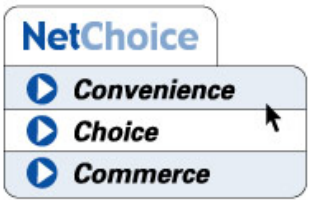
NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Steve DelBianco, President
Carl Szabo, Vice-President & General Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7498



www.netchoice.org

November 8, 2018
SUBMITTED ELECTRONICALLY
United States Department of Commerce
National Telecommunications and Information Administration

NetChoice Response to National Telecommunications and Information Administration Request for Request for Comments on Developing the Administration's Approach to Consumer Privacy - Docket No. 180821780-8780-01

NetChoice submits this response regarding the National Telecommunications and Information Administration's ("NTIA") request for comments on "Request for Comments on Developing the Administration's Approach to Consumer Privacy."

NetChoice is a trade association of leading e-commerce and online companies promoting the value, convenience, and choice of internet business models. Our mission is to make the internet safe for free enterprise and for free expression. We work to promote the integrity and availability of the global internet and are significantly engaged in privacy issues in the states, in Washington, and in international internet governance organizations.

The role for government should be in areas where users and business cannot act alone, such as including law enforcement, international data flows, and pre-empting a patchwork of state laws conflicting with federal interests. Government should use its powers to pursue online fraud and criminal misuse of data, not to create rules that narrowly prescribe what and how data should be used.

Overall, we support the notion that companies and customers – not governments – must take the lead on data privacy. Companies need to pursue innovation without asking for permission from government agencies. And consumers must understand the decisions they make, but they must be allowed to make those decisions for themselves.

Discussion about advancing consumer privacy while protecting prosperity and innovation is at its core a conversation about consumer choice. It is essential to consider (1) whether consumers should be empowered to decide what information they are comfortable sharing

online and (2) whether consumers should be empowered to choose between competing services that offer varying levels of personalization. If consumer choice is to be preserved, any regulation must heed these questions and proceed accordingly.

At the same time, we must balance consumer choice interests with a recognition that the option for consumers to share personal data in exchange for free or discounted personalized services can provide a great benefit to consumers. NTIA should seek to protect such consumer benefits rather than hamper American innovation.

To that end we suggest that the NTIA create and promote federal legislation that sets a nationwide standard for privacy laws and data breach laws.

Americans Prefer Choice Over Regulation

State and federal legislators on both sides of the aisle have called for more regulation of the technology industry. However, new research from NetChoice shows that Americans want a light regulatory touch for tech companies, believing that consumer spending and online surfing habits should be the ultimate means of ensuring competition and consumer choice.[1]

According to a survey of more than 1,200 U.S. consumers conducted by Zogby Analytics, 48% of consumers say government regulations on the internet are bad for consumers with only 16% believing that Apple, Google, and Facebook could not be unseated by better competitors.

Americans Oppose Heavy-Handed Government Regulation

NetChoice polling found that:

- 48% of consumers say government regulations on the internet are bad for consumers with only 16% believing that Apple, Google, and Facebook could not be unseated by better competitors.
- 40% of consumers say any tech breakup would mainly reward traditional industries competing with tech or anti-business groups.
- 86% of Americans with an opinion said that the government should not prevent tech companies from acquiring startups.

NetChoice polling also shows that Americans prefer that consumers have control over how to use their tech. This was evident through responses on a variety of subjects spanning from children's tech use to default color schemes on phone screens.

As online platforms have grown and are increasingly a central part of modern-day life, some politicians feel the urge to regulate them. Policy proposals range from privacy regulation to antitrust reform, but our polling revealed that the public does not support further government intervention in the tech industry.

---

[1] Available at NetChoice.org/TechLashPoll

Americans are not comfortable with the government telling either online platforms or their consumers how to offer their services. 75% say that parents should be allowed to have their children use messaging apps that do not collect personal information or permit targeted advertising, and 85% say parents are best situated to decide what tech their children should be able to use.

