Committee For Justice
Holding Judges and Politicians Accountable to the Constitution

The Committee for Justice
1629 K St. NW Suite 300
Washington, D.C. 20006

(202) 270-7748
committeeforjustice.org
@CmteForJustice

Comments filed with the Federal Trade Commission:

RE: Hearings on Competition and Consumer Protection in the 21st Century: Consumer Privacy Pre-Hearing Comments

DOCKET ID: FTC-2018-0098
SUBMITTED: DECEMBER 21, 2018

ASHLEY BAKER
DIRECTOR OF PUBLIC POLICY
THE COMMITTEE FOR JUSTICE

INTRODUCTION

Founded in 2002, the Committee for Justice (CFJ) is a nonprofit legal and policy organization that promotes and educates the public and policymakers about the rule of law and the benefits of constitutionally limited government. Consistent with this mission, CFJ advocates in Congress, the courts, and the news media about a variety of law and technology issues, encompassing administrative law and regulatory reform, online free speech, antitrust law, and data privacy.

Additionally, CFJ has a long history of leadership on the issue of federal judicial nominations and the confirmation process in the Senate. We have focused our attention on issues at the intersection of law and technology by highlighting how those issues will be impacted. For example, CFJ submitted a letter to the Senate Judiciary Committee explaining why the confirmation of Supreme Court Justice Brett Kavanaugh would be good for technological innovation and the economic growth it spurs.[1]

In recent years, CFJ has actively advocated for digital privacy protections in Congress, the federal courts, and the Supreme Court.[2] Today, our focus is on innovation, free speech, and economic growth. We believe that restrictive new requirements or penalties for data collection and use are not only unwarranted but would also threaten the online ecosystem that has transformed our daily lives in the last few decades.

Last month, CFJ responded to the National Telecommunications and Information Administration's (NTIA) Request for Comments on Developing the Administration's Approach to Consumer Privacy (available as an appendix).[3] Similarly, these comments emphasize the need to prioritize economic prosperity and

[1] Curt Levey and Ashley Baker, *Letter to the Senate Judiciary Committee on the Nomination of Brett Kavanaugh to the Supreme Court*. 4 Sept. 2018, https://www.committeeforjustice.org/single-post/Letter-for-the-Record-on-the-Nomination-of-Brett-Kavanaugh-to-the-Supreme-Court.

[2] See, *e.g.,* amicus briefs filed in *Carpenter v. United States.* 11 Aug. 2017, https://www.scribd.com/document/356288790/Amicus-Brief-Filed-in-Carpenter-v-United-States and *United States v. Kolsuz*. 20 March 2017, https://www.scribd.com/document/355249553/United-States-v-Kolsuz-Amucis-Brief; The Committee for Justice, *Letter to Congress in Support of the Clarifying Lawful Use of Overseas Data (CLOUD) Act.* 13 Feb. 2018, https://www.committeeforjustice.org/single-post/support-clarifying-lawful-use-data.

[3] Ashley Baker, *Comments submitted to the National Telecommunications and Information Administration in the Matter of: Request for Comments on Developing the Administration's Approach to Consumer Privacy*, Docket

preserve the United States' role as leader in technological innovation by learning from the disastrous results of privacy regulations abroad.[4]

RESPONSES TO QUESTIONS

What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these benefits?

The costs to consumers of a world with less information collection, sharing, aggregation, and use, is not only a world of greater information scarcity, but of less consumer welfare. These impacts are already being felt in Europe as a result of the European Union's (EU) implementation of the General Data Protection Regulation (GDPR) this past May. Writing at the American Enterprise Institute some months after GDPR's implementation, Daniel Lyons notes the effects such a rule would be likely to have on diminished consumer welfare:

> *The chilling effect on digital products available to European consumers could be significant. Even if companies are not actively marketing to European residents, they may have European visitors interacting with their webpage, taking advantage of marketing offers, or subscribing to newsletters. If these interactions result in retention of personally identifiable information, the company is subject to the GDPR. The ease with which a company may find itself bound, coupled with the cost of compliance and potentially draconian penalties for violation, creates strong incentives for companies to withdraw -- aggressively -- from European markets.*[5]

