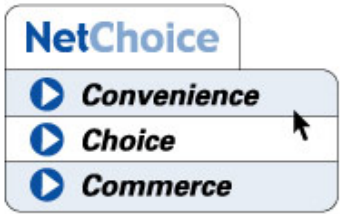


Promoting Convenience, Choice, and Commerce on the Net

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

January 28, 2011

US Department of Commerce
Office of the Secretary
In the Matter of the Request for Reply Comments on
Information Privacy and Innovation in the Internet Economy
Docket No. 101214614–0614–01

NetChoice Reply Comments on Department of Commerce Green Paper –
Commercial Data Privacy in the Internet Economy: A Dynamic Policy Framework

NetChoice welcomes this opportunity to comment on the nexus between privacy policy and innovation. In its Green Paper, the Department of Commerce rightly recognizes that Internet commerce is vital to US innovation and prosperity, and that public policies can help or harm the growth of e-commerce.

NetChoice is a coalition of trade associations and e-commerce companies, plus thousands of small businesses that rely on e-commerce. We work to promote the integrity and availability of the global Internet and is 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 specify how data can be collected, used, and shared also create barriers to legitimate online commerce.

Executive Summary

NetChoice's comments propose a role for all stakeholders—government, industry, and civil society—to improve the effectiveness and enforcement of privacy policies. Our position is that privacy is not a zero-sum game where either consumers or industry must win or lose.

Likewise, the Department of Commerce's Internet Policy Task Force Green Paper largely agrees that public polices can encourage innovation in commercial privacy as well as commercial products. Yet, the Green Paper recommends that Fair Information Practice Principles (FIPPs) be

adopted to respond to consumer privacy concerns "by filling gaps in current data privacy protections." NetChoice disagrees with this underlying premise for FIPPs and does not support statutory means to enact FIPPs.

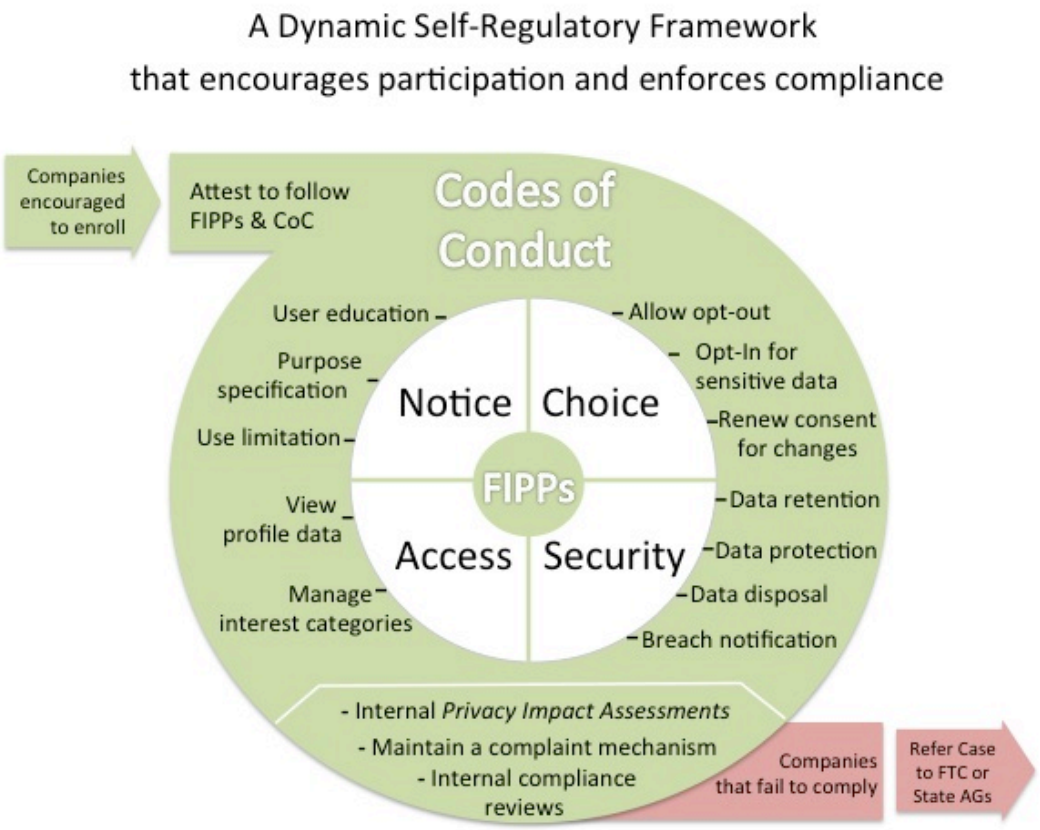
The Green Paper's assertion of "gaps" in data privacy protections implies that government must act to correct an obvious market failure. NetChoice considers this supposed "gap" to also be positive, as it is a *space for innovation*.

Still, we acknowledge that a self-regulatory framework for commercial data privacy needs to be more understandable and useful to consumers. We also recognize that more companies need to enroll in self-regulatory programs, and that more enforcement tools are needed to hold companies to keep their privacy promises.

The role for government should be in areas where users and business cannot act alone, including law enforcement, international data flows, and pre-empting a patchwork of state laws. 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.

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, FIPPs form the aspirational core that drives business conduct for data privacy. From previous work by the FTC, NAI, and IAB, we've retained the four FIPPs that we believe are the foundational principles for the collection and use of personal information: notice, choice, access, and security.

Codes of Conduct (Codes) enable implementation and enforcement of the FIPPs. 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.

Significantly, this framework does not require legislation to establish FIPPs as a matter of law.

