulations:[3]

1. First, prove the existence of market abuse or failure by documenting actual consumer harm;
2. Then, explain how current law or rules are inadequate, and show that no alternatives exist including market correctives, deregulatory efforts, or public/private partnerships to solve the market failure; and finally
3. Demonstrate how the benefits of regulation will outweigh the potential countervailing benefits, implementation costs, and other associated regulatory burdens.

Is there a market failure in privacy? The case is thin. As will be detailed below, some make the strong claim that bias in privacy decision-making necessitates strong regulatory correctives. But the reality is far more complex. As two economists noted, "identifying an inconsistency in someone's behavioral preferences (meaning those that actually determine choice) is not the same

[1] Will Rinehart is Director of Technology and Innovation Policy at the American Action Forum.
[2] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," https://www.ftc.gov/system/files/documents/public_comments/2017/10/00006-141501.pdf
[3] https://www.americanactionforum.org/comments-for-record/policies-will-foster-growth-artificial-intelligence/

as identifying someone's true preferences."[4]

Additionally, opt-in mandates and privacy laws place a heavy burden on innovation, and this impact is not just felt in the tech sector, but across all industries and firms that use data processing—which is increasingly all actors.

The follow comments are broken into two sections, which correspond to the first and the third parts of the test. The first part explores the problem of an information market failure that opt-in mandates are meant to correct. As should be apparent by the end, opt-in mandates do little to correct this problem, if it is indeed a problem that should be corrected. The second section reviews the literature on the cost of privacy regulations and concludes that they are onerous. Just because privacy is an important value doesn't mean privacy regulations should get a pass. Policy makers should be keenly aware of the pitfalls of privacy regulations.

Part One – The Informational Market Failure

Defining Privacy and Privacy Risk

As countless surveys attest, Internet users are concerned about and value their privacy.[5,6,7] But privacy is a multifaceted term that can carry a variety of definitions.[8] Famously, Warren and Brandeis described privacy in the 1890s as the right to be left alone. Alan Westin thought privacy could be understood as the control over and safeguard of personal information, while more recent interpretations of the idea see it as an aspect of dignity, autonomy, and human freedom. For the purposes of privacy regulation, it is important to broadly distinguish data security concerns from concerns about control of data collection and use because the term privacy is often used for both.

In one sense, privacy often just means data security, the protection of digital data from the unwanted actions of unauthorized users, such as a cyberattack, a data breach, or fraud. On the other hand, privacy as term has also come to reference laws and regulations that limiting legitimate actors from using, disclosing, or collecting information. The distinction becomes especially clear when privacy as an issue of data control is explicitly broken out from data fraud, like the Census has done. Since 1994, the Census working in conjunction with the National Telecommunications and Information Administration have surveyed Internet users. When users were asked about their top concerns in the most recent polling, identity theft and credit card or banking fraud top the list, at 57

[4] Mario J. Rizzo and Douglas Glen Whitman, "The Knowledge Problem of New Paternalism," https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2461&context=lawreview
[5] Mary Madden and Lee Rainie, "Americans' Views About Data Collection and Security," http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/#few-feel-they-have-a-lot-of-control-over-how-much-information-is-collected-about-them-in-daily-life
[6] Julie Beck, "People Are Changing the Way They Use Social Media," https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/
[7] Rimma Kats, "Many Facebook Users Are Sharing Less Content," https://www.emarketer.com/content/many-facebook-users-are-sharing-less-content-because-of-privacy-concerns
[8] Adam Moore, "Defining Privacy," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1980849

percent and 45 percent.[9] Yet, concerns about data collection and loss of control over personal data rank far lower, at 22 percent and 21 percent. American Action Forum survey data confirms this finding. When the concept of privacy is broken into constituent parts, fraudulent activity is leaps and bounds more of a concern than control of data, by nearly three times.[10]