Policies offered up by anti-tech advocates aren't popular either. Only 6% of Americans would support a government mandate that requires phone screens being set to black and white by default.[2]

Americans aged 18-24 also trust tech platforms more than many other major industries.

Young Americans aged 18-24 also trust tech platforms more than many other major industries. Only 26% of Americans aged 18-24 said they don't trust tech platforms, whereas almost a third said they don't trust internet service providers—and over half said they don't trust oil companies. Almost half of all Americans agreed with the overall statement that government regulation on the internet would be bad for consumers.

Online platforms are becoming a central part of modern life, but that doesn't mean they require heavy-handed government intervention to prevent consumer harm. Low barriers to entry and the highly competitive nature of online markets have ensured that while dominant tech platforms have emerged, consumers remain empowered and don't believe the government needs to step in to protect them.[3]

Clearly there is a disconnect between American consumers and the anti-tech community as Americans prefer to make their own decisions rather than having a heavy-handed government determine what is "best" for them.

Americans Know that Technology Platforms Help Small Businesses

Tech also helps small businesses. According to 72% of Americans, online services like Google and Facebook keep them in better touch with their communities. Further, 71% of those aged 18-34 have discovered small businesses thanks to online platforms.

---

[2] *Id*.

[3] *Id.*

Internet Platforms Generate Significant Economic Benefits

Internet platforms also generate significant economic benefits. 77% of those polled say digital ads are valuable for small businesses, and 36% even say these ads are very valuable. 70% say digital advertising platforms are valuable to the national economy.

The Ad-Supported Model Works

The ad-supported model works.

- 42% of Americans prefer ad-supported Internet platforms that deliver ads based on preferences,
- 29% of Americans prefer ad-supported Internet platforms that deliver the same ads to all users.
- Only 16% of Americans are willing to pay for online platform services.

In 2018, politicians became concerned that online platforms use targeted advertising to fund their platforms. Yet consumers undoubtedly benefited from the wide availability of free online services made possible with the use of targeted ads.

Americans still prefer the targets advertising model over paying for online services by a margin of almost 3-to-1.

Our polling shows that Americans still prefer the targets advertising model over paying for online services by a margin of almost 3-to-1.

- Only 16% of Americans prefer to pay for online platforms like Facebook rather than see advertisements on them.

While privacy concerns may exist, consumers do not want to change the underlying model.

- 82% of Americans with an opinion prefer that online services be supported through advertising rather than charging end users.

Americans are largely content with the services they receive—a majority of Americans have never decided to stop using a social media platform.

Americans oppose antitrust actions against the tech industry

Despite what special interests say, Americans are overwhelmingly opposed to antitrust actions against tech platforms. Polling found that:[4]

- Only 10% of Americans think the government should prevent successful online businesses from acquiring other companies, and

[4] *Id*.

- Only 5% of Americans thought the government should most focus its anticompetitive resources on tech platforms. Instead, 29% think the government should most focus its anticompetitive enforcement on pharmaceutical companies, and 11% said it should most focus on the electricity and gas industry.
- Only 9% of Americans aged 18-24 believe that consumers would benefit from a break up of big tech.

Recommended Federal Actions to Create Nationwide Standard on Privacy

It is clear that as we start to see fracturing of the internet across national, and now state lines, the time has come for establishment of a nationwide standard for privacy online. This standard, as the NTIA correctly identifies, should be a better way to protect all — not relying on failed approaches abroad or domestically.

The first step is to create federal legislation that is preemptive of state privacy laws. The internet has no borders and businesses in one state should not be subjected to the whims of a foreign state's legislature. Much in the way the U.S. led in Children's Online Privacy Protection Act (COPPA)[5] and Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM),[6] we should enact federal legislation that creates a ceiling on privacy protections and creates certainty for consumers and businesses alike. Such an approach must be buttressed with clear definitions of who and what are covered.

NTIA should create federal legislation that is preemptive of state privacy laws.

This approach should also preempt the patchwork of fifty state data breach laws by creating a nationwide data breach rule.

The NTIA should then advance this better approach on privacy internationally. This would include integration of the American privacy approach in trade agreements. Also establishing that compliance with US privacy laws is adequate for foreign country's privacy laws.

