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

June 14, 2010

FILED ELECTRONICALLY

National Telecommunications and Information Administration
US Department of Commerce

In the Matter of the Request for Comments on
Information Privacy and Innovation in the Internet Economy
Docket No. 100402174-0175-01

Comments of NetChoice on Information Privacy and Innovation in the Internet Economy

NetChoice welcomes this opportunity to comment on the nexus between privacy policy and innovation. In its Notice of Inquiry (NOI), 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 over 13,000 small businesses that rely on e-commerce. NetChoice works 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 to use online innovations that clashed with legacy regulations designed to protect traditional business models. Today, NetChoice members face proposals to regulate social networking websites, tax out of state retailers, and restrict marketing to teenagers.

Privacy-related laws that specify how data can be collected, used and shared also create barriers to legitimate online commerce. As Internet commerce knows no borders, online companies have had to be vigilant and work vigorously to keep state laws roughly consistent when it comes to information privacy. So while there is a constant threat of new state privacy regulations,

online companies have thus far managed to avoid an unworkable patchwork of inconsistent laws here in the United States.

However, as our members expand to international markets, they need an effective advocate before national governments and intergovernmental organizations.

The Department of Commerce can be this advocate. The Department was a champion for online commerce through the administration of the US - European Union (EU) Safe Harbor Framework. 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.

At the Department's recent symposium on privacy and innovation, one of the panelists, Leslie Harris of the Center for Democracy and Technology, remarked on how the US is often viewed by other countries as an outlier on privacy regulation.[1] Yet, she followed by noting that the US is the innovation leader in privacy-enabling technologies, and that we need to lead on privacy policy too.

NetChoice agrees that the US must lead in policy, just as our companies lead in privacy. In an effort to help the Department advocate for US interests on privacy and innovation, we focus our comments on four of the issues raised in the NOI: The US Privacy Framework Going Forward; US State Privacy Laws; International Privacy Laws and Regulations; and The Role for Government/Commerce Department.

The Privacy Framework Going Forward (NOI request 1)

The NOI seeks comment on "the current privacy framework" and ways in which such a framework needs adjusting to preserve and enhance innovation and privacy. This inquiry raises weighty issues that require more than a cursory analysis of current privacy-related laws and business practices. There must also be a fundamental discussion of what privacy is, how it is valued by some consumers, and what should be the proper focus of privacy-related public policy.

Defining the privacy framework

When studying the interplay between privacy and innovation, the Department should recognize that privacy is often an abstract and individualized concept. Privacy is a subjective condition people experience when they have power to control information about themselves. But privacy is also objective, and can be measured against terms of service or on the basis of unfair or deceptive practices that result in measurable harm to consumers.

[1] Department of Commerce, *A Dialogue on Privacy and Innovation*, Washington, DC, May 7, 2010, agenda available at http://www.ntia.doc.gov/internetpolicytaskforce/privacy/symposiumagenda_05072010.pdf

As the Italian Google case revealed, Europeans and Americans attach different meanings to privacy.[2] Europeans view privacy as a fundamental human-dignity right, to be protected by government. Americans view privacy as a protection *against* government overreaching, and as part of a consumer's relationship with providers of products and services.

Therefore, in today's globally connected society, innovation and international harmonization will be best served when policymakers focus on regulating objective aspects of privacy. Policymakers can and should continue to focus on a "harms-based" approach toward enforcement. The abuse and misuse of data should be considered unfair or deceptive.

The Obama Administration should encourage the Federal Trade Commission (FTC) to increase its enforcement efforts against unfair or deceptive data practices. Enforcement actions based on fraud and other unfair practices would be consistent with the NOI's reference to a "use-based model." This model would apply rules not to the collection of personal information, but to purposes for which personal information may be used.[3] However, any use-based privacy model should first derive its rules from consumers in the marketplace, as we explore in the next section.

