



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

February 18, 2011

US Federal Trade Commission
In the Matter of Questions for Comment on Proposed Framework
Protecting Consumer Privacy in an Era of Rapid Change

**NetChoice Reply Comments on Preliminary FTC Staff Report –
*Protecting Consumer Privacy in an Era of Rapid Change:
A Proposed Framework for Business and Policymakers***

NetChoice welcomes this opportunity to comment on the nexus between privacy policy and innovation.

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 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. Today, NetChoice is concerned that privacy-related regulation that overly restricts collection and use of data could also create barriers to legitimate online commerce.

Executive Summary

As a threshold matter, we see no evidence for the report’s assertion that data privacy self-regulation has failed.¹ Moreover, we respectfully disagree with the Chairman’s proclamation that “self-regulation of privacy **has not** worked adequately and **is not** working adequately for American consumers.”² The tone of the Commission’s report and the Chairman’s remarks do not square with the evident reality of today’s online marketplace. Judging by their comments attached to the report, at least two Commissioners share our doubts about the failure of self-regulation.

Consumers have adopted online applications and services at an unprecedented rate when compared to previous new technologies. Last year’s holiday season saw a 12% increase in online retail sales, with consumers spending more than \$32 billion online.³ Consumers rated their online shopping experience at the highest level since 2001.⁴ Perhaps most informative, research shows that advertising

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.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf> (emphasis added).

³ As seen in the comScore report earlier this year.

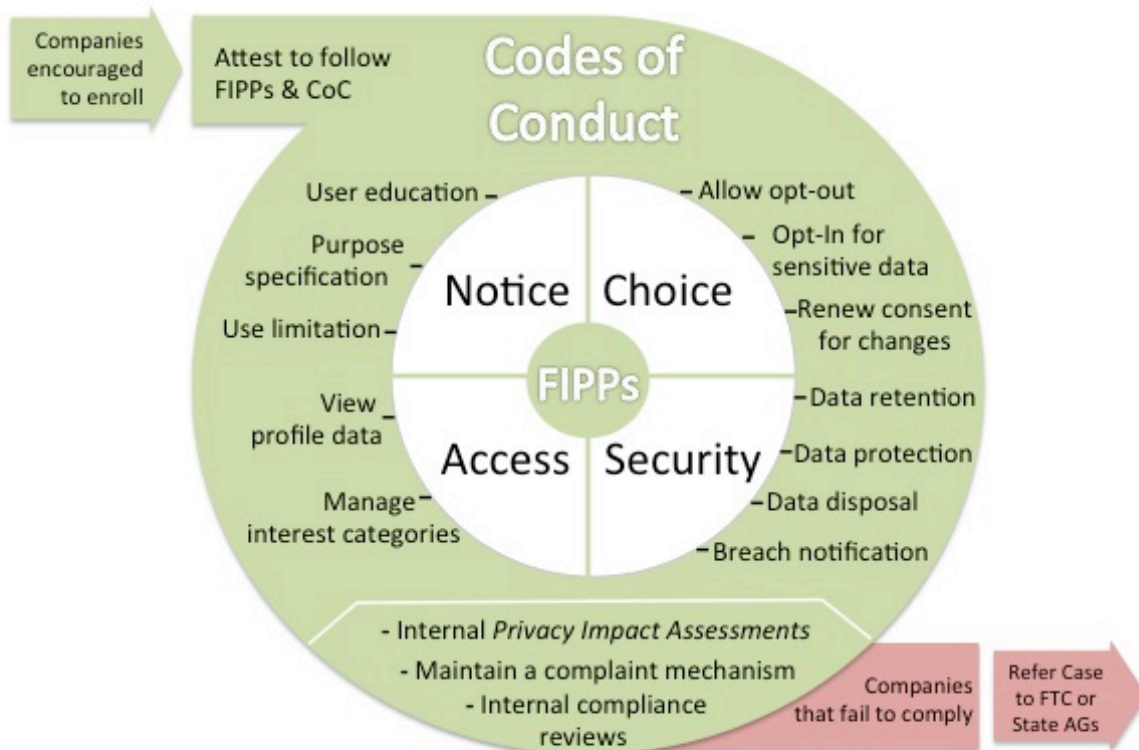
⁴ ForeSee Results’ E-Retail Satisfaction Index

and marketing practices are not making consumers more reluctant to go online. And of those consumers who *were* reluctant to shop online, just 0.1% cited concerns over privacy.⁵

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 Fair Information Practice Principles (FIPPs) and Codes of Conduct, while continuing to rely on the FTC for enforcement:

A Dynamic Self-Regulatory Framework that encourages participation and enforces compliance



As envisioned above, FIPPs form the aspirational core that drives business conduct for data privacy. We’ve embraced the four foundational principles advanced by the Commission for the collection and use of user personal information: notice, choice, access, and security.⁶

⁵ 2009 survey by the National Retail Association

⁶ FTC Report, p.6.