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

> Administration encouragement for companies to adopt the self-regulatory program;
>
> Commerce Department coordination of a multi-stakeholder process to suggest Codes of Conduct for industry to consider; and
>
> FTC and state Attorneys General enforcement when companies fail to honor the principles and codes they have promised to uphold.

Turning to the issue of data breach notification, NetChoice supports preemption of state data security breach laws through legislation to create a national standard for notification rules. A national standard would promote global data portability and sends an important message to the other countries that the US is committed to data security.

Finally, NetChoice encourages Commerce, the FTC, and other regulatory bodies to defer proposals for mandating *Do Not Track* mechanisms. Time should be given for Commerce's recommended approach of a self-regulatory framework of FIPPs and Codes of Conduct.

In the balance of this reply comment, NetChoice answers the specific questions posed in the Department's Green Paper. Again, we thank the Department for this opportunity to comment.

Respectfully submitted,

Steve DelBianco, Executive Director

Braden Cox, Policy Counsel

Question 1, regarding baseline Fair Information Practice Principles (FIPPs)

NetChoice supports the notion of Fair Information Practice Principles (FIPPs). However, they should be voluntarily adopted by industry and not be creations of legislation or regulation.

As a threshold matter, we should challenge the assumption that data privacy self-regulation has failed.[1] Consumers have adopted online applications and services in unprecedented numbers when compared to previous new technologies. The Internet and the new ways people share and use information is a true American success story.

Also, at the onset, we should distinguish among the different flavors of FIPPs. Principles can be established by law or be created by standards or self-regulatory bodies. Principles can also apply to government agencies or exist to guide private commerce. The genesis and application of different FIPPs must be taken into account.

For instance, the FIPPs listed on page 26 of the Commerce Green Paper were devised for the Department of Homeland Security's collection and use of a citizen's personally identifying information (PII). These FIPPs were adopted after new laws were passed in the wake of the terrorist attacks of September 11, a time of heightened tension between security and privacy. DHS adopted its FIPPs to ensure compliance with the Privacy Act of 1974 and assuage privacy concerns of citizens.

Today, some claim there is a similar tension between online commercial data practices and the privacy concerns of consumers. But we see major differences here.

First, DHS is a government entity whose reach no citizen can choose to avoid. As an agency of government bound by the Constitution, DHS must uphold all rights and therefore should not diminish one right to enhance another. DHS appropriately acknowledges that "[t]he Privacy Office has not adopted the notion of balancing privacy against other values because that paradigm results in a zero-sum outcome and privacy often is diminished at the expense of security."[2]

On the other hand, consumers of commercial online services do have choices, and they make balancing decisions about costs, features, and privacy. And when companies fail to meet consumer expectations, we readily observe the disciplining effect of seeing customers take their business elsewhere.

That's why there is and *should be* a difference between how we view FIPPs created by government, for government—and those that would apply to commercial entities. Commercial privacy principles should not necessarily match the DHS principles cited in the Green Paper.

The Green Paper also recommends the creation of voluntary Codes of Conduct to work in conjunction with FIPPs. As a threshold matter, we are unclear about the exact relationship Commerce is suggesting between FIPPs and Codes. The Green Paper suggests that Codes are intended to "address emerging technologies and issues not covered by current application of baseline FIPPs." That would seem to imply that Codes would only apply to future innovations, and not to present practices. NetChoice believes that Codes of Conduct should apply to current issues and technologies, too.

---

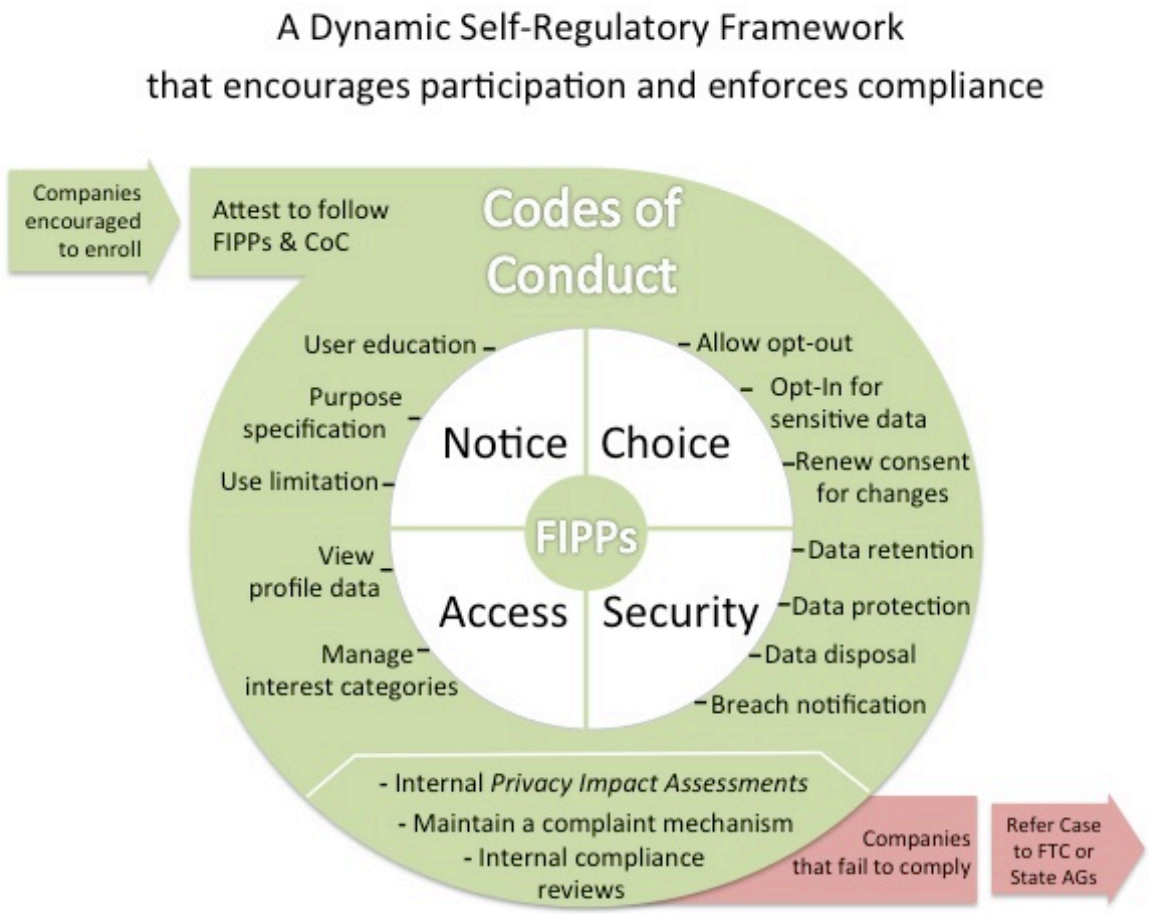
[1] FTC report—"[I]ndustry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."