Consumer Expectations are Evolving

As consumers disclose and share more of their personal information, users of online sites have been demanding more control over their information. Online companies are responding to customer feedback and creating more flexible and more granular privacy controls. Consumers have the ability to change their preferences or leave the service—the latter being the ultimate expression of customer feedback.

Consumer expectations about new technologies are always in flux. In the 1990s, telephone caller ID services that displayed the caller's phone number were feared by some as privacy invasions. But now we expect to see caller ID or message sender information before we engage with an incoming phone call, text message, friend request, or tweet.

Innovative social media technologies are creating new ways for users of all ages to create and share content and information. At the same time, online business models increasingly depend on advertising revenue to offer their products free of charge to their users.

Online companies are therefore experimenting with new ways to make advertising more relevant to their customers, often by collecting and using information from and about their users. With this rise in the commercial use of data about a person (but not necessarily personally identifying information), we have seen rising expectations from users about how much control they have in sharing their information.

Some of the most popular companies on the 'Net are working hard to meet these expectations. Last month, Facebook unveiled new privacy controls that simplify how its users control who can

[2] See Adam Liptak, "When American and European Ideas of Privacy Collide", New York Times, Feb 26, 2010, available at http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html
[3] NOI at 21229.

see photos, comments, and activities.[4] Facebook also allows users to easily turn-off information sharing with third party applications hosted on Facebook.

Facebook is offering new privacy controls at the same time it introduces new product features. Facebook's "instant personalization" feature helps selected websites customize content based on a user's Facebook profile. And a "social plugin" for third party websites allows Facebook users to seamlessly recommend content or news articles to their friends.

Facebook's innovations help create a personalized and social Internet experience, and they do it through the sharing of information. For online services to truly maximize the value of new product features, they will want to encourage users to try them, and will set user defaults accordingly. As we explore in the next section, defaults for how and to whom users share information are an integral part of online innovations.

Privacy Frameworks Must Preserve Flexibility in Setting User Defaults for new forms of Information Sharing

The NOI clearly captures the challenge facing policymakers: "Our challenge is to align flexibility for innovators along with privacy protection."[5] No matter what the privacy framework, online services need the flexibility to set user defaults when changing functionality or adding new features.

Flexibility means that online companies should have the legal ability to make decisions on how to best carry-over a user's preference from a prior product version to a new one. It also means that online services should be able to make assumptions on user privacy preferences for new features.

These considerations matter whenever an online service tries to increase its social networking functionality. As an example, Yahoo recently announced that it will change how status updates appear in its Yahoo Mail service.[6] Like Google and Facebook before it, Yahoo is adding features that make user information more public. According to Yahoo:

> Before Yahoo! Updates is expanded to Yahoo! Mail where many more people will see their Contacts' activity, we want you to explore your Updates settings and make sure you know who can see what you're publishing. Even if you are among the many Yahoo!

---

[4] See Mark Zuckerberg, The Facebook Blog, May 26, 2010, available at http://blog.facebook.com/blog.php?post=391922327130

[5] NOI at 21227.

[6] See Michael Arrington, "Yahoo Expands Yahoo Updates, Tiptoes on Privacy", May 31, 2010 at http://techcrunch.com/2010/05/31/yahoo-expands-yahoo-updates-tiptoes-on-privacy/ that describes the change:
[C]urrently to see status updates for others in Yahoo Mail, you have to have a mutual follow, meaning both people have agreed to be "friends." You can then see that user's Yahoo status updates as well as updates on third party services that they have added to their Yahoo profile as well. In the new version there will no longer be a requirement for a mutual follow. So, like on Twitter, users can follow whomever they choose. This isn't actually a dramatic change for Yahoo, since users can follow others in this way already on Yahoo Messenger.

> users who haven't ever generated an update, we want to encourage everyone to actively manage these settings. Because the majority of events listed within Updates are inherently public activities, our defaults are set to allow anyone to see them (that is, for people over 18; we have different defaults that are age-appropriate for people under 18 – learn more in our FAQ).[7]

As online services add features and functionality, they will strive to seek a balance. They will want to respect previously expressed user preferences, while defaulting settings so that people see and are encouraged to use new features.