A 2013 report commissioned by the U.S. Chamber of Commerce notes similar impacts that would be felt by consumers as a result of potential trade disruptions to cross-border data flows stemming from the GDPR. The report argues that the negative impact on EU gross domestic product (GDP) could reach -0.8% to -1.3%.[6] It continues:

> *EU services exports to the United States drop by -6.7% due to loss of competitiveness. As goods exports are highly dependent on efficient provision of services (up to 30% of manufacturing input values come from services), EU manufacturing exports to the United States could decrease by up*

Number 180821780-8780-01. 9 Nov. 2018. https://www.scribd.com/document/393092584/Committee-for-Justice-Comments-to-the-NTIA-on-Developing-the-Administration-s-Approach-to-Consumer-Privacy#from_embed. ("Many of the recent privacy proposals wouldn't protect consumers, but would make America more like Europe. The United States' economic growth and status as a global leader in innovation will depend on a thorough evaluation of risks when crafting our nation's approach to consumer privacy. As calls for data privacy in the United States echo those heard in Europe, it is important to remember the fate of the European Union's digital economy at the hands of a strict regulatory regime. We should learn from their mistakes.")

[4] Ashley Baker, "CFJ Files Comments with NTIA on Developing the Administration's Approach to Consumer Privacy," 13 Nov. 2018. https://www.committeeforjustice.org/single-post/Developing-the-Administration%E2%80%99s-Approach-to-Consumer-Privacy.

[5] Daniel Lyons, "GDPR: Privacy as Europe's tariff by other means?," American Enterprise Institute, 3 July 2018, https://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/.

[6] Matthia Bauer, et. al., "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce," European Centre for International Political Economy, report commissioned by the U.S. Chamber of Commerce, Mar. 2013, p. 3, https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

to -11%, depending on the industry. In such case, the export benefits produced by the EU-U.S. FTA are eradicated by a good margin.[7]

The end result would be a direct negative welfare effect on four-person households of about $1,353 per year.[8] As these examples show, government-imposed restrictions on data collection would undercut economic growth, the vibrancy of the online ecosystem, and consumer satisfaction.[9]

In recent decades, consumers' personal and professional lives have been transformed for the better by a vast collection of data-driven online resources that are subsidized by advertising and made available at no cost. These resources are an engine of economic growth, even when other sectors experience difficult economic times. Data-driven marketing is estimated to have added more than $200 billion to the U.S. economy in 2014, a 35% increase over just two years earlier.[10]

Restrictions on such marketing would slow or reverse this economic growth, while hurting consumers by causing the demise of many of the data-driven online resources they rely on. Policies must strike a balance between realistic consumer privacy preferences and access to information.

Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?

Consumer variation in privacy preferences are no different than the variance in individual preferences for any other type of good or service. The strength and vibrancy of the American economy is predicated on a choice-based market architecture that optimizes the distribution of scarce resources to their highest leveraged uses.

What are the effects, if any, on competition and innovation from privacy interventions, including from policies such as data minimization, privacy by design, and other principles that the Commission has recommended?

Anticipatory regulatory frameworks that attempt to address privacy concerns by relying on broad one-size-fits-all rules will inevitably come at the expense of both innovators and consumers.

Data minimization and purpose-limitation mandates make it far more difficult to transmit information between firms, industries, and national borders.[11] The impact of such rules would have negative

[7] *Id.*

[8] *Id.*

[9] *See,* Curt Levey and Ashley Baker, *Letter for the Record to Members of the House Committee on Energy and Commerce on Facebook, Transparency, and Use of Consumer Data*. 10 April 2018, https://www.committeeforjustice.org/single-post/Letter-for-the-Record-to-Members-of-the-House-Committee-on-Energy-and-Commerce-on-Facebook-Transparency-and-Use-of-Consumer-Data.