[2] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf at p.2

For the past decade, the FTC has been holding companies to their privacy policies—and rightly so. But the effect has been that privacy policies have become legal documents for lawyers, not useful information for customers to make decisions. We acknowledge that our self-regulatory framework for commercial data privacy needs to be more understandable and useful to consumers. Moreover, we recognize that more companies need to enroll in self-regulatory programs, and that more enforcement tools are needed to hold companies to their policies.

We offer the following as our vision for an improved industry self-regulatory framework that would dynamically adapt to new technologies and services, encourage participation, and enhance compliance.

The diagram below captures the interaction of FIPPs and Codes and emphasizes Administration support on the front-end as well as FTC enforcement on the back-end:



As envisioned above, FIPPs form the aspirational core that drives business conduct for data privacy. From previous FTC, NAI, and IAB efforts, we've retained the four FIPPs that we believe are the foundational principles for the collection and use of user personal information: notice, choice, access, and security.

The Codes of Conduct are there to enable companies and consumers to implement the FIPPs in their websites and services. The Administration could help drive the development of Codes through encouragement and expert advice.

Participating companies would publicly attest to their commitment to implement the Codes within their business operations and perform periodic reviews to ensure compliance. If a company failed to comply with the adopted Codes, existing laws allow FTC and state Attorneys General to bring enforcement actions (as we discuss in response to Question 3).

While our framework calls for continued industry self-regulation, it relies on government in three critical ways:

1. Administration support on the front-end to encourage companies to adopt and attest to the self-regulatory program;

2. Commerce Department coordination of multi-stakeholder processes to suggest Codes of Conduct for industry to consider; and

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

1(a) Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or through other formal means to address how current privacy law is enforced?

The Green Paper recommends that Fair Information Practice Principles (FIPPs) be adopted to respond to consumer privacy concerns "by filling gaps in current data privacy protections." NetChoice disagrees with this underlying premise for FIPPs and does not support statutory means to mandate FIPPs.

The Green Paper's assertion of "gaps" in data privacy protections implies a negative—and suggests that government must act to correct an obvious market failure. But NetChoice believes that this supposed "gap" is also positive space, since it has become a *space for innovation*.

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.

But it doesn't have to be this way. If prescriptive privacy laws had been in place, they might have prevented many recent innovations in online services. In previous comments, Facebook described how some of its "most popular innovations were initially met with skepticism from privacy advocates and others. For example, Facebook's *News Feed* faced significant controversy when it was first released in 2006."[3]

Facebook is just one of many proof points for why the appropriate measure of success for self-regulation is not the quantity of rules, but the balance between effective regulation and innovation. The US is the world leader in Internet innovation. Here, there is an ongoing and vibrant movement for self-regulation that will provide enhanced transparency and user controls for data collection and use.

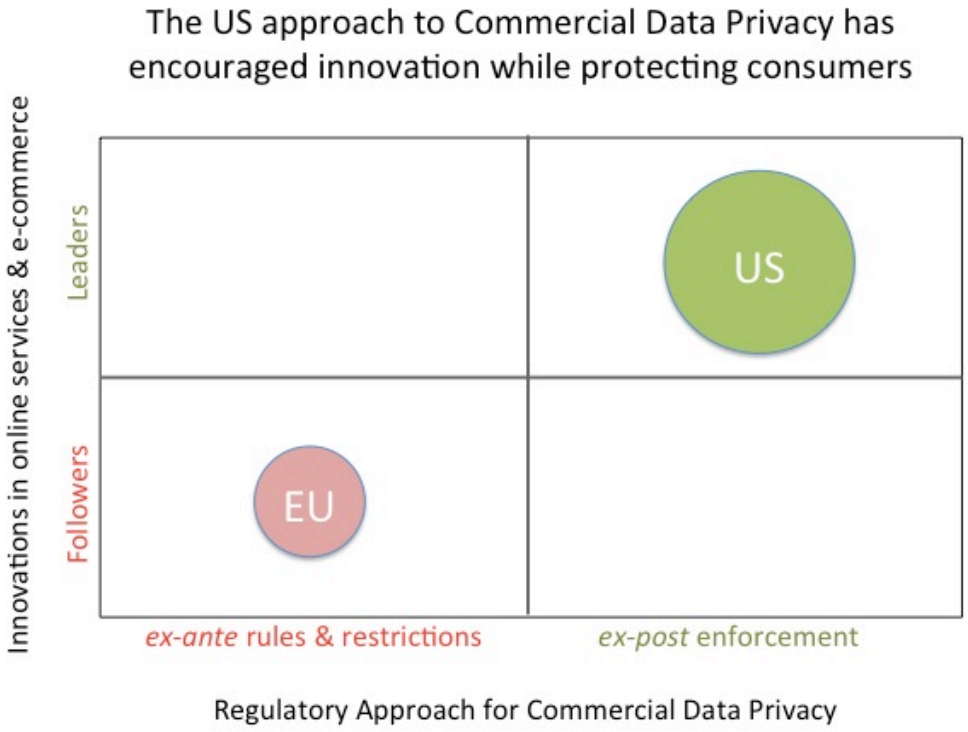
This is not the norm in Europe, which regulates with prescriptive and restrictive rules based on fundamental privacy rights. European consumers—no matter how well-informed—cannot bargain, consent to, or otherwise waive these privacy rights. In other words, consumers have no