In the case of Yahoo, its Messenger service makes user updates public, so Yahoo will also make updates public in Mail. But in another sense, Yahoo must make assumptions—that users want to have their updates be public. Hence the rationale for Yahoo's explanation: *Updates are inherently public activities, our defaults are set to allow anyone to see them*.

Yahoo is also making it easy for users to control and opt-out of sharing status updates:

> "[Y]ou can easily limit who sees your Updates stream either by editing the controls for each specific activity…or by turning your Updates stream off entirely in one simple step."

Thus the challenge for policymakers is a similar calling for online companies—"align flexibility for innovators along with privacy protection"—in order to earn consumer trust. But if the threat of regulation becomes too great, companies will be afraid to take risks and introduce new services. A privacy framework that mandates opt-in arrangements would force many online services to perpetually maintain original settings and limit innovative business models. In the case of Internet commerce, strict consistency will become a brake on innovation.

Companies won't always find the right balance right away. Online services need the freedom to experiment with new ways for publishing and sharing information, with the expectation that they will adjust quickly based on user response.

As the social web matures, we'll see more and more sites confronted with this balancing act. They'll need to carryover preferences from old to new versions, and make assumptions on what information most users will or will not want to disclose. If sites get it wrong, some users will change their settings, while others will leave—ultimately, either is a better expression of user preferences than any law or regulation.

In conclusion, no matter what the privacy framework, it should be flexible and based on harmful uses, not theoretical abuses.

US State Privacy Laws (NOI request 2)

Below we discuss some recent state proposals to regulate online privacy in ways that would harm innovation on the Internet.

[7] Yahoo Corporate Blog, available at http://ycorpblog.com/2010/05/31/yahoo-privacy/

Examples of State Legislative Activity

NetChoice has been active in state legislatures to oppose laws that govern how companies collect, use and disclose personal data. Compliance with a state law by a company that operates websites available nationally (and internationally) is difficult and burdensome.

For example, NetChoice was lead plaintiff in a lawsuit challenging a Maine law that placed broad restrictions on the collection and transfer of personal information about minors. The law, passed in 2009, required websites to obtain "verifiable parental consent" before collecting personal data or marketing to Maine teens under the age of eighteen.

As a result of the lawsuit, Maine's Attorney General agreed not to enforce the law, pending revision or repeal by the legislature. As a result, the legislature organized a two-day joint hearing of the judiciary committee where NetChoice and a number of affected companies filed comments and traveled to Augusta to testify and persuade the committee to recommend full repeal of the law.

Earlier this year, Maine's Senate took-up legislation to repeal the law, but added replacement language focused on medical products and services. The new language would have required verifiable parental consent for showing ads relating to any health concerns. Eventually, the sponsor dropped her replacement language and the legislature repealed the marketing to minors law.

NetChoice has also opposed online safety-related legislation that would have had serious privacy implications. Last year, New Jersey proposed a law to extend the federal COPPA requirements from children twelve and younger to include teens up to 17 years old.[8] As is the case under COPPA, Internet services and Web sites would have been required to obtain verifiable parental consent when attempting to collect personal information from teenagers in addition to children twelve and under.

The bill would have extended COPPA's reach to apply to all Internet websites "directed at adolescents" and dramatically altered the innovative landscape of online services. It would have effectively required parental consent before any teenager could obtain an e-mail address, Instant Message address or register to receive information from a website. It would also have clearly applied to many social networking websites.

The bill was withdrawn by its sponsors before it could be heard in committee, after a groundswell of opposition from child safety experts, public interest groups, legal experts, and industry.