The distinction between these two versions of privacy comes in expectations. Most expect that health, banking, and financial information won't be leaked because it could affect the availability or price of employment, credit, or insurance, or it could contribute to risks of identity theft or fraud. As Joseph Farrell, formerly of the Federal Trade Commission pointed out, harms from "the unexpected revelation of previously private information" is a driving concern for consumers. Any successful policy discussion over privacy will need to carefully disaggregate these instrumental concerns from more intangible concerns like data control.[11]

Just as privacy is a polysemous term, so is value. Value can be understood in one context as quality of a good that makes it desirable, which is usually reflected in the price of an item. But value can also be about the propriety of an object or activity, "whether the object or activity is compatible with or supports the moral standards of the relevant individual or group."[12] Thus, when discussing value of privacy, the issue of economic cost is naturally associated with larger societal values about privacy. Viewed from this lens, whether or not privacy laws actually grant consumers a higher level of protection isn't important. What is important is that pass privacy laws are passed to signaling that the United States collectively values privacy. However, just because privacy regulations are salient, that doesn't mean they are prudent.

Making the Case for Opt-in

Privacy law in the United States is governed by a sectoral approach, where specific kinds of sensitive data, like health or financial data, are protected by narrow laws. The result is variation. The Children's Online Privacy Protection Act or COPPA requires that the parent or guardian of a child under the age of 13 must affirmatively opt-in before companies can collect or use their personal information, for example. Other federal laws have chosen to give consumers an opt-out choice. The Gramm-Leach-Bliley Act (GLBA), which includes financial privacy protections, mandates such an opt-out.

With a comprehensive federal privacy law now being discussed, policymakers and advocates have been jostling for an opt-in requirement for all forms of data collection. California Representative Ro Khanna made opt-in a central feature of his Internet Bill of Rights, but admitted that "if you have to click on something 50 times, it kind of defeats the purpose."[13] (Weak opt in, where one click suffices all requirements, contrasts with strong opt in, where consent must be granted for all types of data collection and process.) Internet rights group Access Now made an opt-in an explicit part of their

---

[9] Rafi Goldberg, "Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds," https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds

[10] American Action Forum, "New AAF Net Neutrality Survey," https://www.americanactionforum.org/survey/new-aaf-net-neutrality-survey/

[11] Joseph Farrell, "Can Privacy Be Just Another Good?" http://www.jthtl.org/content/articles/V10I2/JTHTLv10i2_Farrell.PDF

[12] Keith Tester, "Media Culture, and Morality," https://books.google.com/books/about/Media_Culture_and_Morality.html?id=sa9A9h3ZicAC

[13] Kara Swisher, "Introducing the Internet Bill of Rights," https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html

guidelines for lawmakers for the adoption of a new U.S.-wide privacy law.[14] Senior policy counsel at the Open Technology Institute Eric Null has also made the case 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?"[15]

Null evinces a common and important support for the change to an opt-in 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. So, until consumers know what they are agreeing to, the default must be no collection, many argue.

Many people don't read the terms of service contracts and yet agree to them anyway.[16,17] One study suggested that only about one in a thousand people click on a site's terms of service.[18] So there is a tenuous connection *at best* between affirmative consent in agreeing to online services and absolute knowledge of what that consent fully entails. At the heart of the opt-in regime is an affirmative choice that doesn't seem to mean all that much.

Opt-out and opt-in mandates don't differ in their choices or in the kind of information that consumers can access, as will be discussed later. Rather, data collection is a default yes in the case of a privacy opt-out, while the default becomes no for an opt-in regime. What is truly at stake in the opt-in versus opt-out debate then is where the default should be. As Obama's chief regulatory czar wrote of this topic, "setting default options, and other similar seemingly trivial menu-changing strategies, can have huge effect on outcomes." Those outcomes, which affect innovation and jobs, are the reason why an opt-in mandate shouldn't be pursued.