Codes of Conduct are there to enable companies and consumers to implement FIPPs in their online services. The Administration could encourage and guide the development of Codes. With its authority to regulate unfair and deceptive practices, the FTC could encourage adoption by following up on Commissioner Rosch's belief that companies who don't adopt a privacy policy invite Section 5 liability "in that it would entail a failure to disclose material facts."⁷

Participating companies would publicly attest to their commitment to implement the Codes and perform periodic reviews to ensure compliance. If a company failed to comply with its adopted Codes, existing laws empower the FTC and state Attorneys General to bring enforcement actions.

Our framework calls for continued industry self-regulation and relies on government in three ways:

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

Commerce Department and FTC coordination of multi-stakeholder processes to suggest Codes of Conduct for industry to use when implementing principles; and

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

Finally, Chairman Leibowitz asks a provocative question to "professional naysayers" as a last point in his remarks to the report: "What are you for? Because it can't be the status quo on privacy."

But the Chairman's challenge presumes that the state of online privacy is now static, whereas there is unquestionable progress in terms of user awareness and empowerment. Moreover, the Chairman declares that this status quo is unacceptable, whereas consumers are embracing free online services at unprecedented rates of adoption without any apparent harm. Stronger evidence than presented here should be required before regulators ruin an evolving ecosystem of advertising-supported online services that employs over three million Americans and delivers value to nearly all of us⁸.

When asked what we are for, our answer is, continued industry self-regulation and increased enforcement of existing laws that prohibit unfair and deceptive practices.

In the balance of this reply comment, NetChoice answers selected questions posed in the Commission's report. Again, we thank the Commission for this opportunity to comment.

Respectfully submitted,

Steve DelBianco, Executive Director

Carl Szabo, Policy Counsel

⁷ FTC Report – Concurring Statement of Commissioner J. Thomas Rosch, page E-1.

⁸ Department of Commerce Intern Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 2010).

A. Scope of Proposed Framework

Our framework applies in all situations: when users view a site and provide personal information, and when websites collect data, including personal information. But the collection of data and the linking with personal information are two separate concerns and the Commission should view them as such.

We often hear from pro-regulatory privacy advocates that IP addresses and location data are personally-identifiable information (PII) because they can be merged with other data that will identify individuals. But for purposes of a privacy framework, we should differentiate between what data *can* be linked and what data actually *is* combines to identify a person. Rules—including data security safeguarding and notifications—should apply differently when data has been merged to identify a person.

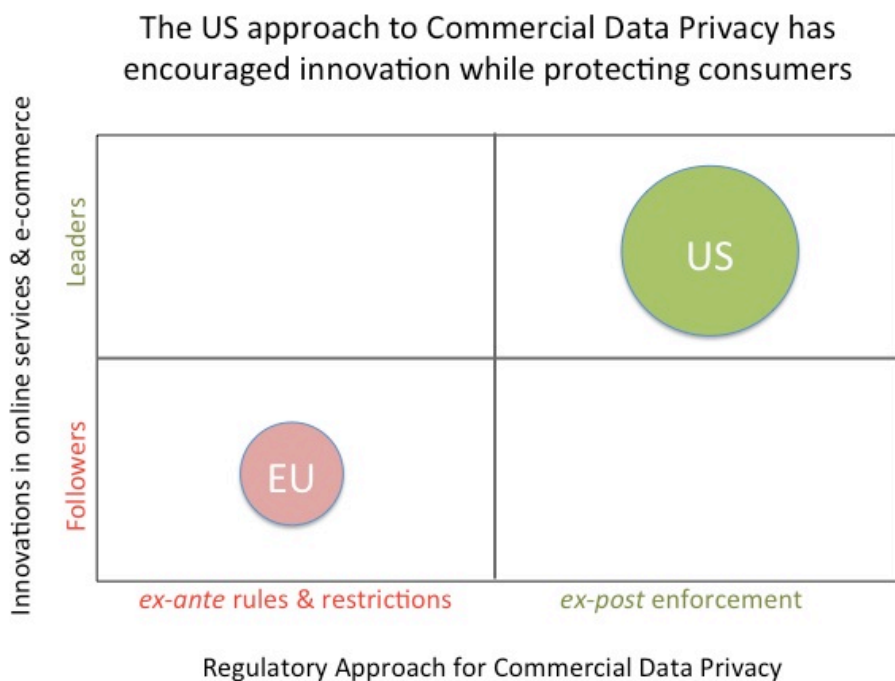
For instance, IP addresses alone cannot be considered personally identifiable information. To be personally identifiable, it must identify a person. An IP address identifies a computer. It does not identify users because the addresses don't include people's names or addresses.