Another variant of online safety bills are of the same variant of COPPA and the New Jersey bill, but would apply only to social networking websites. These bills required parental consent before a minor can become a registered user of a social networking website. Variants of this

[8] 213th Legislature, Reg. Sess. (N.J. 2008), available at http://www.njleg.state.nj.us/2008/Bills/A0500/108_I1.PDF

requirement were introduced in Connecticut, Georgia, Mississippi and North Carolina in 2007 or 2008, and in Illinois last year.[9]

The typical bill language used to create a duty on social networking websites to obtain verifiable parental consent goes something like this:

> No owner or operator of a commercial social networking website shall allow a minor using a protected computer to create or maintain a personal webpage on a social networking website without first obtaining the permission of the minor's parent or guardian and without providing the parent of guardian access to the personal webpage at all times the commercial social networking website is operational.

The typical bill language used to create a duty to authenticate age and parental identity is as follows:

> Any owner or operator of a social networking website shall adopt and implement procedures to confirm the identity and age of parents or guardians who are providing permission for their minor children and members at the time of registration by validating the accuracy of personal identification information submitted at the time of registration.

Finally, social networking websites would have to retain permission records, perhaps indefinitely:

> The owner or operator of a social networking website must keep either a hard copy or electronically scanned copy of the written permission of the parents or guardians in a database maintained by the social networking website.

NetChoice worked with other members of the online community to present the privacy pitfalls involved with collecting and keeping additional personal information just in order to comply with new legislation. To verify parental consent, for example, online services must require parents to provide personally-identifying data (such as credit card information). As a result, private companies would have to store vast amounts of parents' personal information and, by doing so, increase customers' vulnerability to security breaches and identity theft.

A 2008 report by the Berkman Center's Internet Safety Technical Task Force did not recommend remote age and identity verification for use by online forums and social networks, saying, *"there are significant potential privacy concerns and security issues given the type and amount of data aggregated and collected by the technology solutions…"*[10]

As mentioned above, state privacy laws do not yet present insurmountable compliance barriers. While there have been state legislative proposals on privacy, industry has thus far minimized the

---

[9] H.B. 6981 (Conn. 2007), S.B. 59 (Ga. 2008), S.B. 2586 (Miss. 2008), S.B 132 (N.C. 2008), HB 1312 (Ill. 2009).

[10] John Palfrey et al., *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States* (2008), available at http://cyber.law.harvard.edu/pubrelease/isttf/

patchwork problem for interstate e-commerce. However, as we note in the next section, if Congress were to enact federal privacy law, it should occupy the field and prevent states from burdening online companies with multiple, inconsistent laws.

The Federal / State Balance: Preemption Should Establish a Ceiling, While Allowing for State Enforcement Action

If Congress were to enact legislation to regulate information collection, use and sharing, it should broadly preempt the states. Different state-level privacy laws and regulations would increase compliance costs and frustrate the product development process of online services. Congress should therefore establish a ceiling, not merely a floor, for privacy-related legislation.

But we should emphasize that federal preemption does not mean that states are kept off the field entirely. Rather, states can and should retain their consumer protection role. The Department should coordinate with the FTC and state attorneys general to target bad actors that impact online commerce by reducing consumer trust and confidence.

Aggressive enforcement will help foster a better climate for innovation than would expanded regulation. New regulations are followed only by legitimate businesses who were already complying with the old regulations. Bad actors, on the other hand, ignore both old and new regulations with impunity (e.g., Spammers are still spamming even after the FTC issued new regulations pursuant to the CAN-SPAM Act). Moreover, the Internet knows no borders, and delivers advertising and services to US consumers from foreign companies that cannot be compelled to follow US law.

Still, as we discuss in the next section, the Internet allows for global commerce. Federal preemption applies to states, but will not impact the privacy laws of other countries. FTC enforcement does not apply extraterritorially. Continued innovation and growth for online companies based in the US means that they will have to navigate international privacy laws and regulations.