Privacy Preferences

Privacy preferences, like all preferences, tend to be formed at the moment when it is elicited, like when a surveyor asks a question or when a user has to choose among privacy settings. Internet users generally do engage in cost benefit analyses regarding their privacy, but preferences are highly contingent on how survey questions and experimental designs are framed.

The former head of OIRA during the Obama Administration, Cass Sunstein, recently ran an experiment that helps to illustrate some of these framing issues in privacy.[19] He asked two groups of people similar questions about the value of Facebook but differed slightly how they were asked.

---

[14] Access Now, "Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers," https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf

[15] Eric Null, https://twitter.com/ericnull/status/999360346396741632

[16] Shankar Vedantam, "Do You Read Terms Of Service Contracts? Not Many Do, Research Shows," https://www.npr.org/2016/08/23/491024846/do-you-read-terms-of-service-contracts-not-many-do-research-shows

[17] Caroline Cakebread, "You're not alone, no one reads terms of service agreements," https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11

[18] Yannis Bakos, Florencia Marotta-Wurgler, and David R. Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443256

[19] Cass Sunstein, "How Much Is It Worth to Use Facebook? It Depends," https://www.bloomberg.com/opinion/articles/2018-05-03/facebook-users-want-to-be-paid-a-lot-to-quit

The first group was posited, “Suppose that you had to pay for the use of Facebook. How much would you be willing to pay, at most, per month?” The second group, however, was asked: “Suppose that you are being offered money to stop using Facebook. How much would you have to be paid per month, at a minimum, to make it worth your while to stop using Facebook?” For the first question, the median answer was just $1 per month, while the second question clocked in at a media of $59 per month. Depending on where the question begins, the value of Facebook can vary widely. That people tend to ascribe more value to things merely because they own them is known as the endowment effect and it is a tendency that has been catalogued throughout decision making.

Decisions regarding privacy are affected by a number of cognitive biases. 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.[20] (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.[21] 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.”[22]

Indeed, the value of privacy does vary depending on the context. For example, one group of researchers found that the clear majority of customers will buy from a more privacy-invasive firm that was selling DVDs if they offered only a slightly lower price.[23] 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.[24] As one seminal study noted, “most subjects happily accepted to sell their personal information even for just 25 cents.”[25] 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.[26] The average consumer was also willing

---

[20] David W. Wilson and Joseph S. Valacich, “Unpacking the privacy paradox: Irrational decision-making within the privacy calculus,” https://arizona.pure.elsevier.com/en/publications/unpacking-the-privacy-paradox-irrational-decision-making-within-t

[21] David Ryan Polgar, “RIP, Privacy? The Strange Paradox of How We Act Online,” https://bigthink.com/david-ryan-polgar/the-privacy-paradox-an-interview-with-manoush-zomorodi

[22] Susanne Barth and Menno D.T.de Jong, “The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review,” https://www.sciencedirect.com/science/article/pii/S0736585317302022

[23] Sören Preibusch, Dorothea Kübler, and Alastair R. Beresford, “Price versus privacy: an experiment into the competitive advantage of collecting less personal information,” https://link.springer.com/article/10.1007/s10660-013-9130-3

[24] Christian Happ, André Melzer, and Georges Steffgen, “Trick with treat – Reciprocity increases the willingness to communicate personal data,” https://www.sciencedirect.com/science/article/pii/S0747563216301935

[25] Jens Grossklags and Alessandro Acquisti, “When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information,” https://www.econinfosec.org/archive/weis2007/papers/66.pdf

[26] Scott J. Savage and Donald M. Waldman, “The Value of Online Privacy,” https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5735f456b654f9749a4afd62/1463153751356/The_value_of_online_privacy.pdf

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.[27] Context matters.