[10] John Deighton and Peter Johnson, "The Value of Data 2015: Consequences for Insight, Innovation and Efficiency in the U.S. Economy." Data & Marketing Association. Dec. 2015, http://thedma.org/advocacy/data-driven-marketing-institute/value-of-data/.

[11] *See*, Sarah Wheaton, "5 BIG Reasons Europe Sucks at Curing Cancer," *Politico*, 12 Oct. 2018, https://www.politico.eu/article/cancer-5-big-reasons-europe-sucks-at-curing/.

consequences for every sector of the economy that makes use of data and the ripple effect would be felt across the entire economy.[12]

Similarly, mandating opt-in default architectures imposes very real economic costs to firms and researchers. When platforms have to obtain affirmative consent, companies have less money to invest in research and development.

Furthermore, such requirements favor incumbent firms already known to users, regardless of the data protection frameworks actually implemented in practice.[13]

> *Opt-in can lead to less information sharing not because people who genuinely value privacy are no longer allowing their personal data to be traded, but rather because companies may find it too expensive to administer an opt-in program and because, due to inertia, people simply accept the opt-in no-sharing default regardless of their privacy preferences. An opt-in rule would therefore be inefficient because it could discourage too many individuals from participating.[14]*

Large companies can typically survive these decreases in revenue and increased compliance costs, while smaller companies may no longer be able to operate. Public debate is disproportionately focused on large companies, but the vast majority of Internet companies fall in the latter category and include the very companies that might otherwise grow to compete with and even supplant the other tech giants of today.

These effects are not merely hypothetical. Indeed, one need only look at the devastating impact of restrictive regulations in the EU. For example, following the implementation of the opt-in model mandated in the EU's Privacy and Electronic Communications Directive (2002/58/EC), online ads became 65 percent less effective.[15] This is also one of the reasons for the absence of tech startups in Europe.[16] The inability to generate online revenue and to develop new products forms a roadblock for venture capital investments.

Accordingly, sweeping ex ante regulatory approaches like GDPR, and the recently-passed California Consumer Privacy Act, are also likely to create an artificial imbalance in the competitive ecosystem in which many firms operate. This imbalance is likely to result anticompetitive lock-in effects for incumbent firms. Unlike their resource-lean startup counterparts, large companies are far better situated to devote labor costs and time to addressing the increased compliance costs necessitated by broad data protection

---

[12] The GDPR, for example, would have made it impossible for the Danish Cancer Society to conduct the study that helped dispel the myth of a correlation between mobile cellular phone use and cancer. See Patrizia Frei et al., "Use of Mobile Phones and Risk of Brain Tumours: Update of Danish Cohort Study," BMJ, 20 Oct. 2011, https://www.cancer.dk/dyn/resources/File/file/9/1859/1385432841/1_bmj_2011_pdf.pdf.

[13] Alec Stapp and Ryan Hagemann, *Comments submitted to the National Telecommunications and Information Administration in the Matter of: Request for Comments on Developing the Administration's Approach to Consumer Privacy*, Docket Number 180821780-8780-01, submitted 8 Nov. 2018, p. 4, https://www.ntia.doc.gov/files/ntia/publications/niskanen_center.pdf. ("Opt-in choice architecture is inferior to opt-out because it is biased toward incumbents. Users might be more willing to affirmatively give consent to businesses they already know, even if a newer company with less brand recognition has the same or better data security practices. Any data accountability frameworks, regulations, or principles should expressly disavow a mandatory default opt-in regime for data collection.")

[14] Robert W. Hahn and Anne Layne-Farrar, "The Benefits and Costs of Online Privacy Legislation," AEI-Brookings Joint Center for Regulatory Studies, Working Paper 01-14. Oct. 2001, p. 58, http://papers.ssrn.com/abstract_id=292649.

[15] Alan McQuinn. "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules." Information Technology and Innovation Foundation. 6 Oct. 2017, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.