[3] http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Facebook%20Inc%20Comments.pdf

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 Commerce 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.

1(b) How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions?

Baseline privacy principles are best enforced by informed consumers in a competitive marketplace. Online companies are working on robust mechanisms for monitoring, correcting, and disciplining unwelcome practices. Non-governmental self-regulatory bodies could monitor

how well these companies are following the FIPPs and Codes. The results of their monitoring can help companies improve compliance. And if companies fail to comply with the program they've committed to, non-governmental organizations (NGOs) can forward their findings to the FTC and state AGs to undertake enforcement actions against those companies

As noted in our recommended program, there *should* be a government enforcement role. It should be centered on our fundamental consumer protection statute—the FTC Act—which empowers the FTC and most state AGs to prosecute unfair or deceptive trade practices.

Companies should be encouraged to adopt the FIPPs and Codes so that the FTC and State AGs can hold them accountable. Public attestations for FIPPs and Codes would form the basis of FTC enforcement actions. A company's failure to honor its adopted Codes could trigger a Section 5 action, just as the FTC and state AGs currently treat breaches of privacy policies as a deceptive trade practice.

Current self-regulatory processes have already contemplated how companies would be referred to the FTC for enforcement actions. For example, the *Self-Regulatory Principles for Online Behavioral Advertising*—developed by the Interactive Advertising Bureau (IAB), Direct Marketing Association, and other business associations—describes an accountability principle with three components:[4]

> *Monitoring* — Programs will systematically or randomly monitor the Internet for compliance with the Principles. Programs will maintain a process for taking complaints from the public, from competitors, and from government agencies concerning possible non-compliance with the Principles.
>
> *Transparency and Reporting* — Program findings of non-compliance (in particular those that are not corrected), the reasons for those findings, and any actions taken with respect to instances of non-compliance will be publicly reported by the programs.
>
> *Compliance* — When an entity engaged in Online Behavioral Advertising is informed by a program regarding its non-compliance with the Principles, the entity should take steps to bring its activities into compliance with the Principles. The programs will send the public reports of uncorrected violations (set forth in (2)) to the appropriate government agencies.

As another example, the NAI principles suggest that NAI will refer cases to the FTC:

> These policies and procedures shall not only describe the process undertaken for a compliance review, but shall also articulate the penalties that could be imposed for a finding of non-compliance, including referral of the matter to the US Federal Trade Commission.[5]

Moreover, NAI has procedures for increasing transparency and exposing noncompliant companies. Part (e) of its principles states that "*an annual summary relating to consumer complaints received, and any enforcement actions taken, shall be made available on the NAI website*."[6]

---

[4] http://www.iab.net/media/file/ven-principles-07-01-09.pdf

[5] www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf

[6] NAI princples, p. 12, at hwww.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf

The above shows that self-regulatory bodies are an important part of enforcement, holding member companies accountable when they fail to abide by adopted industry codes of conduct.

1(c) As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rules? What criteria are useful for deciding which FIPPs require further specification through rulemaking under the Administrative Procedure Act?

The Green Paper leaves open for further comment whether the FTC needs enhanced (APA) rulemaking authority in the privacy area. NetChoice opposes giving the FTC blanket, no-holds-barred APA authority, particularly for an issue as broad as commercial data privacy.

As noted in our answer to Question 1, NetChoice does not see a need for legislation or for FTC rulemaking at this point.

1(d) Should baseline commercial data privacy legislation include a private right of action?

Injured persons can sue companies for actual damages arising from negligence or misuse of personal information. But neither Congress nor state governments should create a new private right of action that specifies statutory dollar damages or invites class action suits that would encourage endless litigation.

To authorize lawsuits where there is no evidence of harm is to invite the plaintiff's bar to sue legitimate companies over minor technical violations, knowing that companies will settle to avoid negative publicity. This threat of litigation would chill the release of new products, delay the implementation of new features, and reduce entrepreneurial risk-taking.

Question 2, regarding prioritizing and promoting FIPPs

The task force specifies three principles that it says are a "high priority" to provide greater substantive protections and meet the challenges of today's information-intensive marketplace: 1) enhancing transparency; 2) encouraging greater detail through purpose specifications and use limitations; and 3) evaluation and accountability programs.

NetChoice will address each of these priority FIPPs below.

Enhancing Transparency and Notice

NetChoice supports increased transparency to better inform customers about why their data is collected and how it will be used. We welcome a shift away from relying on extensive, legalistic privacy policies as the primary way to convey information to our customers. But before online companies can comfortably use "enhanced notice" mechanisms, we need assurances from the FTC about its enforcement expectations.

For the past decade, the FTC has been holding companies to their privacy policies—and rightly so. But the effect has been that privacy policies have become legal documents for lawyers, not information documents for customers. Moving toward enhanced transparency means more

reliance on just-in-time notices that—for clarity and space considerations—will not contain every legal or technical nuance. Advice from Commerce and the FTC would be helpful in defining Codes of Conduct.