International Privacy Laws and Regulations (NOI request 3)

At the Department's symposium on privacy and innovation last month, we heard how laws are keeping us apart even as technologies are trying to bring us together.[11] We also heard that government demands for data from the private sector are fatal to international cooperation.[12]

These comments underscore the broad impact that government policies have in the information economy. Laws and regulation can help promote or harm the growth of online commerce across jurisdictions, particularly because data flows today are much more complex than they were even a decade ago. Simple one-way transfers between one country and another have been replaced by multinational corporations that transfer data across multiple jurisdictions on a daily basis.

[11] Fred Cate, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[12] Ibid.

As data flows become more complex and multi-jurisdictional, there must be a mutually recognized framework for information privacy. The Department's symposium exposed a lot of issues that remain to be addressed:

- EU data protection law requires multiple intercompany contracts, which are disproportionately expensive and challenging for small businesses.[13]

- US companies often launch new services in an unfinished "beta" format, but the EU doesn't favor this approach and wants privacy locked-down before a service is launched.[14]
- Inconsistent privacy regulations result in opportunity costs, because new products are not launched, or are not exported to other countries.[15]

The Department can work with foreign regulatory authorities and multi-governmental organizations to develop new mechanisms for achieving mutual recognition. The EU's policy toward Binding Corporate Rules (BCRs) could emerge as a key element of a mutual recognition framework. BCRs are corporate codes of conduct that legally bind a company and its partners to EU-compliant data management systems.[16] BCRs allow companies to share personal data on EU citizens, in-house and worldwide.

However, BCRs represent a serious commitment for companies, and they are out of reach for most American companies. They require extensive time and financial resources to implement. There are also ongoing costs for compliance, internal control and supervision, and auditing. These costs challenge even the largest of companies, but can be prohibitive for small businesses. Still, BCRs are a promising mechanism for cross-border compliance that should be made more widely available to companies of all sizes.

The Department should work with the European Commission to greatly simplify the BCR process and make it more accessible to small businesses. There should also be new rules that encourage and reward member states that implement BCRs. For online companies to be able to take full advantage of the BCR process, European Data Protection Authorities (DPAs) need to fully embrace the BCR process, as only 19 EU member states collaboratively work on BCR applications while others flatly refuse to recognize them.

The Role for Government/Commerce Department (NOI request 8)

Online companies welcome an increased role for the Department in promoting online commerce in a privacy-related context. As previously discussed, the Department should work with the FTC to step-up state and federal enforcement against unfair or deceptive information practices.

---

[13] Jim Halpert, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[14] Dan Burton, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[15] Fred Cate, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[16] Christopher Wolf and Timothy P. Tobin, *The European Union ("EU") Data Privacy Directive* (2007), Proskauer on International Litigation and Arbitration: Managing, Resolving, and Avoiding Cross-Border or Regulatory Disputes.

The current process through which the FTC makes rules, as established by the Magnuson-Moss Act, is a proven and effective vehicle for the regulation of business and provides the Commission with enforcement authority to punish businesses that act in a deceptive manner or in ways that are unfair to the consumer.

But there's another important role for the Department: an international ambassador for innovative American online companies. Now is a critical time for online commerce as international policymakers assess their approaches to privacy. The Department can play an important role as a government-to-government advocate for flexible 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.

As an international spokesman for online service innovation, the Department can promote privacy laws that are flexible enough to permit innovation, and oppose static laws that undermine consumer interests in improved online services. And as a government agency speaking to other government agencies, the Department can bring credibility and leverage that cannot be matched by corporate interests alone.

We note that this month NTIA Assistant Secretary for Communications and Information, Larry Strickling, is scheduled to meet with Neelie Kroes, EU Commissioner for the Information Society. Such a high-level meeting provides the opportunity to identify national regulations that become international barriers to innovation.

NetChoice members encourage the Department to increase its engagement with the EU, OECD, and at the United Nation's Internet Governance Forum. The Department should remain a consistent voice of American business interests in Europe, Asia and globally.

Respectfully submitted,

Steve DelBianco, Executive Director
Braden Cox, Policy Counsel

NetChoice is a coalition of trade associations and e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org