Yet, 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.[28] 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.[29] As Brandimarte, Acquisti, 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." In related research, giving users an increased feeling of control over the publication of their data often results in increased and riskier disclosures.[30]

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,

> The biannual Eurobarometer survey, which interviews 100 individuals from each EU country on a variety of topics, has been tracking European trust in the Internet since 2009. Interestingly, 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. Similarly, European trust in social networks, which the Eurobarometer started measuring in 2014, has also remained flat, albeit low.[31]

In other words, 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. However, social media researchers focused on platform interactions have found that users express increased trust and feelings of control over data when they are more educated about the sites. In one important study on the topic, social scientists discovered that after being told how the Facebook feed works, participants were mostly satisfied with the content on their feeds.[32] In a follow up two to six

---

[27] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti, "Effect of Online Privacy Information on Purchasing Behavior," https://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf

[28] Adam Chilton and Omri Ben-Shahar, "Simplification of Privacy Disclosures: An Experimental Test," https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2443&context=law_and_economics

[29] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency," http://journals.sagepub.com/doi/abs/10.1177/1948550612455931

[30] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, "Misplaced Confidences Privacy and the Control Paradox," http://journals.sagepub.com/doi/abs/10.1177/1948550612455931

[31] Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use," http://www2.itif.org/2018-trust-privacy.pdf

[32] Motahhare Eslami and Karrie Karahalios, "Investigating Users' Understanding of Invisible Algorithms and Designing around It," http://social.cs.uiuc.edu/papers/Algorithms_Workshop_ICWSM.pdf

months later, "algorithmic awareness led to more active engagement with Facebook and bolstered overall feelings of control on the site."

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 Privacy Paradox isn't A Paradox

While the privacy paradox often animates calls for regulation, there isn't really a paradox when you dive deeper into 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 is intangible like privacy.

A privacy paradox only exists 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."[33] As those researchers found, many are ok with giving up shopping histories for a discount card but aren't ok 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.[34]

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.[35] 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.[36] 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.[37]

---

[33] Lee Rainie, "Privacy and Information Sharing," http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

[34] Greg Sterling, "Survey: 58% will share personal data under the right circumstances," https://marketingland.com/survey-58-will-share-personal-data-under-the-right-circumstances-242750

[35] Caleb S. Fuller, "Is the Market for Digital Privacy a Failure?" https://www.ftc.gov/system/files/documents/public_comments/2017/11/00019-141720.pdf

[36] NetChoice, "American Consumers Reject Backlash Against Tech," https://netchoice.org/american-consumers-reject-backlash-against-tech/

[37] Lior Strahilevitz and Matthew B. Kugler, "Is Privacy Policy Language Irrelevant to Consumers?" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449

Even still, users take steps to manage their online privacy experiences. A comScore study on cookies found that about 3 in every 10 Internet users delete their cookies every month, a small but powerful sign of interest in privacy.[38] At least a quarter of all US Internet users employ ad blocking technology.[39] Those aged 18 to 45 are far more engaged.[40] 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 places like 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.[41]

Part 2 – The Cost of Privacy Regulations

The Cost of Opt-In Versus Opt-Out

Overall, users do care about privacy, take actions to stop data misuse, and are aware of the tools that platforms provide to change their privacy settings. In spite of this positive baselines, could opt-in regulations help educate consumers about the decisions they make?

Rather than educating, opt-in mandates add three big hurdles for consumers as decision makers. First, consumers have substantially less information about decisions they make. Before any additional service can be provided, consumers will have to imagine all of the potential benefits, which will be difficult if not impossible for entrants. The biggest players, however, will be able to make a better case about the benefits. Second, consumers will think that that defaults are suggestions by the company. In other words, they will assume that it is a recommended action, even though they are mandated choices by the government. Lastly, these defaults will become the status quo. Any further change from this baseline will require significant effort by company and will be understood by the decision maker as a trade-off, as psychologists have found.[42]

Consider a system where you have only one option, you can either opt-in or not to data collection before you consume the good or service. If you say yes, then the negotiations have effectively ended. No further choices can be expressed unless you exit from the service completely. The contract is explicit and agreed to upfront. If, however, you are given the choice to opt-out of certain kinds of information processing in the future, then the relationship between you and the provider becomes one of an extended negotiation. Thus, privacy negations become a repeated game where a contract is implicitly agreed to but can be modified at some future point.