Privacy Impact Assessments (PIAs)

In addition, the Commerce Green Paper discusses enhancing transparency through privacy impact assessments (PIAs). Presumably these reports would be a voluntary self-assessment, but the Green Paper cites commenters who advocate that impact assessments be made public.[7]

If PIAs were required to be made public in advance of introducing new features or services, this country would effectively be requiring a 'permission slip' for innovation. Public debate over PIAs could be costly and burdensome, especially for smaller companies. If required to be submitted to government or made public, the result would be over-inflation of risks, much like what occurs in SEC filings.

Publishing PIAs would therefore needlessly inflate privacy fears, be exaggerated by pro-regulatory privacy groups, and be hijacked by plaintiff's lawyers.

We believe that requiring published PIAs in the US environment is premature. Many—if not most—companies already assess the privacy implications of new applications and services, in accordance with "privacy by design" considerations. But these are voluntary efforts. In addition, with so many business models, PIAs would be very difficult to standardize—both from a company perspective, but also as a basis for government enforcement.

Indeed, the Green Paper highlights how PIAs might operate by referencing the European RFID PIA (FN 108).[8] Page 3 of the referenced document further describes the European approach and the highly public and sensitive nature of PIAs:

> Mechanisms for reporting PIAs to the competent authorities need to be proportionate and operationally efficient, in particular for those types of RFID Supply Chain Systems and Applications which by their nature strictly operate in business to business environments and do not implicate privacy. The high volume of PIA reports of Supply Chain Systems and Applications might undermine the capacity of the competent data protection authorities to review the PIAs of RFID Applications that do implicate privacy.

The European approach anticipates reporting PIAs to authorities for their review. In the US, the mantra of transparency and mult-stakeholderism will likely mean that these PIAs will be made available—if not explicitly, then through the Freedom of Information Act—for public review, too. That includes privacy advocates who might seek to modify or block an innovation. And competitors will have access to the PIA, giving them insights into innovations planned by a present or potential competitor.

Finally, we note that PIAs are not needed as a basis for FTC enforcement authority. Section 5 of the FTC Act provides the FTC with broad powers to target unfair or deceptive trade practices.

Purpose Specifications and Use Limitations

The Green Paper recommends that companies align their information practices with consumer expectations through a policy of purpose specification and use limitation. This would require

---

[7] Dynamic Privacy Framework report at 35.

[8] http://ec.europa.eu/information_society/policy/rfid/documents/d31031industrypia.pdf

data collectors to specify all the reasons for collecting personal information and then specify limits on the use of that information. NetChoice supports this approach only if it heeds the Green Paper's overall dynamic framework theme—to keep these specifications sufficiently high-level as to be adaptable for all business models.

NetChoice members continuously innovate to implement clear and understandable privacy policies. Part of this approach is to tell users what information is collected and how it will be used. This includes the appropriately named *Self-Regulatory Program for Online Advertising*.[9] Central to this program is the Advertising Option Icon, which allows consumers to understand why it is they received certain targeted ads and to opt-out of future ad targeting. It's a just-in-time approach; the kind of teachable moments that will truly educate and inform users about the meaning behind the choice.

But there is a flipside problem with purpose specificity. If too specific, data collection and use purposes will become a laundry list of uses put forth to satisfy regulators – not consumers. There's nothing dynamic about a delineated list of purposes and uses. We want to avoid consumer confusion through a parade of intended and potential uses, and avoid strict limits that prevent the future use of data in consumer welfare-enhancing ways.

How do we maintain dynamism when specifying collection purposes and data use limits? One possible approach is to create different classification categories for how data will be used, and specify limits depending on which category bucket personal information falls into. In its comments, Microsoft describes such a system:

> The premise of the "use and obligations" model is that the decision to use information creates legal obligations on the organization that uses the information. At a practical level, such a system may classify uses based on standard use categories. These categories might include: (A) fulfillment; (B) internal business processes; (C) marketing and selling of products and service; (D) fraud prevention and authentication; (E) research; and (F) public purposes. Irrespective of where data was collected or by whom, the obligations related to the use categories must be honored.[10]

A category approach could preserve flexibility, allowing companies to categorize data according to their business practices. NetChoice envisions that there could be more creative solutions that would come out of an open, multi-stakeholder process.

Evaluation and Accountability Programs

Finally, the Commerce Department Green Paper recommends evaluation and accountability as means to ensure the effectiveness of commercial data privacy protections. Central to this concept are audits for how well companies follow their own purpose and use specifications.

NetChoice supports the notion of internal audits but strongly opposes requiring external audits if performed by third parties. It's not difficult to imagine how the depth and breadth of these audits would expose sensitive proprietary information, particularly for Privacy Impact Assessments.