Privacy legislation should address massive data collection by Non-Profit Organizations

As identified in the questions presented, we suggest that the privacy protections afforded not only apply to businesses, but also to all entities, including non-profits.

[5] 15 U.S.C. § 6501, *et sec.*

[6] 15 U.S.C. § 103.

We have seen how non-profit groups like Common Sense Media (CSM), for example, actively support legislation that has no impact on the data they collect.[7] CSM does not currently comply with General Data Protection Regulation (GDPR)[8] or the not yet implemented California Consumer Privacy Act (CCPA).[9] CSM requires users to surrender name, email address, and zip code before granting access to research papers.[10] This is just one example that shows the need to expand privacy regulation beyond just businesses.

Likewise, we have seen data breaches at non-profit organizations. Take for example the data breaches at the University of Maryland and Yale University. Since 2005, educational institutions have had an average of over 66 breaches a year.[11] Other non-profits have also had an average of over 9 data breaches since 2005.[12] That is almost one breach per month, yet none of these breaches are subject to most data breach notification laws.

As the FTC's authority is limited to commercial businesses, expended oversight would require allowing the FTC enforcement power over non-profits or allowing enforcement by the Department of Justice who can already take actions against non-commercial entities.

Protection of Small Businesses

We have seen how even the largest businesses spent combined billions of dollars to comply with the European General Data Protection Requirements (GDPR).[13] Of course these costs,

---

[7] *See, e.g.*, COMMON SENSE MEDIA: "Big Win for Kids and Families: California Passes Landmark Privacy Legislation," https://www.commonsensemedia.org/kids-action/campaign/big-win-for-kids-and-families-california-passes-landmark-privacy-legislation (last visited Nov. 1, 2018).

[8] General Data Protection Regulation (EU) 2016/679.

[9] CA Civ. Code § 1798.100, *et sec.*

[10] *See Privacy Policy*, COMMON SENSE MEDIA, https://www.commonsensemedia.org/about-us/our-mission/privacy-policy (last visited Nov. 1, 2018). *See also*, CSMConditioningAccess.png, http://netchoice.org/wp-content/uploads/CSM-conditioning-access.png, showing CSM conditioning access to a report on a visitor's remittance of name, email, and zip code.

[11] *Data Breaches (Organization Type: EDU)*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches?title=&org_type%5B0%5D=259 (last visited Nov. 1, 2018). For example, consider the following data breaches from a span of two months in 2018 alone: Trinity College of Nursing and Health Sciences on August 9, 2018; American Institute of Aeronautics and Astronautics on August 7, 2018; Yale University on July 26, 2018; Purdue University on July 13, 2018; and University of Michigan/Michigan Medicine on July 25, 2018. *Id.*

[12] *Data Breaches (Organization Type: NGO)*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches?title=&org_type%5B0%5D=263. Examples just from the past three years include: SUIU 32BJ on May 25, 2018; Valley of the Sun YMCA on January 17, 2018; YMCA of San Diego on July 12, 2017; UNM Foundation on May 17, 2017; and Public Health Institute on October 5, 2016. *Id.*

[13] "The world's 500 biggest corporations are on track to spend a total of $7.8 billion to comply with GDPR." Jeremy Kahn, *It'll Cost Billions for Companies to Comply with Europe's New Data Law*, BLOOMBERG BUSINESS (Mar. 22, 2018).

while not necessarily as high, are disproportionately expensive for small businesses. The American way on privacy should avoid costly compliance and should shield small businesses who may lack necessary funds and man-power to comply.

Defining Personally Identifiable Information (PII)

When it comes to *what* is covered, NTIA's approach on privacy should limit itself to situations that contribute to actual harms to Americans.

We have seen too often non-exclusive definitions of personally identifiable information (PII) that capture data that is anything but personal or identifying. More often than not, the definitions of PII become a wish-list for anti-business and other special-interest groups.

