



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

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
202.420.7482
www.netchoice.org

November 2, 2012
SUBMITTED ELECTRONICALLY
Federal Trade Commission

**Request for Panelist and Comments for FTC Workshop to Explore Practices and
Privacy Implications of Comprehensive Collection of Internet Users' Data on
December 6, 2012**

NetChoice respectfully requests that Executive Director Steve DelBianco be selected as a panelist on the FTC's Workshop to Explore Practices and Privacy Implications of Comprehensive Collection of Internet Users' Data. NetChoice also provides the following comments.

NetChoice is an association of leading e-commerce and online companies, plus thousands of small businesses that rely on e-commerce. 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.

NetChoice has a long history of breaking down regulatory barriers, beginning with helping travel agents, contact lens suppliers, and real estate brokers whose online innovations clashed with legacy regulations that protect traditional business models.

Privacy-related laws that restrict how data can be collected, used, and shared also create barriers to legitimate online commerce.

Recently, NetChoice has submitted comments to the FTC on the Preliminary FTC Staff Report – *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* and on the review of the Children's Online Privacy Protection Act (COPPA), spoken as a panelist at the FTC's Public Workshop to Explore Advertising Disclosures in Online and Mobile Media, and been an active member in the NTIA Privacy Multistakeholder Process.

In addition, we submit the following topics for inclusion on the workshop's agenda:

- (a) the FTC's section 5 authority can be used in conjunction with an industry self-regulatory process to compel businesses to comply with privacy guidelines;
- (b) limit the discussion of the various uses of personal information; and
- (c) the US should lead and not necessarily follow the EU model when it comes to privacy.

Qualifications of NetChoice Executive Director Steve DelBianco as a Panelist

Steve DelBianco has worked in the online field for over fifteen years and worked with industry on privacy practices. As NetChoice's Executive Director, Steve works with NetChoice members to set and execute the coalition's agenda to promote the integrity and availability of the Internet, in the states, in Washington, and at global Internet governance organizations.

Steve is a well-known expert on online consumer protection, Internet governance, and Internet taxation. He has provided expert testimony in twelve Congressional hearings and in dozens of state legislative hearings. Also he is an active participant in the NTIA Privacy Multistakeholder process.

Most recently, Steve was a panelist at the FTC's Public Workshop to Explore Advertising Disclosures in Online and Mobile Media and will be a moderator at the Family Online Safety Institute's Annual Conference.

For over a decade, Steve has been a powerful advocate for NetChoice positions to the National Conference of State Legislatures as well as the American Legislative Exchange Council, where he was named Private Sector Member of the Year.

Regarding Internet governance, Steve has three times been elected as policy chair for ICANN's Business Constituency. He's participated in all the meetings of the UN's Internet Governance Forum (IGF) and is a leader at the IGF-USA.

This experience in Internet governance and multi-stakeholder processes makes Steve a unique panelist who can shed light on the benefits and pitfalls of such processes.

Steve is frequently quoted on technology issues in the media, including a segment on *60 Minutes* to expose barriers to innovation in residential real estate.

Before his work at NetChoice, Steve was founder and president of Financial Dynamics, an IT consulting firm that he led through the evolution of industry trends. Under Steve's leadership, Financial Dynamics grew to over \$20 million in revenues by 1997.

Today, Steve continues to advise and invest in early stage companies as a partner in venture capital funds. In addition, he served as Vice Chairman of the Board of the Virginia Economic Development Partnership.

Steve holds degrees in Engineering and Economics from the University of Pennsylvania, and an MBA from the Wharton School.