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.

- *Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?*

We believe that a flexible and scalable self-regulatory framework can be adapted to all businesses, large and small. However, if new federal legislation and prescriptive regulations are adopted, small businesses would require an exception for using limited amounts of non-sensitive data.

- *Is it feasible for the framework to apply to data that can be “reasonably linked to a specific consumer, computer, or other device”? And, how should the framework apply to data that, while not currently considered “linkable,” may become so in the future?*

A workable framework should apply principles and codes of conduct for all data, whether presently or prospectively “linkable” to a user or device. Principles and codes governing sensitive data, for instance, would govern collection, consent, and use whether or not this data is linkable.

By the same token, most commercial data is collected to update interest categories that are not sensitive, such as a user’s interest in sports or politics. This non-sensitive data should not be subject to opt-in consent or detailed access and correction, even if it were linked to a specific computer or device.

B. Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services

NetChoice supports a “privacy by design” approach driven by customer preferences, not government regulation. Online companies know that consumer confidence is essential and thus have sufficient incentive to meet consumer expectations, a point not adequately acknowledged in the report. Data breaches, for instance, impose significant economic and reputational costs upon companies.

Companies must maintain the ability to set and experiment with defaults for information sharing without reprisal from government agencies and state AGs. Otherwise, new product development innovation will suffer, ultimately harming consumers.

To encourage companies to adopt privacy by design, our proposed framework includes a code of conduct requirement for *Privacy Impact Assessments* whenever a company designs a new service or feature that affects data collection or use.

Internal Privacy Impact Assessments (PIAs) -- Not for Publication

The Commerce Department Green Paper discussed enhancing transparency through privacy impact assessments (PIAs). Companies adopting an industry self-regulatory framework that included PIAs would commit to do these assessments before releasing a new service or feature that collects or shares user data. The object of the PIA is to determine whether data collection or use would be a material change from existing uses for which consent has already been obtained. For new features that require migration of old user preferences, a PIA could help companies decide default settings and whether additional notice or consent should be obtained.

PIAs should be internal self-assessment exercises, and the code of conduct could require that companies retain their PIA documents for future investigations or enforcement actions.

However, the Commerce Department Green Paper also cited commenters who advocate that impact assessments be made public.⁹ We strongly disagree.

If PIAs were required to be publicized before releasing new services, innovation would effectively require a ‘permission slip.’ Also, public debate over PIAs could be contentious and costly, especially for smaller companies. Required submission of PIAs to the government or the public would result in over-inflation of the risks, much like in SEC filings, and publication of PIAs could disclose far too much information to competitors, including trade secrets.

Publishing PIAs would therefore needlessly inflate privacy fears, be exaggerated by pro-regulatory privacy groups, and be hijacked by competing companies and plaintiff’s lawyers. PIAs should *not* be published in advance of introducing new features and services.

Many—if not most—companies already assess the privacy implications of new applications and services in accordance with “privacy by design” considerations. 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 Commerce Green Paper highlights how PIAs might operate by referencing the European RFID PIA (FN 108).¹⁰ Page 3 of the referenced document further describes the European approach and the highly public and sensitive nature of PIAs:

⁹ Dynamic Privacy Framework report at 35.

¹⁰ http://ec.europa.eu/information_society/policy/rfid/documents/d31031industry pia.pdf.

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, our mantra of transparency will likely mean that reported 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 want to block an innovation. And companies could examine PIAs to learn about 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, whether or not PIAs are published in advance.

- *Should the concept of “specific business purpose” or “need” be defined further and, if so, how?*

NetChoice supports a policy of purpose specification and use limitation. This would require 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 Commerce 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*.¹¹ 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 moment that will truly educate and inform users about the meaning behind the choice.