[16] Mark Scott. "For Tech Start-Ups in Europe, an Oceanic Divide in Funding." *The New York Times*. 19 January 2018. https://www.nytimes.com/2015/02/14/technology/for-tech-start-ups-in-europe-an-oceanic-divide-in-funding.html.

mandates like the GDPR. In other words, as privacy-based compliance costs in a given digital market increase, the level of new entrants to, and competition among firms within, that market is likely to decline.[17]

Prioritizing opt-out regimes could be a more efficacious mean of effectively balancing protections for consumers with privacy concerns against the need for flexibility in new business models whose data collection practices may prove far more appealing to the broader public.

Some academic studies have highlighted differences between consumers' stated preferences on privacy and their "revealed" preferences, as demonstrated by specific behaviors. What are the explanations for the differences?

As the FTC accurately noted in its own background information for this hearing, "consumers have expressed concern about the growing collection and use of their data, and businesses have enhanced their ability to link consumers' behavior across devices and platforms." And yet an "expression of concern" does not necessarily correlate to a subsequent action consumers may take to address those concerns.

Indeed, the wealth of academic literature and behavioral experiments examining the gap between stated and revealed consumer preferences vis-a-vis privacy clearly shows that consumers, on the whole, do not value their online privacy more than access to zero-cost online services. Why the disconnect?

These differences could be the result of privacy being just one component of a more complex bundle of values, the contextual nature of consumer valuations that occur in the moment and are subject to change on a whim, and a general lack of consensus regarding what constitutes the "boundaries" of ownership over individual data.[18] In comments to the NTIA, Alec Stapp and Ryan Hagemann summarized these effects:

> *Most research and behavioral studies conclude that privacy is highly context-dependent. Privacy valuations are subject to cognitive biases, including social desirability bias (e.g., people are less likely to share embarrassing information) and the endowment effect. Most people care a great deal about privacy harms that result in material and financial costs, such as identity theft, or the*

[17] Susan E. McGregor and Hugo Zylberberg, "Understanding the General Data Protection Regulation: A Primer for Global Publishers," Tow Center for Digital Journalism at Columbia University (New York, NY: Mar. 2018), pp. 37-38, https://doi.org/10.7916/D8K08GVB. ("As of 2017, Google and Facebook claim seventy-seven cents of every dollar spent on digital advertising in the United States, with no other single company claiming even as much as three percent of the total market share. While the GDPR may hinder some of these companies' data collection and/or sharing activities, the regulation may well squeeze smaller advertising networks even more, potentially magnifying the dominance of this duopoly in online advertising. These smaller ad networks, for example, typically lack the direct consumer relationships needed to secure consent from users on their own behalf, but may also find that media publishers and other website hosts are reluctant to ask for user consent for the broad range and volume of data that these advertisers can presently access without hindrance. Without access to the data on which they currently rely, smaller advertising networks may be simply cut out of the online market altogether unless they can find a way to gain some advantage over the platforms in compliance, user-friendliness, or rates. In this environment, platform companies and website hosts—such as media companies—that have a brand-name relationship to their users are likely to have more success in persuading individuals to give up their information, and therefore may have increased power in the advertising market under the GDPR.")

[18] Alec Stapp and Ryan Hagemann, *Comments submitted to the Federal Trade Commission in the Matter of: Hearing on Competition and Consumer Protection in the 21st Century: The Intersection Between Privacy, Big Data, and Competition*, Docket Number FTC-2018-0051, Project Number P181201, submitted 20 Aug. 2018, https://niskanencenter.org/wp-content/uploads/2018/08/Comments-Privacy-Big-Data-and-CompetitionFTC.pdf.

> *revelation of sensitive personal information to their close social circles. They tend to care far less about data collected about their purchasing patterns and website browsing activity by companies storing that information on distant, largely-inaccessible data server farms. This is especially true when consumers receive what they judge to be considerable benefits at a functional cost to them of zero dollars and zero cents.*[19]

Public opinion polls showing support for stronger data protections are misleading because they rarely confront consumers with the monetary and other costs of their choices.[20] A 2016 study found that, despite most participants' unease with an email provider using automated content analysis to provide more targeted advertisements, 65 percent of them were unwilling to pay providers *any* amount for a privacy-protecting alternative.[21]

However, in the real world, consumers will lose free email and social media if government-imposed privacy regulations cut into providers' advertising revenue. Moreover, such studies remind us that most consumers do not value data privacy enough to pay anything for it.