---

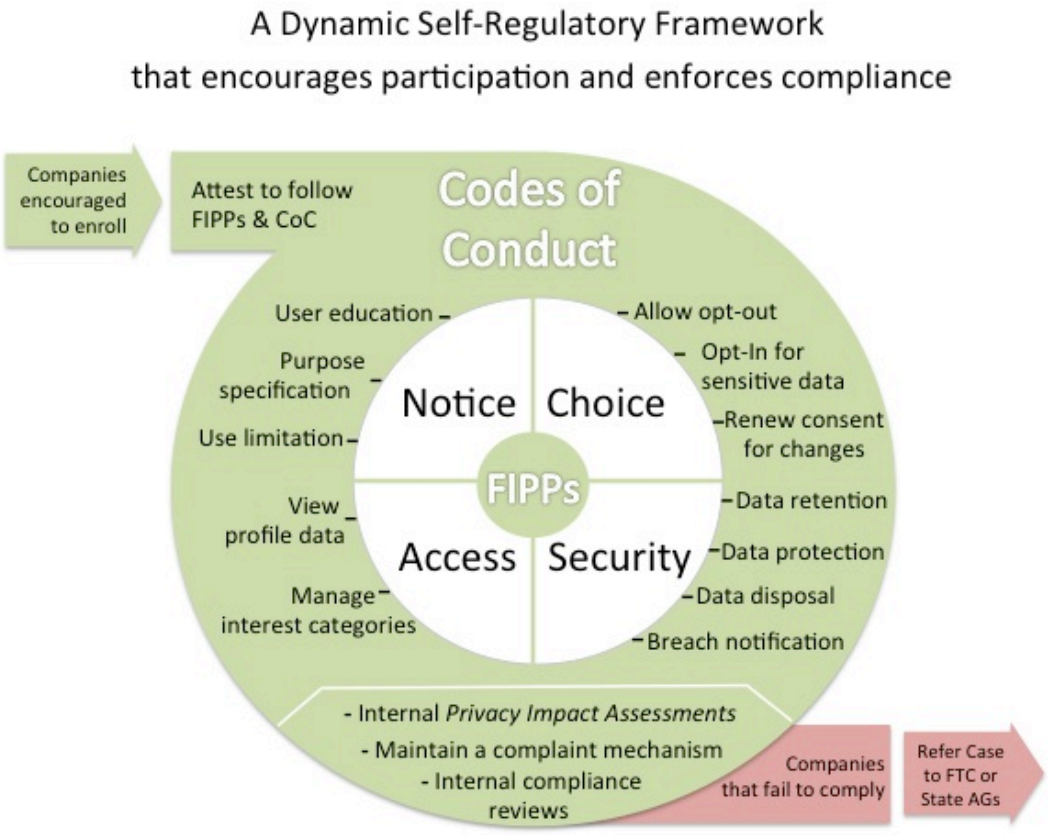
[9] http://www.aboutads.info/

[10] Microsoft comments at 4. http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Microsoft%20Comments%2Epdf

Question 3, regarding FTC-Approved Codes of Conduct

Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support; (b) stepped up enforcement; and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

As previously discussed, we believe an improved industry self-regulatory framework would encourage participation and enforce compliance (conceptual overview repeated here for convenience).



In this framework, Codes of Conduct (Codes) are the operational mechanisms for achieving each of the FIPPs principles. The Codes are also where companies, consumers, policymakers, and the FTC can measure compliance.

Participating companies would publicly attest to follow the Codes. Companies would have flexibility to implement Codes in ways that are tailored to their business operations—some Codes might be relevant, but others might not apply. For instance, interest category management would not be needed on a site where consumers voluntarily post their information onto profile pages, because users can already manage the data on which ads are targeted.

Failure to comply with the Codes would be the basis of a Section 5 complaint, just as the FTC currently enforces breaches of privacy policies as deceptive trade practices. The FTC could also refer cases to state Attorneys General for specific enforcement actions. In some states, AGs may have authority under their state consumer protection laws to pursue violations of publicly attested Codes. .

3(a) public statements of Administration support

We believe that public statements of Administration support are vital for "buy-in" from various stakeholders, including industry, NGOs, and users. There is definitely a role for the Commerce Department to initiate and convene multi-stakeholder processes through a Privacy Policy Office.

3(b) stepped up enforcement

NetChoice has been a consistent proponent of increased FTC enforcement efforts. The FTC already has Section 5 authority to hold companies to the terms of their stated privacy policies. We support similar efforts for FTC enforcement if and when companies who adopt the FIPPs and Codes framework have failed to comply.

3(c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

NetChoice does not support legislation that regulates data privacy or creates private rights of action, and then offers safe harbors from that legislation or litigation. We believe it is much better to have industry participation on the front-end, placing the carrot before the stick.

However, NetChoice does support legislation that would create a national standard for data security breach notifications. Please see our comments on Question 7 below.

Question 4, regarding Commerce Department establishing a Privacy Policy Office

NetChoice supports the creation of a Privacy Policy Office (PPO) that will be an advocate for online business. The office would be a coordinator of voluntary Codes of Conduct and a vital ambassador for online companies doing business overseas, but it should not be a regulator in disguise, advocating for legislation or regulation.

We encourage further involvement by the Department to ensure that public policies related to consumer privacy—both here in the US and abroad—are flexible enough to allow the innovation we all want to see. Now is a critical time for online commerce as international policymakers assess their approaches to privacy. The Department can play an important role as an advocate for flexible national and international rules to promote continued innovation and economic growth.

The Department already has an excellent track record in a number of international fora. ITA currently administers the US-EU Safe Harbor Framework and has worked with the Asia Pacific Economic Cooperation (APEC) member countries to develop a privacy framework. Both are

successful efforts to mutually recognize different compliance laws and allow for innovation across borders.

The PPO could promote privacy laws that are flexible enough to permit innovation and oppose static laws that undermine consumer interests in improved online services. The PPO could also bring international credibility and leverage that cannot be matched by corporate interests alone.

4(a) Should the FTC be given rulemaking authority triggered by failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified time period?

No, the FTC should not be given rulemaking authority to create privacy regulations. For the process to remain innovation-driven and truly a Code of Conduct, there cannot be a looming threat of FTC rulemaking – particularly if the FTC is allowed to use the relatively relaxed APA process.

Instead, the Code of Conduct itself should afford NGOs and other affected participants the ability to press for FTC and state AG enforcement. Such mechanisms as complaints and audits allow dissenting voices to be heard, particularly if it involves a company-specific failure to adhere to a particular Code of Conduct.