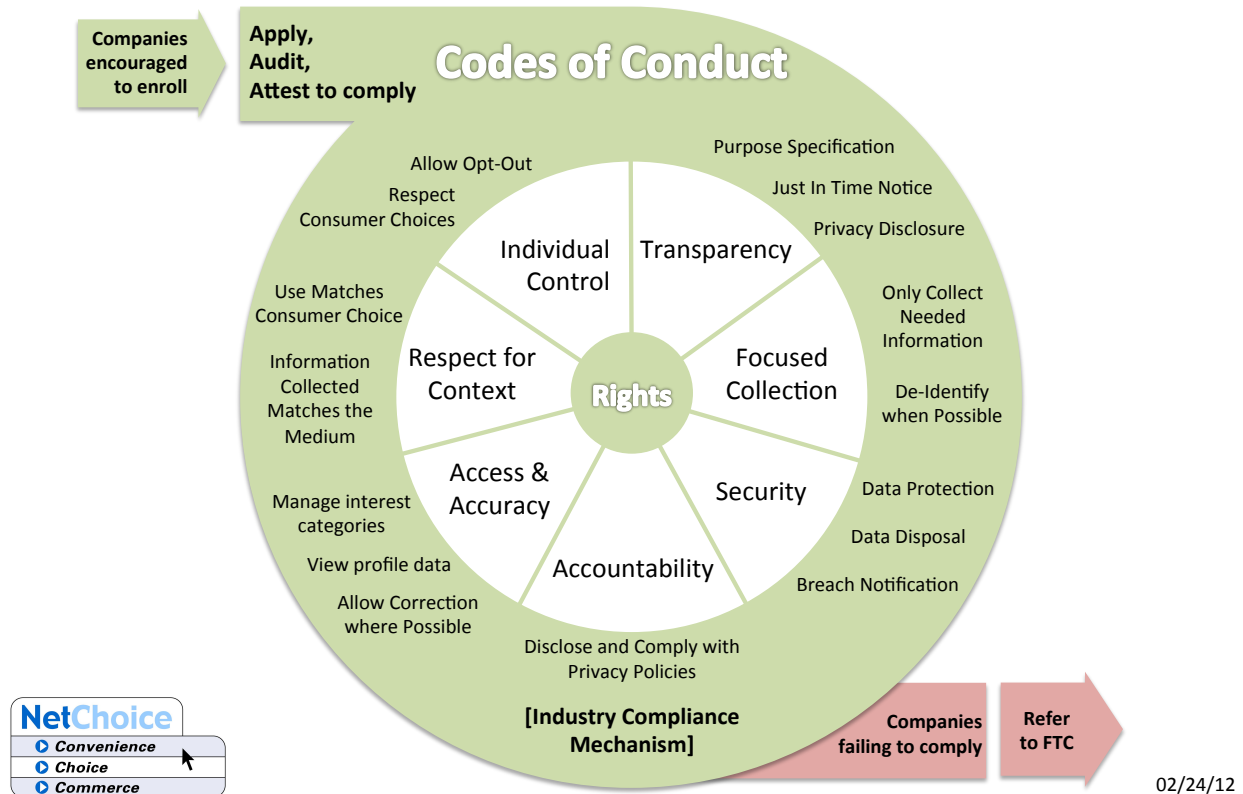
FTC's section 5 authority can be used in conjunction with an industry self-regulatory process to compel businesses to comply with privacy guidelines

Under existing authority, the FTC can encourage companies to adopt codes of conduct. This will drive businesses into adopting a privacy policy and codes of conduct that the FTC can enforce under its existing Section 5 powers.¹

¹ Assistant Secretary Strickling suggested that if a company adopts a code of conduct their violation is enforceable under Section 5 of the FTC's authority. US House of Rep. Energy & Commerce Committee Hearing, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?* (Mar. 29, 2012).

We recommend a framework built around the seven rights set forth in the White House Consumer Privacy Bill of Rights. This self-regulatory framework is dependent on government enforcement, but allows for growth and modification at the speed of the industry.

An Industry Self-Regulatory Framework to Implement and Enforce White House Privacy White Paper



As seen in this conceptual overview, the Consumer Privacy Bill of Rights (Rights) forms the aspirational core that drives business conduct for data privacy. This is accomplished *without* legislation.

Codes of Conduct (Codes) enable implementation and enforcement of the Rights. Participating companies would publicly attest to implementing 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.

Significantly, this framework does not require legislation to establish the Consumer Privacy Bill of Rights as a matter of law.²

While this framework enables continued industry self-regulation, it relies on government in three critical ways:

1. The FTC can coordination of a multistakeholder process to suggest Codes of Conduct for industry to consider;
2. FTC encouragement for companies to adopt the codes of conduct; and

² See, e.g., action taken against Google and Facebook for failure to uphold promises made to consumers.

3. FTC and state Attorneys General enforcement when companies fail to honor the principles and codes they have promised to uphold.

A year ago, NetChoice recommended an industry self-regulatory framework similar to the one above that incorporated all FIPPS.³ That model has been adjusted to incorporate the new Consumer Privacy Bill of Rights.

The FTC should consider discussing this and other proposed self-regulatory approaches to privacy.

Limit the discussion of the various uses of personal information

Rather than encouraging a discussion on *all-possible uses* of PI, we suggest that the workshop frame the discussion of uses for *only PI collected for advertising purposes*. Specifically, the workshop should frame the different uses of personal information (PI) because each use has its own discussion as different uses of PI impact people differently.

For example, the difference between using information for advertising versus its use to determine health insurance represents two different specific business contexts and, therefore, two different conversations.

If the workshop has one conversation that includes multiple uses it risks conflation of the uses and of the risks of data security breaches.

We have already seen how this conflation causes problems in privacy dialogues. In conversations involving PI both for interest-based advertising and determination of health insurance, the latter is used to justify prohibition of the former.