However, if the purpose specificity is too specific, consumers are presented with an easily ignorable laundry list of uses put forth to satisfy regulators – not consumers. We want to inform consumers, not confuse them with a parade of intended and potential uses. And we want to 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 services; (D) fraud prevention and authentication; (E) research; and (F) public purposes. Irrespective of

¹¹ <http://www.aboutads.info/>.

where data was collected or by whom, the obligations related to the use categories must be honored.¹²

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.

- *Is there a way to prescribe a reasonable retention period?*

Prescriptive regulations for reasonable retention periods will inevitably lead to a one-size-fits-all approach. Once again, the reasonableness of a data retention period depends upon a company's business model and the nature of their relationship with users. Neither the Commission nor Congress should attempt to prescribe specific retention periods.

Maintain comprehensive data management procedures

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 framework, 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:¹³

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.

¹² Microsoft comments at 4. <http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Microsoft%20Comments%2Epdf>

¹³ <http://www.iab.net/media/file/ven-principles-07-01-09.pdf>

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.¹⁴

Moreover, NAI has procedures for increasing transparency and exposing non-compliant 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.*”¹⁵

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.

- *How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?*

The FTC has a powerful tool to encourage companies to adopt privacy policies and frameworks. In his concurrence, Commissioner Rosch stated that companies who don’t adopt a privacy policy invite Section 5 liability “in that it would entail a failure to disclose material facts.”¹⁶ We agree, and encourage the Commission to investigate and take enforcement actions against companies who collect user information without adopting a privacy policy.

C. Companies should simplify consumer choice

NetChoice supports efforts to simplify notice and choice methods. But we are convinced that providing “universal choice” to opt-out of all tracking through a *Do Not Track* mechanism would be ineffective for consumers and destructive to ad-supported websites and services.

An overly simplified choice fails to convey to consumers the benefits interest-based advertising provides in funding innovation and free online services. Consumers likely do not understand that they will still see advertising under any universal choice regime – only those ads will be less relevant to their interests. In addition, these ads will provide less revenue to all content publishers, and greatly harm the “long-tail” sites that depend on third-party ad networks the most. Some sites may be forced to go to a less lucrative subscription model or may go out of business entirely. Thus, consumers are hurt through the denial of useful advertisements and companies are harmed through lost revenue. This makes a universal *Do Not Track* mechanism a lose-lose for both consumers and companies.

¹⁴ www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf

¹⁵ NAI principles, p. 12, at www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf

¹⁶ FTC Report – Concurring Statement of Commissioner J. Thomas Rosch, page E-1.

Commonly accepted practices

NetChoice rejects a privacy framework that would require businesses and regulators to determine what is and is not “commonly accepted.”

Online information flows are dynamic and business models are constantly in flux. What is novel and unique today may be commonly accepted tomorrow. A regulatory framework that differentiates between “common” on the one hand and “uncommon” on the other risks harming innovation or effectively prevents it from becoming a common practice.

