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 National Telecommunications and Information Administration:

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 JUSTUCE

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.[1]

In the past year, 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 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?

[1] The Committee for Justice, Letter to the Senate Judiciary Committee in Support of Brett Kavanaugh (Sept. 2018), https://docs.wixstatic.com/ugd/3bb067_f0fe37f564ac4afb8ff8c688a84faa21.pdf.
[2] 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.scribd.com/document/371541902/ClarifyingLawful-Overseas-Use-of-Data-CLOUD-Act-of-2018.

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[3] 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.[4] It is also one of the reasons for the dearth of tech startups in Europe.[5] 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.[6] 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.

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—

[3] OJ L 201, 31.7.2002, p. 37–47, ELI: http://data.europa.eu/eli/dir/2002/58/oj.
[4] McQuinn, Alan. "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules." Information Technology and Innovation Foundation. Oct.6, 2017. https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules
[5] Scott, Mark. "For Tech Start-Ups in Europe, an Oceanic Divide in Funding." The New York Times. January 19, 2018. https://www.nytimes.com/2015/02/14/technology/for-tech-start-ups-in-europe-an-oceanic-divide-in-funding.html.
[6] 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.

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.

What should those definitions be? 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. 1. 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.[7] 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.[8] This is 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"

---

[7] *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.

[8] *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.

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.