For example, last year at a meeting hosted by Common Sense Media⁴ to discuss privacy, the discussion of interest-based advertising occurred alongside fears concerning the use of collected personal information to deny health and housing benefits. A similar situation occurred at the 2012 State of the Net panel discussion.⁵

Moreover, the framing of uses of personal information prevents integrating discussion of collection and security with use. For example, when speaking at the Brookings Institute, Commerce General Counsel Cameron Kerry conflated a discussion of privacy with data security.⁶

In an attempt to quell concerns about use of PI to determine benefits, the DAA and IAB adjusted their self-regulatory program to prohibit the use of collected information for such uses. Nonetheless, these efforts have yet to satisfy certain groups.

Thus, a threshold matter should be to separate the discussion into the different uses of information so that a rational, non-hyperbolic conversation about uses may proceed.

By framing properly, the workshop can maintain a more productive discussion of the uses of PI.

³ See NetChoice comments to the Department of Commerce Green Paper – *Commercial Data Privacy in the Internet Economy: A Dynamic Policy Framework*.

⁴ *Protecting Privacy in the Digital Age*, National Press Club (Oct. 11, 2011).

⁵ *State of the Net 2012 Conference*, (Jan. 17, 2012).

⁶ *For Privacy, "Where's the Beef?" becomes "Where's the Harm?"*, NetChoice (July, 7, 2011), available at <http://www.netchoice.org/for-privacy-wheres-the-beef-becomes-wheres-the-harm/>.

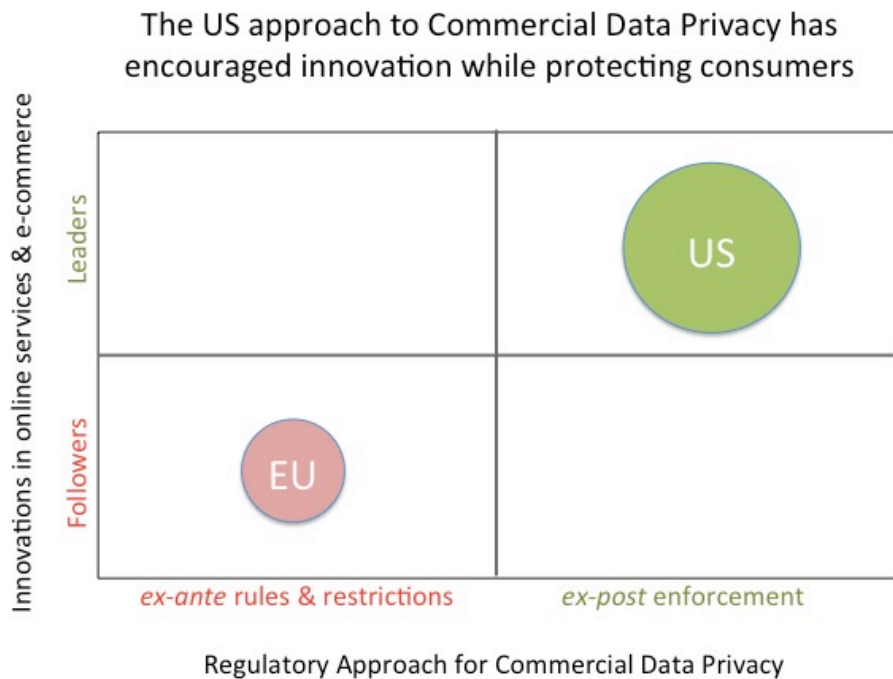
The US should lead and not necessarily follow the EU model when it comes to privacy

In large part, the success of online commerce is owed to a conscious, deliberate, hands-off policy of US policymakers. Thus far, the Federal government has allowed the Internet to develop without prescriptive regulation while still vigorously enforcing consumer protection laws and holding companies to the privacy policies and programs they have voluntarily embraced. This general application of law has helped American companies grow and create jobs.

This is not the norm in Europe, which regulates with prescriptive and restrictive rules based on fundamental privacy rights. European consumers—no matter how well-informed—cannot bargain, consent to, or otherwise waive these privacy rights. In other words, consumers have no choice to participate in the kinds of consensual data collection and use practices that are typical in the US. If applied to American companies, these European laws would restrict the breakneck innovation of the commercial web.

Legislation would necessarily either *require* or *prohibit* certain conduct. For dynamic information industries, a legislative approach is antithetical to the sort of dynamism that allows an innovator to create new ways to manage privacy or increase the efficiency of e-commerce. And, as is often the unfortunate consequence, entrenched incumbents can use existing law to delay or deter new competitors.