With this in mind, we propose the following definition for PII:

1. Identified Individual Information
    a. First name or first initial and last name along with:
        i. Alias, postal address, unique personal identifier, email address, account name, social security number, driver's license number, [or] passport number
        ii. Specific geolocation data
        iii. Professional, employment, and education information
2. Sensitive Personal Information
    a. Information that has a high likelihood of causing financial harm along with Identified Individual Information
3. Personal Information
    a. Information that is not Sensitive Personal Information and identifies, relates to, describes, is capable of being associated with Identified Individual Information

Addressing Data Breach[14] While Addressing Privacy

As the leading concern among consumers is identity theft,[15] a federal privacy bill should also address data breach. Such an approach can be based on elements from proposed federal data breach legislation. The definition for "Sensitive Personal Information" (above) can be used for addressing what is covered in a federal data breach approach.

Draft Data Breach Language:

(a) A breach notice [is required] in the event of unauthorized access that is reasonably likely to result in identity theft Sensitive Personal Information, fraud, or economic loss.[16] Such notice shall be made within a reasonable time.

---

[14] See section on "Breach Notification" below.

[15] *See* the Federal Trade Commission 2017 Consumer Sentinel Network Data Book.

[16] *See* H.R. 6743, 115th Cong. (2018).

A Covered Entity that owns or licenses computerized data that includes Sensitive Personal Information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data

(1) whose unencrypted Sensitive Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, or,
(2) whose encrypted Sensitive Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.

Disclosures shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A covered entity that maintains computerized data that includes Sensitive Personal Information that the covered entity does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A covered entity that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

(2) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(3) The title, text, and headings in the notice shall be clearly and conspicuously displayed.

> (4) For a written notice described in paragraph (1) of subdivision (d), use of the model prescribed security breach notification form or use of the headings described in this paragraph with the information described in paragraph (1), written in plain language, shall be deemed to be in compliance with this subdivision.[17]

Addressing Cross-Border Activity

Countries around the world are weaponizing "Privacy" as a trade barrier to American innovation and competition. Moreover, this new trade barrier is also acting as a form of extraterritorial reach where American businesses must now comply with foreign laws – even when the business has no presence or activity abroad.[18]

NTIA should aggressively oppose this attack on American businesses.

Federal privacy legislation could create a rebuttable presumption for American businesses and protect American businesses from extraterritorial overreach by foreign countries.

One step could be enshrining in federal legislation that compliance with the American approach constitutes compliance with requirements of foreign privacy requirements such as GDPR. In essence, the U.S. could create a rebuttable presumption for American businesses and protect American businesses from extraterritorial overreach by foreign countries.

Another approach is to incorporate such presumptions into international agreements and treaties.

We also suggest that the Commerce Department include Section 230 of the Communications Decency Act and platform liability protections into trade agreements. This further advances American notions of free expression, free enterprise, and innovation worldwide.

Self-Regulation

Rather than relying on governmental enforcement and constant oversight, we suggest an industry self-regulatory approach. The NTIA, FTC, or similar body can certify industry self-regulatory approaches. Compliance with the self-regulatory body constitutes compliance with the privacy regime. This further eliminates the need for protracted rulemakings and instead