That should not be too surprising considering that today's thriving but largely unregulated social media ecosystem is not something that was thrust upon consumers or arose from factors beyond their control. Instead, it arose through the collective choices and values tradeoffs of billions of consumers.

CONCLUSION

In a 2014 *Foreign Affairs* essay, Craig Mundie considers what might have become of the digital economy "if, in 1995, comprehensive legislation to protect Internet privacy had been enacted."

Such policies, Mundie concludes, would have utterly failed to anticipate the complexities that arose after the turn of the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in ways that were difficult to imagine over a decade and a half ago, and it has created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later.[22]

As the FTC continues to consider the issue of consumer privacy in the digital age, it would do well to embrace a policy of restraint and forbearance.

---

[19] Alec Stapp and Ryan Hagemann, *Comments submitted to the National Telecommunications and Information Administration in the Matter of: Request for Comments on Developing the Administration's Approach to Consumer Privacy*, Docket Number 180821780-8780-01, submitted 8 Nov. 2018, p. 10, https://www.ntia.doc.gov/files/ntia/publications/niskanen_center.pdf.

[20] Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules." Information Technology and Innovation Foundation. 6 Oct. 2017, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.

[21] Lior Jacob Strahilevitz and Matthew B. Kugler. "Is Privacy Policy Language Irrelevant to Consumers?" *The Journal of Legal Studies* 45, no. S2. Sept. 9, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449.

[22] Craig Mundie, "Privacy Pragmatism," Foreign Affairs, Vol. 93, No. 2 (March/April 2014), p. 517, http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.

APPENDIX A: SUMMARY OF COMMENTS FILED WITH THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

CFJ Files Comments with NTIA on Developing the Administration's Approach to Consumer Privacy

On Friday, November 9, the Committee for Justice (CFJ) responded to the National Telecommunications and Information Administration's (NTIA) Request for Comments on Developing the Administration's Approach to Consumer Privacy. CFJ's comments emphasize the need to prioritize economic prosperity and preserve the United States' role as leader in technological innovation by learning from the disastrous results of privacy regulations abroad.

Key recommendations include:

- **Many of the recent privacy proposals wouldn't protect consumers, but would make America more like Europe.** The United States' economic growth and status as a global leader in innovation will depend on a thorough evaluation of risks when crafting our nation's approach to consumer privacy. As calls for data privacy in the United States echo those heard in Europe, it is important to remember the fate of the European Union's digital economy at the hands of a strict regulatory regime. We should learn from their mistakes.
- **Data protection policies could deter venture capital investments and strangle U.S.-based tech start-ups.** The EU's Directive 2002/58/EC, which mandated an opt-in policy to obtain affirmative consent, is an unfortunate example of this. Additionally, as a result of these measures, small companies have less money to invest in research and development for new products and services and may even shut down. Opt-in policies are also illogical since the knowledge that privacy settings can be changed acts as a form of affirmative consent.
- **Data privacy concerns should not be confused with the constitutional right to privacy found in the Third, Fourth, and Fifth Amendments—which protect us from government intrusions—or even the common law and statutory protections available when a private actor coercively violates our privacy.** The public debate often conflates the true privacy rights that protect us from involuntary intrusions by the government and private actors with proposed privacy policies affecting the data we voluntarily convey to tech platforms. This conflation has been made worse by the European Union, which has labeled its package of privacy policies as a fundamental right, even though many of those policies are at odds with the free speech and economic rights prized by Americans (for example, see the EU's "Right to Be Forgotten"). This is a very important distinction to maintain.
- **The Federal Trade Commission (FTC) already has the appropriate statutory authority to protect consumer privacy.** The FTC should continue its role as the safeguard against unscrupulous data practices. Rushed attempts to implement a federal privacy policy are unnecessary since the FTC has proven to be an effective policeman. As for changes with regard to process, it could be helpful for the FTC to develop guidelines to determine the need to bring an enforcement action, especially as the data ecosystem expands with the Internet of Things (IoT). However, this should only be done after the careful evaluation of public input.
- **The Administration should pay particular attention to proposed state regulations that threaten to create a patchwork of regulations that could strangle new businesses and technologies with contradictory laws and enforcement.** When faced with compliance and financial burdens, new