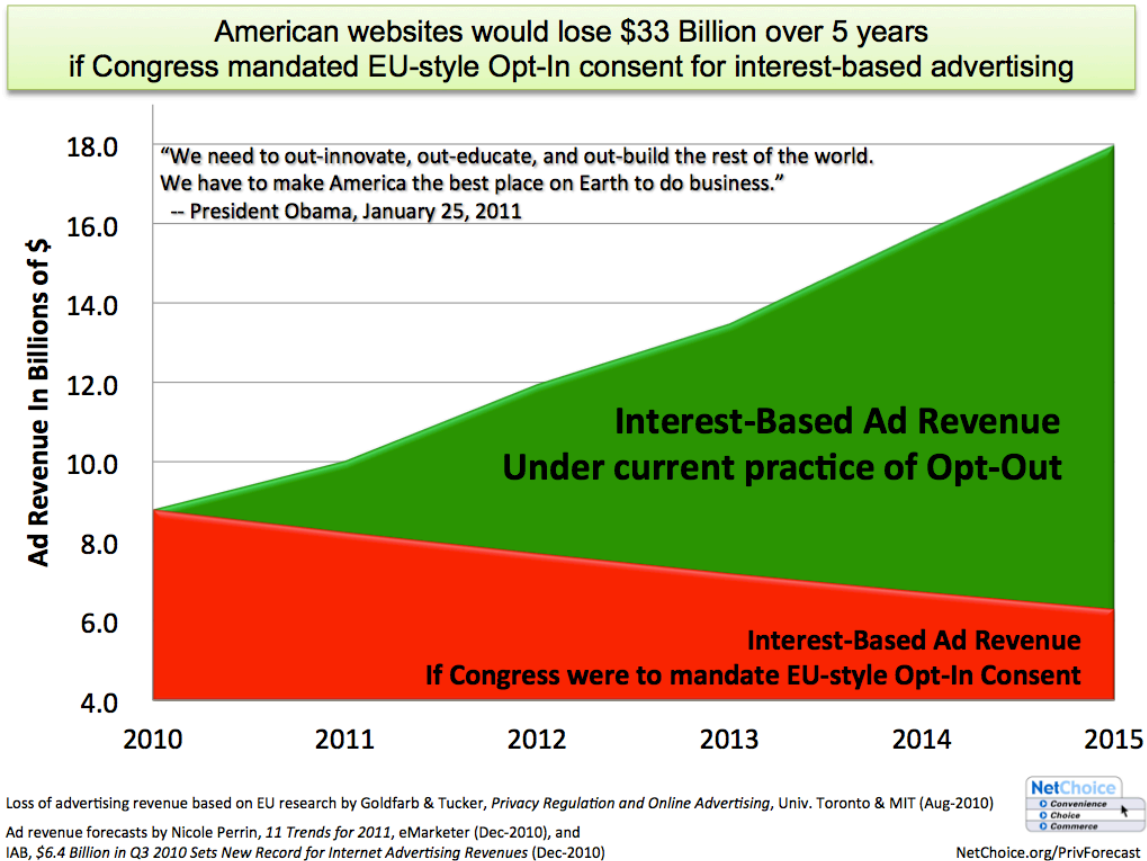
The chart below is a conceptual way to contrast the EU and US approaches to the regulation of commercial data privacy:



NetChoice supports a voluntary and dynamic program to create and enforce commercial data privacy principles. These mechanisms could encompass much of what has been proposed by the Commerce Department in its Green Paper. In addition, this would include the enforcement powers of the FTC. But the key is to retain the vibrancy of the market in policy and to enforce laws against bad actors instead of

prescribing rules covering entire industries. We note that there is a growing movement in the EU toward this sort of *ex post* enforcement and regulation of commercial data privacy.

Moreover, building off the work in a MIT-University of Toronto study,⁷ we forecast the effect of an EU-style opt-in legislation on American websites. Our forecast identified a \$33 billion loss to American websites over five years.



This Graph shows the revenue losses would have serious consequences for websites and consumers, too:

1. Websites will show more ads to make up some of the revenue loss.
2. Websites will have less to spend on content, services, and innovation.
3. Some websites will erect pay walls for content that users get for free today.

This means that, under a mandatory EU-style opt-in consent system, US consumers could end up seeing more ads, get fewer features, see less innovation, and find themselves paying for content they previously received free.

In the alternative it could result in preventing new entrants to the market.

⁷ Goldfarb & Tucker, *Privacy Regulation and Online Advertising*, Univ. Toronto & MIT (Aug. 5, 2010)

If the workshop chooses to discuss the EU style opt-in approach, we ask that the FTC also consider including a discussion of these costs to US businesses.

Conclusion

We look forward to working with the Commission as this process moves forward and welcome the opportunity to serve on a panel. Also, we welcome the opportunity to further expand upon our comments and answer any other questions that may arise.

Respectfully submitted,



Steve DelBianco
Executive Director, NetChoice



Carl M. Szabo
Policy Counsel, NetChoice

NetChoice is a coalition of leading online services and e-commerce companies, with the shared goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org