---

[38] Gian M. Fulgoni, "Cookie Deletion Rates and the Impact on Unique Visitor Counts," https://www.comscore.com/chi/Insights/Blog/Cookie-Deletion-Rates-and-the-Impact-on-Unique-Visitor-Counts?cs_edgescape_cc=US

[39] eMarketer, "eMarketer Scales Back Estimates of Ad Blocking in the US," https://www.emarketer.com/Article/eMarketer-Scales-Back-Estimates-of-Ad-Blocking-US/1015243?ecid=NL1001

[40] Remie Arena, "What Are Consumers Doing to Keep Their Personal Data, Well, Personal?" https://www.emarketer.com/content/what-are-consumers-doing-to-keep-their-personal-data-well-personal?ecid=NL1001

[41] Reuters Poll Data, "Social Media Usage Poll," http://fingfx.thomsonreuters.com/gfx/rngs/FACEBOOK-PRIVACY-POLL/010062SJ4QF/2018%20Reuters%20Tracking%20-%20Social%20Media%20Usage%205%203%202018.pdf

[42] William Samuelson and Richard Zeckhauser, "Status Quo Bias in Decision Making," https://sites.hks.harvard.edu/fs/rzeckhau/status%20quo%20bias.pdf

As Nicklas Lundblad and Betsy Masiello explain,

> This ought to evolve into an ongoing negotiation and game of repeated trust between the service provider and the user. But what we observe in account-based opt-in decisions is a one-time ex-ante limited choice which applies over the lifetime of a service contract. This actually risks the user's privacy over the long term because the deal requires no further negotiation on the part of the service provider.[43]

Moving data industries to opt-in choices modifies the user's relationship with the processor in a way that changes the relative positions within the negotiation process. Privacy is now, as Haggerty and Ericson explained in 2000, "less a line in the sand beyond which transgression is not permitted, as a shifting space of negotiation where privacy is traded for products, better services or special deals."[44]

The debate over opt-in or opt-out isn't centered around knowledge but around changing the default for consumer preferences. Opt-in defaults show markedly lower participation rates to opt-out defaults even though the good or service is exactly the same. The classic example is organ donation. Although there is widespread support for organ donation, only about 28 percent actually volunteer to be donors, despite the fact that around 85 percent claim to want to be donors. Some countries automatically enroll everyone for organ donation and then allow for opting out, which results in participation rates of 85 percent and higher.

Below is a compendium of studies testing these defaults. Even though consumer options and protections are the same, the default changes participation rates dramatically.

Subject Area	Opt-In Participation Rate	Opt-Out Participation Rate	Source
An on-line survey asking participants if they want to be contacted further about health surveys	48.2 percent	96.3 percent	[45]
Organ donation in Austria		99.98 percent	[46]
Organ donation in Belgium		98 percent	[46]

[43] Nicklas Lundblad and Betsy Masiello, "Opt-In Dystopias," https://www.scribd.com/document/30469167/Opt-in-Dystopias
[44] Kevin D. Haggerty and Richard V. Ericson, "The surveillant assemblage," http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.9622&rep=rep1&type=pdf
[45] Eric J. Johnson, Steven Bellman, Gerald L. Lohse, "Defaults, Framing and Privacy: Why Opting In-Opting Out," https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf
[46] Eric J. Johnson and Daniel Goldstein, "Do Defaults Save Lives," http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.2319&rep=rep1&type=pdf

Organ donation in Denmark	4.25 percent		[46]
Organ donation in France		99.9 percent	[46]
Organ donation in Germany	12 percent		[46]
Organ donation in Hungary		99.9 percent	[46]
Organ donation in Netherlands	27.5 percent		[46]
Organ donation in Poland		99.5 percent	[46]
Organ donation in Portugal		99.6 percent	[46]
Organ donation in Sweden		85.9 percent	[46]
Organ donation in the United Kingdom	17.2 percent		[46]