For instance, 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.”¹⁷

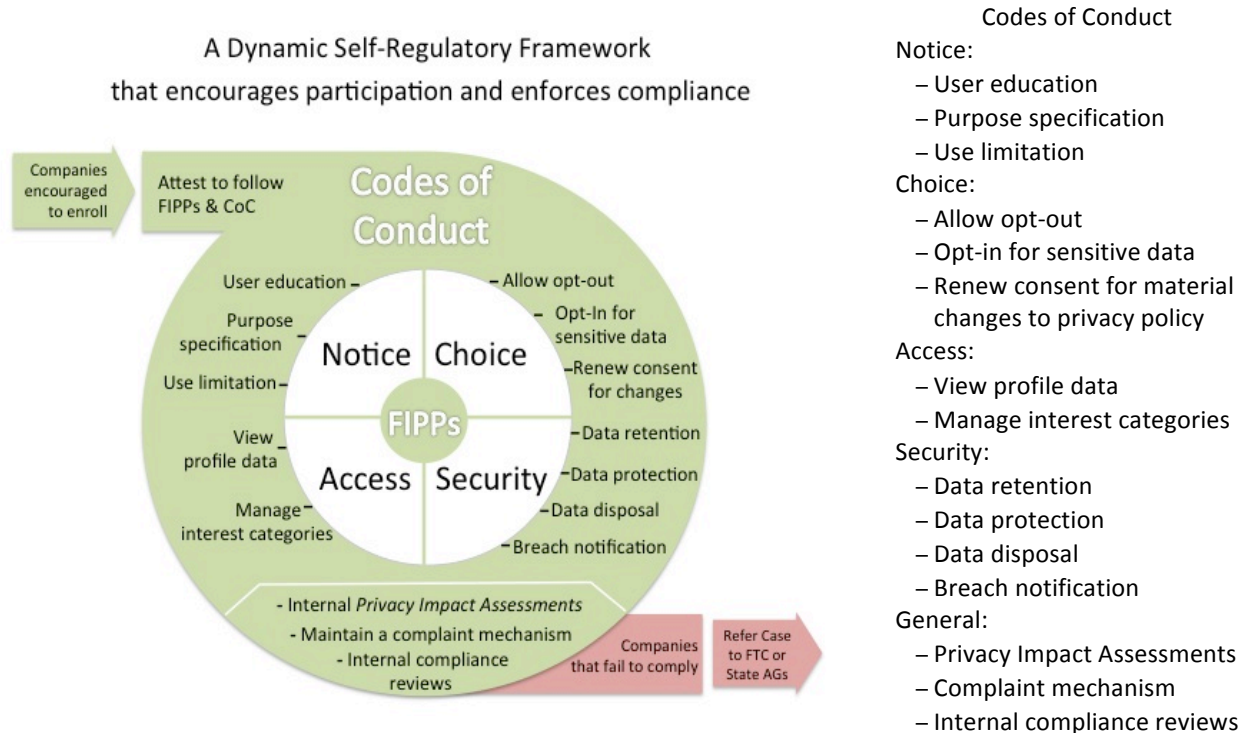
Facebook is just one of many proof points for why the appropriate measure of success for self-regulation is not the quantity of rules, but the balance between effective regulation and innovation. The US is the world leader in Internet innovation. Here, there is an ongoing and vibrant movement for self-regulation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

The report’s discussion of “commonly accepted practices” is similar to “operational purpose” described in recent Congressional legislation. Both concepts attempt to create safe harbors for data collection and use that an average user would consider reasonable, given the value they receive from the website or online service.

- *Is the list of proposed “commonly accepted practices” set forth in Section V(C)(1) of the report too broad or too narrow? Are there practices that should be considered “commonly accepted” in some business contexts but not in others?*

As described earlier, NetChoice proposes a *Codes of Conduct* approach to assure consumers that their data is being collected and used in accordance with fair information principles. A preliminary set of codes of conduct are shown in our conceptual overview and listed on the right.

¹⁷ <http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Facebook%20Inc%20Comments.pdf>



- *What types of first-party marketing should be considered “commonly accepted practices”?*

NetChoice believes that static regulations describing commonly accepted practices would stifle innovation in new services. Also, the distinction between first-party and third-party is too subtle a distinction for most consumers, who quite reasonably regard everything on a webpage as the responsibility of the party who composed and sent the page back to their browser.

If we are truly serious about transparency and choice, we must minimize static and legalistic distinctions such as first-party and third-party and encourage companies to adopt a privacy framework for all content they deliver to their users.

Practices that require meaningful choice

- *Should the method of consent be different for different contexts?*

Yes, consent methods should depend upon the context of how information can be used and upon the nature of the information. More sensitive PII should be treated differently from less sensitive PII. In particular, non-PII data used to deliver more relevant ads should, at most, be subject to an opt-out method of consent.

- *Under what circumstances (if any) is it appropriate to offer choice as a “take it or leave it” proposition, whereby a consumer’s use of a website, product, or service constitutes consent to the company’s information practices?*

If the FTC attempts to impose a *Do Not Track* regime, some websites may turn to a “take it or leave it” approach to privacy.

- *Should additional protections be explored in the context of social media services? For example, one social media service has stated that it limits default settings such that teens are not allowed to share certain information with the category “Everyone.” What are the benefits and drawbacks of such an approach?*

One of the key aspects of COPPA’s success is that it applies to a well-defined demographic—young children under the age of 13. As opposed to teenagers, younger children are not as active on the Internet and have distinct tastes, preferences, and aptitude levels. It is therefore easier to determine whether a website is directed to young children than it is to assess whether sites are directed to teenagers, who share interests, aptitude, and abilities more in common with adults.