4(b) How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?

We would ask that the Commerce Department advocate on behalf of online companies and insist that developments of any *Do Not Track* proposal do not block legitimate business and marketing operations.

Do Not Track mechanisms are described in the FTC's privacy report from December 2010. The FTC calls for a "uniform and comprehensive" way for consumers to decide whether they want their activities tracked.[11] The Commission points to a *Do Not Track* system consisting of browser settings that would be respected by web tracking services. A user could select one setting in Firefox, for example, to opt out of all tracking online. We think that the FTC wrongly calls this "universal choice."

Instead, it's a universal *response*. It's a single response to an overly-simplified set of choices we encounter on the web. This single response means that tracking for the purpose of tailored advertising is either "on" or "off." There is no proposal to allow consumers to opt back "in" for trusted sites and services. But it is the comfortable "middle" where we want consumers to be—an educated setting where consumers understand the tradeoffs of interest-based advertising. In return for tracking your preferences and using them to target ads to you, you get free content/services.

But an on/off switch for interest-based advertising is too blunt an instrument. There is no incentive for consumers to learn about the positives; they'll opt-out because simply because they fear a worst-case scenario. In return, they'll also opt-out of the benefits of targeting and tracking.

[11] http://ftc.gov/os/2010/12/101201privacyreport.pdf

As Fred Wilson described in a recent New York Times debate,

> "[t]racking is the technology behind some of the most powerful personalization technologies on the Web. A Web without tracking technology would be so much worse for users and consumers."[12]

At the very least, NetChoice encourages Commerce to insist that *Do Not Track* proposals not interfere with the operational purposes of legitimate websites whose sole purpose is marketing and advertising.

Prior legislative proposals have introduced the concept of an "Operational Purpose" to exempt the need to obtain express consumer consent for the collection of covered personal information.[13] However, the exemption was too narrow—it would not permit use of covered personal information for "marketing or advertising purposes, or any use of or disclosure of covered information to a third party for such purposes."[14] The result would be that any data collected or used to serve ads more effectively would require opt-in consent from every user, even if it is directly in service of the operational purpose of the website.

Ideally, NetChoice encourages Commerce, the FTC, and other regulatory bodies to defer proposals for mandating *Do Not Track* mechanisms. Instead, Commerce's Green Paper relies on Codes of Conduct on which to gauge company performance with consumer preferences. The Code of Conduct approach is granular, while *Do Not Track* is broad and blunt instrument of user control. Moreover, Codes can be tailored to a wider range of possible uses of personal information beyond the collection and serving of ads.

4(c) Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by a multi-stakeholder process to produce an approved code of conduct?

NetChoice believes that the multi-stakeholder process should be led by industry participants who would be the primary adopter of a framework of FIPPs and Codes. Therefore, the process would have inherent incentives to succeed. However, we admit that "success" is in the eye of the beholder, and some stakeholders will not be happy with the overall product. But "failure" is also in the eye of the beholder. That's why all stakeholders should view the Codes process as dynamic and continuously evolving. Success or failure will be a healthy debate that can be managed by the PPO without calls for regulation or legislation. NGOs can still file complaints with the FTC and encourage investigations when enrolled companies fail to honor the Codes of Conduct they have publicly adopted.

---

[12] http://www.nytimes.com/roomfordebate/2010/12/02/a-do-not-call-registry-for-the-web/tracking-personalizes-the-web

[13] Rush bill; "Operational purpose" exception to express consent for customer service, security, business functions, IP rights, safety, and law enforcement. Also Boucher/Stearns

[14] Rush bill, avail at http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111UnXKfn

4(d) How can cooperation be fostered between the National Association of Attorneys General, or similar entities, and the PPO?

State AGs could work hand-in-hand with the FTC to enforce the Codes. The FTC could refer cases to AGs, or AGs could independently litigate violations pursuant to their state's consumer protection statutes, commonly known as "mini-FTC" acts.

Question 5, regarding role of FTC as Lead Enforcement Agency

5(a) Do FIPPs require further regulatory elaboration to enforce, or are they sufficient?

FIPPs and Codes of Conduct in a self-regulatory framework would be subject to FTC enforcement if companies fail to honor a Code of Conduct they have voluntarily adopted and publicly embraced.

5(b) What should be the scope of FTC rulemaking authority?

The current process through which the FTC makes rules, as established by the Magnuson-Moss Act, is the appropriate process for creating new regulations on general business activity.

However, as noted earlier, we believe that the FTC's current authority under Section 5 grants the necessary enforcement powers to punish businesses that act in a deceptive manner or in ways that are unfair to the consumer.

5(c) Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigations still be conducted under FTC Act Section 5 "unfair and deceptive" jurisdiction, buttressed by the explicit articulation of the FIPPs?

FIPPs should not be considered an independent basis for FTC enforcement. As previously described, a voluntary framework of FIPPs and Codes should provide the FTC and state AGs adequate basis to hold enrolled companies accountable to honor the adopted Codes of Conduct.

5(d) Should non-governmental entities supplement FTC enforcement of voluntary codes?

NGOs should be able to file complaints with the FTC and state AGs to encourage investigations of companies who fail to follow their adopted Codes of Conduct.

5(e) At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante "seal of approval," delaying approval until the code is in use for a specific amount of time, and delaying approval until enforcement action is taken against the code.

The FTC should not be able to "approve" voluntary Codes of Conduct. The FTC is the lead consumer enforcement agency, but this does not translate to prior approval of or restraints on business conduct.

However, the FTC has gained considerable expertise through its many public comment periods and privacy roundtables, and its input would be valuable and welcomed.