Changing defaults to require that every person affirmatively consents to a data collection service is likely to reduce the total number of people choosing yes, driving down the effectiveness of data processing. For those companies that rely on processing of data, which is increasingly every company, less data will tend to decrease their ability to service consumers. In "The Economics of Privacy," a wide-ranging review of economic research in this space, the authors highlight the trade-offs present in information disclosure,

> Individuals can benefit from protecting the security of their data to avoid the misuse of information they share with other entities. However, they also benefit from the sharing of information with peers and third parties that results in mutually satisfactory interactions.[47]

A reduction in the exchange of data isn't welfare enhancing. Opt-in privacy regimes have been tried before in the United States and were found to be costly. In a court case with US West, a telephone company that is now part of CenturyLink, it was revealed that obtaining permission to sell their services cost the company between $21 and $34 per consumer.[48] By their own internal calculations,

[47] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," https://www.ftc.gov/system/files/documents/public_comments/2017/10/00006-141501.pdf
[48] Julie Tuan, "U.S. West, Inc. v. FCC," https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1276&context=btlj

US West had to make 4.8 calls to each customer household before they reached an adult who could grant consent to share information. In one-third of households called, U.S. West never reached the customer. Altogether, customers received more calls from the opt-in regime than in an opt-out system even though many weren't able to enjoy the benefits of new services.

In other industries where opt-in regimes have been imposed, studies have found higher costs and slowed innovation. A 2000 Ernst & Young study of financial institutions found that these mandates cost the entire industry $56 billion.[49] For charities, the cost of compliance with an opt-in privacy law would have been nearly 21% of their total revenue.[50] In contrast, industry estimates from the American Banker suggest that around 5 percent of people choose to opt out of sharing financial information under GLBA requirements, a significantly smaller impact.[51]

The implementation of the General Data Protection Regulation (GDPR) in Europe at the end of May should serve as a stark warning to policymakers here in the United States as it is an opt-in privacy regime. Early research on the regulatory impact of the GDPR find that the biggest players have been able to weather the storm while smaller firms have been wiped out.[52] Smaller advertising firms have lost between 28 and 32 percent of their placements on web sites, while Google was able to increase their web presence by 1 percent. Economists focused on privacy predicted exactly this result years earlier.[53]

While the rule change with GDPR is still recent, earlier privacy regulation in Europe suggests that the impact on small sites could be massive. The implementation of restricted information sharing rules under e-Privacy decreased the efficacy of advertising by 65 percent relative to the rest of the world, cutting off the lifeblood of Internet startups.[54] Those hardest hit were general content sites like news outlets. The cost of privacy regulation is one of the reasons why Europe lags in startups.

The Cost of GDPR and Other Privacy Regimes

The early costs involved with GDPR compliance hints at the costs that United States industries would face if a broad privacy law were implemented. Importantly, the GDPR imposes three kinds of costs on firms. First, the regulation forces firms to retool data processes to realign with the new demands. This is generally one-time fixed cost that raises the cost of all information using entities. Second, the regime adds risk compliance costs, causing companies to staff up to ensure compliance. Finally, the law will change the investment dynamics for all those affected industries.