Yet, at the Commission’s COPPA Rule Review roundtable event, we heard participants advocate for increasing COPPA’s scope to cover teenagers. Some think that there’s an adolescent “gap” that should be addressed. Even if the Commission were inclined and had the authority to increase the age of applicability for COPPA, Congress specifically selected children under 13 as deserving of special attention. And COPPA is not alone with identifying age 13 as a milestone:

- The Federal Communications Commission defined “children” as *under the age of 13* for purposes of the Children’s Television Act.
- MPAA movie ratings – PG 13 (“Parents strongly cautioned—some material may be inappropriate for children under 13”).
- Entertainment Software Rating Board computer and video game ratings – T (“Teen”) rating indicates that content “may be suitable for ages 13 and older.”
- Internet Education Foundation Parental Empowerment and Convergence Guide – 13 is threshold age for exposure to more mature movies, TV programs, and computer/video games.

Increasing COPPA’s age threshold to age 15, or even 17, would be a wrongheaded approach. It would greatly expand COPPA’s reach and create new liability for thousands of websites.

It could also force sites to age-verify and obtain parental consent on a massive scale. Yet, we know that it is impossible to precisely determine a child’s age online. According to a report of Harvard University’s Berkman Center, “*age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness.*”¹⁸

There are practical problems of parental verification on a widespread scale. Verifiable parental consent is difficult to implement, and many sites simply lock-out their websites to anyone indicating they are less than 13 years old.¹⁹ However, a simple COPPA lock-out won’t easily translate to the 13 to 17 age

¹⁸ Available at <http://cyber.law.harvard.edu/pubrelease/isttf/>.

¹⁹ Berin Szoka and Adam Thierer, COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech, Progress & Freedom Foundation, available at <http://www.pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf>.

bracket affected by this Act, as teenagers are more adept at circumventing online locks of any kind. And because it requires involvement by parents, relying on parental verification may not protect society's most vulnerable minors who have absentee parents.

In addition, there are privacy and security concerns related to age verification methods. After all, the process of verifying age necessarily entails the collection of data sufficient to determine proof of age, and all this data must be transmitted, processed, and stored.

Finally, it should be recognized that Congress chose not to apply COPPA's parental consent regime to teenagers because of free speech concerns. In many circumstances, such as access to reproductive health information, adolescents have First Amendment rights on par with adults. Therefore, the rights of 13 to 17 year olds to access and receive information are stronger than those of younger children.

Universal choice for online behavioral advertising: *Do Not Track*

A regulatory or legislative *Do Not Track* regime would become a brake on legitimate business and marketing and undermine the revenue that's driving online innovation.

As described in the report, the FTC is calling for a "uniform and comprehensive" way for consumers to decide whether they want their activities tracked.²⁰ 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* to an overly-simplified choice. 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 simply because they fear a worst-case scenario. In doing so, they'll reduce the revenue earned by websites for advertising that's targeted through tracking and threaten the free or discounted services that users have come to expect.

Similar to the way that television programming is paid for, much of the content and services available online are paid for by advertising revenue. For example, The New York Times provides its content online at no cost to consumers because it generates revenue through ads targeted to user interests. Websites provide free services such as search, social networking, and email because they too are paid for with targeted advertising.

Preventing companies from using user tracking technology will result in lower ad revenue. Companies will either reduce their spending on content and services, or they will dedicate more space to show even more advertisements as they try to replace the lost revenue.

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

²⁰ <http://ftc.gov/os/2010/12/101201privacyreport.pdf>

“[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.”²¹

At the very least, *Do Not Track* should 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.²² 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.”²³ 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, we encourage a framework that includes Codes of Conduct that can be adapted and tuned to each unique website and online service. A Code of Conduct approach is granular, while *Do Not Track* is a 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.

NetChoice does not support universal choice mechanism for serving interest-based ads.

- *If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?*

NetChoice does not support legislation that creates private rights of action against business and then offers safe harbors from these lawsuits. We believe it is much better to have industry participation on the front-end, using a carrot instead of a stick.

Moreover, the FTC should not embark on rulemaking process 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 allow privacy advocates and affected individuals to press for FTC and state AG enforcement. Complaints and investigations allow dissenting voices to be heard, particularly if it involves a company-specific failure to adhere to a particular Code of Conduct.

D. Companies should increase the transparency of their data practices

We support greater transparency through clear, simple, and standardized privacy policies.