5(f) What steps or conditions are necessary to make a company's commitment to follow a code of conduct enforceable?

Companies need to attest to the FIPPs and Codes in their Terms of Service or Privacy Policy in order for the FTC to have Section 5 enforcement authority. Part of the attestation process might include a seal that would be displayed on the website indicating adherence to the FIPPs and Codes.

Question 7, regarding Comprehensive Commercial Data Security Breach Framework

7(a) What factors should breach notification be predicated upon?

NetChoice supports a national framework for data security breach notifications. A national framework will promote global data portability and sends an important message to the other countries that their information is safe and secure. Accomplishing this national framework requires preemption of state data security breach laws.

A federal bill would in many ways borrow from the elements of existing state laws. Current laws seek to avoid over-burdening companies and desensitizing consumers through over-notification, while notifying consumers when their sensitive information is actually at risk. Thus, these rules are based on risk assessment and potential harm. Federal breach notification legislation should therefore be premised upon:

a) unauthorized acquisition of

b) unencrypted and unredacted personal information that

c) creates a significant risk of identity theft, fraud, or other economic or physical harm to an individual.

Question 9, regarding States' role in a National Privacy Framework

9(a) Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

As a threshold matter, NetChoice does not support national data privacy legislation at this time. In this reply comment we have recommended an enhanced self-regulation program, backed by FTC and state Attorneys General enforcement to hold companies to the Codes of Conduct they have adopted.

However, *if* federal privacy legislation were to be considered, it should include a preemption provision that sets both a floor and ceiling on state regulation.

9(b) How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are useful criteria for comparatively assessing how protective different laws are?

As a threshold matter, NetChoice does not support national data privacy legislation at this time. In this reply comment we have recommended an enhanced self-regulation program, backed by FTC and state Attorneys General enforcement to hold companies to the Codes of Conduct they have adopted.

However, *if* federal privacy legislation were to be considered, it should include a preemption provision that sets both a floor and ceiling on state regulation.

With respect to data security breach notification, NetChoice does support federal legislation that preempts state laws in this regard. For a data security breach law, comparison criteria would include a) who has a duty to notify, b) what is a security breach, c) the definition of personal information, d) who must be notified, and e) how must notification be accomplished.

9(c) To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation?

As a threshold matter, NetChoice does not support national data privacy legislation at this time. In this reply comment we have recommended an enhanced self-regulation program, backed by FTC and state Attorneys General enforcement to hold companies to the Codes of Conduct they have adopted.

However, it is critical to note that state Attorneys General already have authority to enforce self-regulatory frameworks, by holding companies to the policies and codes of conduct they have professed to follow. First, state AGs can work hand-in-hand with the FTC in its enforcement proceedings. Second, the FTC can refer cases to AGs. And finally, state AGs can independently litigate violations pursuant to their state's consumer protection statutes, commonly known as "mini-FTC" acts.

However, we do not favor letting Attorneys General outsource enforcement to the plaintiff's bar, as private attorneys have different incentives to litigate and do not consider cost-benefit public policy analysis.

Additionally, we do not support private rights of action, which would have a deleterious effect on a consistent, national privacy framework. Private litigation creates case law that often differs among the circuit courts. While this is acceptable and even beneficial for some areas of the law, it would create a patchwork of law that would impede national data flows. Moreover, it would inevitably lead to forum shopping. The result would be an inconsistent application of federal law, chipping away at Congressional intent to provide a uniform national framework that fosters the growth of the US technology sector and future innovation.

9(d) Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

As a threshold matter, NetChoice does not support national data privacy legislation at this time. In this reply comment we have recommended an enhanced self-regulation program, backed by

FTC and state Attorneys General enforcement to hold companies to the Codes of Conduct they have adopted.

As noted above, state Attorneys General already have authority to enforce their own consumer protection statutes (usually based on Section 5 of the FTC Act) in order to hold companies accountable to their stated privacy polices.

Question 10, regarding ECPA

NetChoice supports ECPA reform. The Electronic Communications Privacy Act (ECPA) is outdated and reform should clarify the roles of online companies when responding to law enforcement requests.

Increasingly, online companies are called into action by federal, state, and local law enforcement to provide information on their customers. In the first half of 2010, Google counted more than 4,200 requests for customer data from law enforcement in the United States.[15] Facebook reportedly responded to over 7,000 requests in 2009.[16]

The text of ECPA refers to "communications" but there's so much more to what we store online than email. An immense amount of personal information exists online. Back in 1986 when ECPA was passed, it was mostly email that was the privacy concern. Today there are tweets, friend updates, photo comments, status changes, and online storage of not just emails, but photos, videos, and documents. We also leave traceable trails online—the websites we've visited, the search terms we've used. All of this is highly personal and often meant to be private. So there's a gap in what's protected. There's also some arbitrary distinctions made with email.

ECPA today extends greater privacy protections to emails stored for less than 180 days than emails stored for more than 180 days. These distinctions might have made some sense in 1986, when email services did not automatically retain messages for long periods of time. But that distinction no longer bears any relationship to reality—hosted email and other online services almost invariably store emails and other content for years, and users reasonably expect these communications to remain just as private on day 181 as on day 179. An update to ECPA would give our customers the confidence that the use of our online services would not require sacrificing their privacy.

For these reasons, ECPA must be modernized to establish consistent, predictable privacy protections that are technologically neutral. An ECPA update can be done in ways that address not just the goals of privacy and law enforcement, but also to advance the development and use of new technologies.

---

[15] http://www.google.com/transparencyreport/governmentrequests/

[16] http://www.nytimes.com/2011/01/10/technology/10privacy.html?emc=eta1