

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

Steve DelBianco, Executive Director
Carl Szabo, Policy Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7498



www.netchoice.org

The Honorable Penny Pritzker, Secretary
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230

February 27, 2015

RE: NTIA's Proposed Privacy Legislation

Dear Secretary Pritzker,

We are writing to express concerns about the NTIA's comprehensive privacy legislation discussion draft. We would first like to thank John Verdi, John Morris, and the NTIA staff for their effort on this project.

However, the discussion draft creates new barriers to innovation in online and offline markets, and undermines our ability to forestall onerous regulation being pursued by foreign governments.

Erosion of existing industry self-regulatory practices

NetChoice has been a staunch proponent of industry self-regulation in government safe harbors. We advocated for such actions in our comments to the Department of Commerce regarding the multistakeholder process to develop consumer data privacy codes of conduct.¹

However, we worry the likely outcome of this legislation is to upend existing industry self-regulatory practices in the privacy space. The discussion draft makes the FTC sole arbiter over whether a self-regulatory program satisfies the FTC's requirements as a privacy safe-harbor. Unfortunately, the FTC is already predisposed to find fault in existing self-regulatory practices.² Thus, we find it highly unlikely the FTC will approve existing self-regulatory programs as a safe-harbor without forcing significant changes onto the existing programs.

If this is not the intention of the discussion draft, and the NTIA believes existing programs do provide adequate protections for consumers, the legislation should be modified to grant existing programs safe-harbor status.

¹ NetChoice Comments to the Department of Commerce, *Re: Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*, Docket No. 120214135-2135-01, April 2, 2012.

² See e.g. FTC Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009) "[S]taff recognized that existing self-regulatory efforts had not provided comprehensive and accessible protections to consumers."

[Creates a new definition of personal data which applies to basically every piece of electronics](#)

In today's world almost any data *could* be linked to an individual. Even de-identified data has the potential of being re-identified to connect with an individual.³ However, just because something is possibly linkable does not suggest that it is reasonably likely this data would be linked to an individual.

Unfortunately, the discussion draft ignores this difference and instead defines personal data as almost any information on any device. In essence, the legislation's definition of personal data is regulated with the higher standard this nation has used for sensitive personal information like credit or health data. Because the definition of personal data is "any device that *could be* linked to an individual" suddenly MAC addresses on household printers, college dorm routers, and apartment building server exchanges are considered "personal data." As we move into the internet-of-things, the breadth of what's covered by this new definition will only expand.

Such a broad definition of personal data gives greater authority to the FTC to regulate all online transactions, since every transaction involves collection of an IP address necessary to deliver content. Moreover, this definition threatens the ability of businesses to deliver general content that might be considered by the FTC as "personal." This represents a massive expansion of FTC power and one we caution against.

[Giving the FTC authority to levy fines grants it first-strike powers and legislative control](#)

Today, the FTC can levy fines only when a business violates an existing privacy or security settlement with the agency. This ensures the FTC acts as a regulatory agency – responding to misdeeds or consumer complaints. If the FTC is given broader powers to levy fines, the burden-of-proof is shifted away from the FTC to prove a misdeed and to a business that must now prove its innocence.

Moreover, with the ability to slap businesses with penalties of \$16,500 per violation per day, the FTC can bully business behavior under the threat of racking-up substantial fines. For example, a business with a million users and one alleged misdeed could face a fine of \$16.5 billion. With fines like that, businesses would likely bend to FTC demands rather than risk the entire business by challenging the fine.

In essence, giving the FTC broader ability to impose fines is akin to giving them rulemaking and/or legislative powers: Either do what the FTC demands, or face devastating fines.

[Degradation of Magnuson-Moss Act](#)

When Congress passed the Magnuson-Moss Act in 1975⁴ it checked the FTC's exceptionally broad powers over "unfair or deceptive" acts by requiring a transparent rulemaking process. This act by a Democratic Congress was in reaction to FTC attempts to ban broad categories of advertising and assertions that it could even use its "unfairness" power to regulate business activities beyond just trade and commerce.

However, provisions of the NTIA's discussion draft reveal an effort to roll-back this check on FTC rule-making powers. Although limited to only rule-making authority over Independent Review Boards,

³ See, e.g. Natasha Singer, *With a Few Bits of Data, Researchers Identify 'Anonymous' People*, N.Y. Times (Jan. 29, 2015). "In a study in 2008, two computer scientists, Arvind Narayanan and Vitaly Shmatikov, reported that they had been able to reidentify some Netflix users in a database of nameless customer records the company had made available for researchers competing to improve the company's recommendation engine."

⁴ See Title I of the Magnuson-Moss Warranty - Federal Trade Commission Improvements Act -- (1975) warranty provisions

NetChoice fears that any contraction of Magnuson-Moss limitations risks eroding the safeguards that Congress enacted forty years ago.

Moreover, if existing safeguards are repealed, an unchecked FTC could use its new powers to regulate the notice & choice regime under which online users consent to data practices – often in exchange for free content and services.

Threat to international agreements

The Department of Commerce advocates on behalf of American businesses on international issues like safe-harbor reauthorization. But this sweeping new regulation would provide new justification for foreign techno-nationalists to prevent American online businesses from engaging with their country's citizens.

In essence, the Department cannot say that American businesses adequately protect the privacy of foreign citizens at the same time it is advocating new legislation to solve troubling new privacy problems at home.

Lack of Justification for Legislation

When designing legislation of this magnitude, it is incumbent on the proponent to provide justification. This discussion draft lacks such justification lest you risk creating laws that do more harm than good. To date we have not seen an identification of actual harms, analysis of how existing laws address these harms, or a cost-benefit analysis of the legislation.

Recent privacy reports from the White House have relied almost exclusively on anecdotes⁵ -- not facts or analysis. Likewise, recent privacy reports from the Federal Trade Commission (FTC) failed to engage in “economically sound and evidence-based approach to consumer protection, privacy, and regulation of the Internet of Things.”⁶ Legislative proposals of this magnitude should be based on facts and analysis – not a hypothetical *parade of horrors*. Without this analysis it is unclear whether this legislation achieves the desired outcome and if such outcome overcomes its restrictions on innovation.

The Department of Commerce and NTIA are the voice of American innovation. We ask that they reconsider this discussion draft since it could seriously degrade this innovation.

We thank you for your consideration.

Sincerely,



Steve DelBianco
Executive Director, NetChoice



Carl M. Szabo
Policy Counsel, NetChoice

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

⁵ For example, the White House Report on Big data states: “current knowledge is mainly anecdotal”, and “anecdotal evidence suggests” White House *Big Data And Differential Pricing Repot*, Feb. 2015, p.11, p.17.

⁶ Dissenting Statement of Commissioner Joshua D. Wright, Issuance of *The Internet of Things: Privacy and Security in a Connected World* Staff Report, Jan. 27, 2015. “An economically sound and evidence-based approach to consumer protection, privacy, and regulation of the Internet of Things would require the Commission to possess and present evidence that its policy recommendations are more likely to foster competition and innovation than to stifle it.”