technology companies—and the tax revenue and job creation they produce—tend to move to favorable regulatory environments. Since technology, by nature, cannot be confined within state borders, these companies are more likely to choose to operate outside of the United States.

- **When crafting a data protection framework, it is especially important that our government understands the unique features of emerging technologies in order to avoid ill-suited or unnecessary regulations that would impede their adoption.** For instance, the protection of privacy in AI systems can be facilitated by the "black box" nature of machine learning combined with careful handling of the training data sets used. If those data sets are properly disposed of once the learning phase is complete, the neural network capture the knowledge they need to perform without preserving any of the individual data that could compromise privacy.

APPENDIX B: TEXT OF COMMENTS FILED WITH THE NTIA

RE: Developing the Administration's Approach to Consumer Privacy

DOCKET ID: 180821780-8780-01
SUBMITTED: NOVEMBER 9, 2018

ASHLEY BAKER
DIRECTOR OF PUBLIC POLICY
THE COMMITTEE FOR JUSTICE

INTRODUCTION

Founded in 2002, the Committee for Justice (CFJ) is a nonprofit legal and policy organization that promotes and educates the public and policymakers about the rule of law and the benefits of constitutionally limited government. Consistent with this mission, CFJ advocates in Congress, the courts, and the news media about a variety of law and technology issues, encompassing administrative law and regulatory reform, free speech, data privacy, and antitrust law.

CFJ has a long history of leadership on the issue of federal judicial nominations and the confirmation process in the Senate. Our voice and influence are amplified during confirmation battles for judicial nominees and the period of close analysis of their rulings that inevitably follows, giving us a unique and high-profile platform to focus attention on issues at the intersection of law and technology by highlighting how those issues will be impacted. For example, CFJ recently submitted a letter to the Senate Judiciary Committee explaining why the confirmation of Supreme Court Justice Brett Kavanaugh would be good for technological innovation and the economic growth it spurs.[23]

In the past year, CFJ has actively advocated for digital privacy protections in Congress, the federal courts, and the Supreme Court.[24] Today, our focus is on innovation, free speech, and economic growth. We believe that restrictive new requirements for data collection and use are not only unwarranted but would also threaten the online ecosystem that has transformed our daily lives in recent decades.

RECOMMENDATIONS

Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items? Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes are described? Are there any risks that accompany the list of outcomes, or the general approach taken in the list of outcomes?

[23] The Committee for Justice, *Letter to the Senate Judiciary Committee in Support of Brett Kavanaugh.* 4 Sept. 2018, https://docs.wixstatic.com/ugd/3bb067_f0fe37f564ac4afb8ff8c688a84faa21.pdf.

[24] See, *e.g.,* amicus briefs filed in *Carpenter v. United States* (August 2017), https://www.scribd.com/document/356288790/Amicus-Brief-Filed-in-Carpenter-v-United-States *and United States v. Kolsuz* (March 2017), https://www.scribd.com/document/355249553/United-States-v-Kolsuz-Amucis-Brief; letter to Congress in support of the CLOUD Act (March 2018), https://www.committeeforjustice.org/single-post/support-clarifying-lawful-use-data.

The United States' economic growth and status as a global leader in innovation will depend on a thorough evaluation of risks when crafting our nation's approach to consumer privacy. As calls for data privacy in the United States echo those heard in Europe, it is important to remember the fate of the European Union's digital economy at the hands of a strict regulatory regime.