Improved privacy notices

²¹ <http://www.nytimes.com/roomfordebate/2010/12/02/a-do-not-call-registry-for-the-web/tracking-personalizes-the-web>

²² For example, the Rush bill has an “Operational purpose” exception to express consent for customer service, security, business functions, IP rights, safety, and law enforcement. In addition, the Boucher/Stearns bills have similar provisions.

²³ Rush bill, avail at <http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111UnXKfn>

NetChoice agrees with the Chairman's call for privacy choices to be presented to consumers in a "simpler, more streamlined way."²⁴

We support 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, companies need assurances from the FTC about its enforcement expectations.

Chairman Leibowitz criticized current privacy notices as being "long, incomprehensible privacy policies and user agreements that consumers don't read, let alone understand."²⁵ We share the Chairman's critique, but also believe that current FTC enforcement policy is partially to blame.

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.

- *What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?*

We agree with the Chairman's call for privacy notices to be "clearer, shorter, and more standardized, so people understand what's happening with their information and who's watching what they do online—and off."²⁶

Reasonable access to consumer data

It's essential to remember that data access is not cost-free. Companies will have to develop IT systems that can authenticate users requesting access, retrieve data applied to that user, and respond to requests for opt-out or data deletion. Ironically, this process may require re-aggregating data in a way that identifies specific users, which itself raises privacy issues.

- *Should companies be able to charge a reasonable cost for certain types of access?*

Companies are already allowing consumers free access to the interest categories that drive more relevant ads. For instance, Yahoo displays interest categories behind ads served in its website, as seen in the example below. Moreover, Yahoo's AdChoices feature lets users freely adjust their interest categories or to opt-out altogether from interest-based ads:

²⁴ <http://www.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf>

²⁵ *Id.*

²⁶ *Id.*

Your Interest Categories [?](#)

We use information about many of the pages you have visited, ads you have seen and clicked, and some of your searches on Yahoo! to create interest categories that help us choose the kinds of ads you'll see. You can edit or de-select categories here or opt out of interest-based ads altogether. [See All Standard Categories](#)

Interest Categories: Set to:

Automotive	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF
Finance	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF
Finance > Investment	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF
Miscellaneous > News	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF
Miscellaneous > News > Business and Finance	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF
Retail	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF
Retail > Books	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF
Sports	<input checked="" type="checkbox"/> ON	<input type="checkbox"/> OFF

[+ Show All](#)

Interest-based Ads:
Are currently on.

You must allow cookies from Yahoo! in order to opt out. To make your opt-out apply to every computer you use you must be signed in to your Yahoo! account. [Learn more.](#)

However, if regulation or legislation were to require companies to retain the detailed historical data that contributed to these categories, then companies *should* be able to charge for that additional storage and retrieval. In any event, historical data should not be subject to correction, since the consumer can already correct the interest categories that result from historical tracking.

- *Should consumers receive notice when data about them has been used to deny them benefits?*

This question implies that the Commission may consider requiring consumer notification whenever data contributes to denial of benefits or services. If the Commission and Congress were to mandate such notice, it should be done with sectoral specificity, for sectors such as financial services, insurance, and health care. And any such notice requirements should apply equally to all data that informs such decision. It would be blatant discrimination and obviously ineffective to require such notice *only* for data that was collected through *online* mechanisms.

Material changes

- *What types of changes do companies make to their policies and practices and what types of changes do they regard as material?*

As we described in the section on Privacy by Design, companies can conduct internal privacy impact assessments before making a change to how they collect or use user information. A Privacy Impact Assessment would determine whether the changes are material, and what level of consent should be acquired before implementing the change. For example, a material change in how non-sensitive user information is used in a website should require, at most, an opt-out consent from users.

- *What is the appropriate level of transparency and consent for prospective changes to data-handling practices?*

As discussed above, NetChoice believes that the notion of “appropriate” with respect to transparency and consent must be handled on a case-by-case basis.

Consumer education

The effort to educate consumers is already underway, as seen in the *Self-Regulatory Program for Online Behavioral Advertising*. Central to it is the Advertising Option Icon, which allows consumers to understand why they see a given ad, to adjust their interest categories, and even to opt-out of future targeted ads. It’s a just-in-time approach that gives the kind of teachable moments that will truly educate and inform the meaning behind the choice. The icon has only recently been activated, and the mechanisms to hold companies accountable will go live this year.