Currently, the retooling costs and the risk compliance costs are going hand in hand, so it is difficult to suss out the costs of each. Still, they are substantial. A McDermott-Ponemon survey on GDPR preparedness found that almost two-thirds of all companies say the regulation will "significantly

---

[49] Cynthia Glassman, "Customer Benefits from Current Information Sharing by Financial Services Companies"
[50] Fred Cate, "The Privacy Problem," https://web.archive.org/web/20150912045126/http://www.firstamendmentcenter.org/madison/wp-content/uploads/2011/03/FirstReport.privacyproblem.pdf
[51] W.A. Lee, "Opt-Out Notices Give No One a Thrill," https://www.americanbanker.com/news/opt-out-notices-give-no-one-a-thrill
[52] Björn Greif, "Study: Google is the biggest beneficiary of the GDPR" https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr
[53] James Campbell, Avi Goldfarb, and Catherine Tucker, "Privacy Regulation and Market Structure," https://onlinelibrary.wiley.com/doi/abs/10.1111/jems.12079
[54] Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259

change" their informational workflows.[55] For the just over 50 percent of companies expecting to be ready for the changes, the average budget for getting to compliance tops $13 million, by this estimate. Among all the new requirements, this survey found that companies were struggling with the data-breach notification the most. The inability to comply with the notification requirement was cited by 68 percent of companies as posing the greatest risk because of the size of levied fines.

The International Association of Privacy Professionals (IAPP) estimated the regulation will cost Fortune 500 companies around $7.8 billion to get up to speed with the law.[56] And these won't be onetime costs since, "Global 500 companies will be hiring on average five full-time privacy employees and filling five other roles with staff members handling compliance rules." A PwC survey on the rule change found that 88 percent of companies surveyed spent more than $1 million on GDPR preparations, and 40 percent more than $10 million.[57]

It might take some time to truly understand the impact of GDPR, but the law will surely change the dynamics of countless industries. For example, when the EU adopted the e-Privacy Directive in 2002, Goldfarb and Tucker found that advertising became far less effective.[58] The impact seems to have reverberated throughout the ecosystem as venture capital investment in online news, online advertising, and cloud computing dropped by between 58 to 75 percent.[59] Information restrictions shift consumer choices. In Chile, for example, credit bureaus were forced to stop reporting defaults in 2012, which was found to reduce the costs for most of the poorer defaulters, but raised the costs for non-defaulters.[60] Overall the law lead to a 3.5 percent decrease in lending and reduced aggregate welfare.

In the United States, because of differences in the roll out of electronic health records, two professors, Amalia Miller and Catherine Tucker, were able to test the impact of state privacy regulations on health outcomes.[61] Their analysis put a number on the cost privacy applies to EMR adoption. Privacy laws reduced adoption by some 24 percent. Why is this important? Better health data leads to better understanding of patients and typically better outcomes. Live are on the line, since a 10 percent increase in the adoption of such systems can reduce infant mortality by 16 deaths per 100,000 births.

Conclusion

---

[55] Ashley Winton, Larry Ponemon, and Mark E. Schreiber, "New study highlights lack of GDPR preparedness," https://iapp.org/news/a/new-study-highlights-lack-of-gdpr-preparedness/
[56] Daily Dashboard, "Global 500 companies to spend $7.8B on GDPR compliance," https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/
[57] PwC, "Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies," https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html
[58] Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1100.1246
[59] Anja Lambrecht, "E-Privacy Provisions and Venture Capital Investments in the EU," https://www.ceps.eu/sites/default/files/E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments%20in%20the%20EU.PDF
[60] Andres Liberman, Christopher Neilson, Luis Opazo, and Seth Zimmerman, "The Equilibrium Effects of Information Deletion: Evidence from Consumer Credit Markets," https://www.nber.org/papers/w25097
[61] Amalia R Miller and Catherine E. Tucker, "Can Healthcare IT Save Babies?" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1080262

In a zeal to ensure that consumers express their true preferences, opt-in mandates tax the exchange of data. Since privacy valuations are both contextual and highly personal, there is no guarantee that opt-in will yield the right balance between innovation and default protection. As detailed throughout this comment, opt-in regimes don't lead to an optimal level of privacy.

Further, privacy regulations impose real costs on the economy, on innovation, and on real lives. Those who are engaged in the policy discussion and who believe in strong privacy regulations shouldn't be dismissing that costs occur. Rather, they should be upfront with what they are willing to sacrifice for more data control.