The European Union's Directive 2002/58/EC[25] is an unfortunate example of this. The rule mandated an opt-in policy requiring businesses to obtain affirmative consent from consumers before collecting and processing data about them, because they believe such a requirement is necessary to ensure people have full control of their personal information.

In the recent debate over data privacy in the United States, many proposals have included an opt-in policy. The decision to include a similar measure would have huge implications for the availability and use of data in the ad-based revenue model that is the lifeblood of the online ecosystem. When platforms have to obtain affirmative consent, companies have less money to invest in research and development for new products and services and may even shut down.

Although a reduction in advertisements and data use may initially sound appealing to the Administration, the prospect of becoming more like Europe undoubtedly does not. After Europe implemented this opt-in model, online ads became 65% less effective.[26] It is also one of the reasons for the dearth of tech startups in Europe.[27] The inability to generate online revenue and to develop new products forms a roadblock for venture capital investments.

Although privacy fundamentalists stress the necessity of opt-in notifications, a recent poll indicates that 74 percent of Facebook users are aware of their current privacy settings, and 78 percent said they knew how to change them.[28] Therefore, opt-in policies would not only harm small businesses, they are also based on the falsehood that most American consumers are unwittingly opting for lesser privacy protections.

This decision has huge implications for the availability and use of data in the online ecosystem that is built on the financial model of online ads that run off this information. When platforms have to obtain affirmative consent, companies have less money to invest in new products and services and can even be forced to shut down. Opt-in policies are also less user-friendly, and they are designed to meet the demands of a small group of privacy advocates. The only difference is the economic impact.

Should the Department convene people and organizations to further explore additional commercial data privacy-related issues? If so, what is the recommended focus and desired outcomes?

It is especially important that our government has an understanding of the unique features of emerging technologies in order to avoid ill-suited or unnecessary regulations that would impede their adoption. For instance, the protection of privacy in AI systems can be facilitated by the "black box" nature of machine learning combined with careful handling of the training data sets used. If those data sets are properly disposed of once the learning phase is complete, the neural network capture the knowledge they need to perform without preserving any of the individual data that could compromise privacy.

[25] OJ L 201, 31.7.2002, p. 37–47, ELI: http://data.europa.eu/eli/dir/2002/58/oj.

[26] Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules." Information Technology and Innovation Foundation. 6 Oct. 2017, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.

[27] Mark Scott, "For Tech Start-Ups in Europe, an Oceanic Divide in Funding." *The New York Times*. 19 Jan. 2018, https://www.nytimes.com/2015/02/14/technology/for-tech-start-ups-in-europe-an-oceanic-divide-in-funding.html.

[28] *Reuters*/Ipsos poll. *Three-quarters Facebook users as active or more since privacy scandal*. May 2018, https://www.reuters.com/article/us-facebook-privacy-poll/three-quarters-facebook-users-as-active-or-more-since-privacy-scandal-reuters-ipsos-poll-idUSKBN1I7081.

An effective approach would also pay particular attention to proposed state regulations that threaten to create a patchwork of regulations that could strangle new businesses and technologies with contradictory laws and enforcement. When faced with compliance and financial burdens, new technology companies—and the tax revenue and job creation they produce—tend to move to favorable regulatory environments. Since technology, by nature, cannot be confined within state borders, these companies are more likely to choose to operate outside of the United States.

Do any terms used in this document require more precise definitions? Are there suggestions on how to better define these terms? Are there other terms that would benefit from more precise definitions? What should those definitions be?

While consumer privacy is an important concern of our legislators and regulators, it should not be confused with the constitutional right to privacy found in the Bill of Rights' Third, Fourth, and Fifth Amendments –which protect us from government intrusions – or even the common law and statutory protections available when a private actor coercively violates our privacy, say by breaking into our computer. Although there is a clear legal distinction in the United States, the public debate often conflates the true privacy rights that protect us from involuntary intrusions by the government and private actors with proposed privacy policies affecting the data we voluntarily convey to tech platforms.