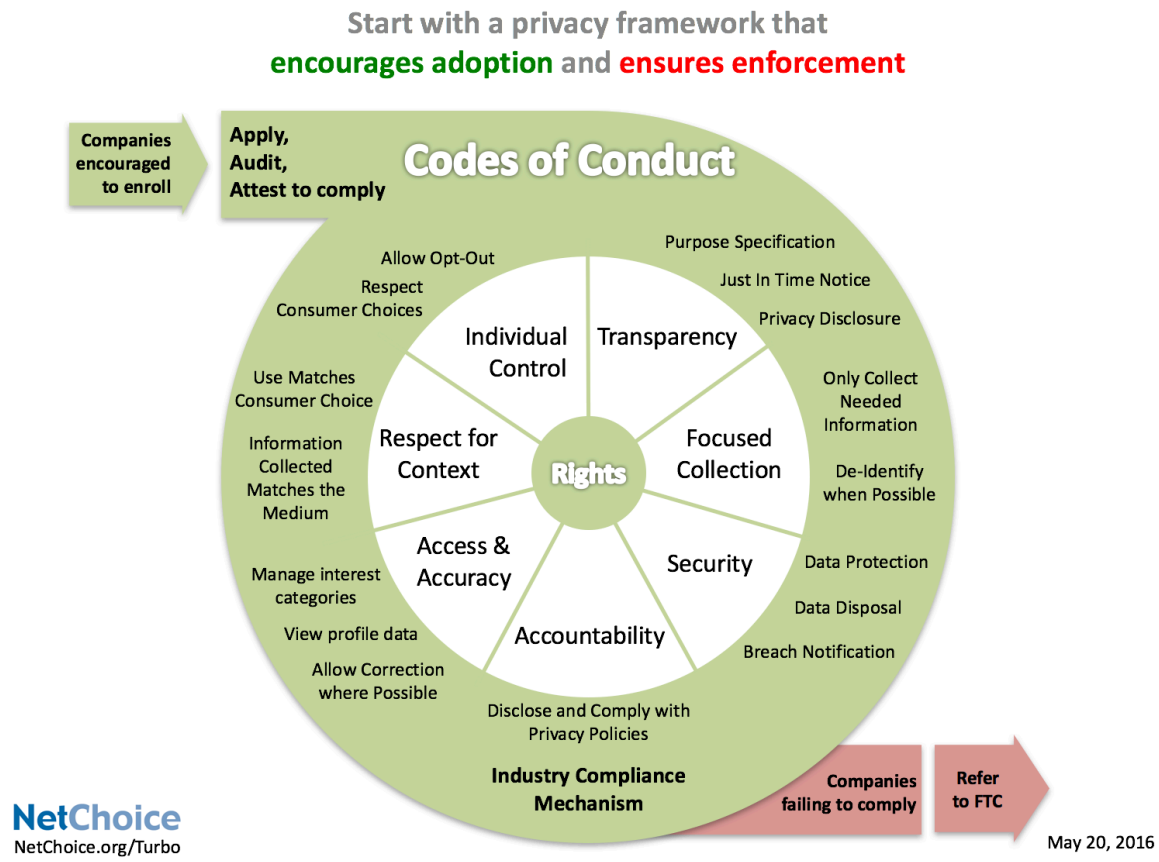
---

[17] This section is based on California data breach law. CAL. CIV. CODE § 1798.82(a).

[18] For example, GDPR applies to businesses that collect information about European citizens, even when the European citizen is in the United States. This means that a coffeeshop in DC might need to comply with GDPR if a Parisian enters the store and uses a credit card to make a purchase.

allows regulation at the speed of innovation. This approach has succeeded in protecting privacy via laws like COPPA by providing flexibility and accountability.

We offer this conceptual view of an industry self-regulatory framework that dynamically adapts to new technologies and services, encourages participation, and enhances compliance.



As seen in the conceptual overview above, components of the Fair Information Practice Principles form the aspirational core that influences business conduct regarding data privacy. From previous work by the FTC, NAI, and IAB, we've established the foundational principles for the collection and use of personal information: individual control, transparency, respect for context, access and accuracy, focused collection, accountability, and security.

Industry safe-harbors have succeeded in protecting privacy via laws like COPPA while providing flexibility and accountability.

Participating companies would publicly attest to implement Codes within their business operations, including periodic compliance reviews. If a company failed to comply with the adopted Codes, the FTC and state Attorneys General could bring enforcement actions, as is currently the case when companies fail to honor their adopted privacy policies.

Conclusion

Now is the time for America to lead the world towards a privacy protection approach that is better than the flawed efforts of foreign countries and American states. Now is the time for the NTIA to lead the effort to create a nationwide standard on privacy and data breach, and then using that as a shield to protect American businesses.

We thank you for your consideration.

Sincerely,

Steve DelBianco
President, NetChoice

Carl M. Szabo
Vice-President & General Counsel, NetChoice

NetChoice is a trade association of e-Commerce and online businesses. *www.netchoice.org*