This conflation has been made worse by the European Union, which has labeled its package of privacy policies as a fundamental right, even though many of those policies are at odds with the free speech and economic rights prized by Americans (for example, see the EU's "Right to Be Forgotten"). The Administration needs to avoid conflation of true privacy rights and proposed privacy policies because failure to do so can a.) lead to legislation or regulations that unnecessarily increase the very intrusion and excessive executive power that the Bill of Rights' privacy protections were aimed against, and b.) cut off the debate and balancing that is needed to weight the benefits of those policies against the harm they can do to American innovation and leadership in the online ecosystem and the economic growth and consumer choices that has spurred.

One of the high-level end-state goals is for the FTC to continue as the Federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction. In order to achieve the goals laid out in this RFC, would changes need to be made with regard to the FTC's resources, processes, and/or statutory authority?

No changes to statutory authority are necessary because consumer data is protected by the Federal Trade Commission's vigorous enforcement of its data privacy and security standards using the prohibition against "unfair or deceptive" business practices in Section 5 of the Federal Trade Commission Act 15 U.S.C. §45(a), The FTC has already proven to be an effective safeguard against unscrupulous data practices.[29] While some would argue that without formal rulemaking authority the FTC cannot adequately protect consumers, past examples prove the contrary. FTC enforcement protects against identifiably harmful practices, not potential future harm.

For example, the FTC's complaint against Sequoia One alleged that the company sold the personal information of payday loan applicants to non-lender third-parties and one of these third parties used the information to withdraw millions of dollars from consumers' accounts without their authorization.[30] This is

[29] *See, e.g.,* Federal Trade Commission. *FTC Staff Report: Self-regulatory Principles for Online Behavioral Advertising*. 2009. https://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral; Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace*. 2000. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[30] Federal Trade Commission. *FTC Puts an End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts.* 2016. https://www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million.

just one case in which the FTC has shown a willingness to bring enforcement actions against companies that sell their analytics products to customers if they know or have reason to know that those customers will use the products for illegal purposes.

While the FTC's statutory authority is adequate, it is not known whether future resources may be needed in order to provide the agency with technical ability and required expertise. This is something the NTIA could evaluate. As for changes with regard to process, it could be helpful for the FTC to develop a "test" or set of guidelines that would determine the need to bring an enforcement action. This could be helpful in providing efficient protection as the data ecosystem expands with the Internet of Things (IoT). However, this should only be done after the careful evaluation of public input.

CONCLUSION

To fundamentally address the current privacy concerns about the Internet, we really would need to start over from scratch. That's because the privacy problems have their roots in decisions made and directions taken decades ago concerning the Internet's technical structure and the business model that supports most of the enterprises on the world wide web.

When the Internet was conceived and designed 50 years ago, the goal was to make the flow of data easy and virtually indiscriminate in both directions – that is, sending and receiving. The Internet privacy problem arises from the successful achievement of that goal. Contrast that with television and radio, which has a one-way flow, or traditional telephony, in which only a limited amount of information flows back to the service provider.

In the 1990s, when the world wide web emerged and made the Internet a household word, people wondered how the exploding number of websites were going to convert their popularity into profitability and sustainability. The answer turned out to be, for the most part, selling advertising. It was inevitable that web sites would sell their competitive advantage – that is, access to user data – to advertisers, which provided the second necessary component for today's privacy problem. With an open Internet architecture and a business model driven by user data, it was just a matter of time and growth until today's controversies erupted.

That said, it is not feasible to start over from scratch. The open, two-way architecture of the Internet is baked in and it is hard to see how any substantial change would be possible. Business models evolve slowly rather than abruptly, so an end to websites' reliance on user data-driven advertising is not something we'll see in the next decade if ever. With the two big enablers of today's privacy concerns here to stay, if the United States to continue its role as a leader of technological innovation enjoy the economic prosperity that it creates, we are stuck with the technological ecosystem that we currently have. Trying to reinvent the wheel through data privacy regulations would make the United States less great and more like Europe. It is best to proceed with caution and learn from the mistakes and failures of others abroad.