

Testimony of Ira Rubinstein

**Adjunct Professor and
Senior Fellow, Information Law Institute
New York University School of Law**

**Legislative Hearing Examining H.R. 5777, the BEST PRACTICES Act, and the Boucher-Stearns
Discussion Draft**

**Before the
Subcommittee on Commerce, Trade, and Consumer Protection**

**U. S. House of Representatives
July 22, 2010
2322 Rayburn House Office Building**

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today on H.R. 5777, the BEST PRACTICES Act, and the Boucher-Stearns discussion draft. My name is Ira Rubinstein and I am Adjunct Professor at New York University School of Law and a Senior Fellow at the Information Law Institute. I am grateful for the opportunity to appear before the Committee this afternoon and also for your efforts in developing comprehensive legislation that responds to growing public concern over privacy in the digital era.

I will focus my comments specifically on a key question in Congress' longstanding effort to regulate online privacy—what is the relationship between privacy legislation and industry self-regulation? To what extent should Congress encourage self-regulation by allowing alternative forms of compliance based on “safe harbor” provisions? Have existing safe harbor programs achieved their goals and, if not, how might they be changed to make them more effective?

Background: What is a Safe Harbor?

To answer these questions, I first need to say a few words about how safe harbors work, in theory and in practice. A safe harbor is a regulatory strategy under which a federal statute recognizes differences in industry performance explicitly by treating regulated firms who qualify more favorably than non-qualifying firms. In other words, safe harbors shield or reward firms if they engage in desirable behavior as defined by statute. Favorable treatment for better performing firms might include immunity from liability, protection from certain penalties,

exemptions from certain requirements, and/or permission to engage in certain desired behaviors. The key point to emphasize is that eligibility for the benefits conferred by a safe harbor are contingent upon a participating firm meeting a higher standard of performance than what is otherwise required of firms covered by the relevant statute.

In the privacy arena, the most familiar example of a safe harbor is the Children's Online Privacy Protection Act (COPPA). Section 5503 of this Act establishes an alternative means of compliance for operators that follow self-regulatory guidelines issued by an industry representative and approved by the Federal Trade Commission (FTC), subject to a notice and comment procedure. The COPPA safe harbor seeks to facilitate industry self-regulation in two ways: first, by granting enforcement-related benefits (operators that comply with approved self-regulatory guidelines are deemed to be in compliance with the law); and, second, by allowing greater flexibility in the development of self-regulatory guidelines in a manner that takes into account industry-specific concerns and technological developments. FTC approval of a COPPA safe harbor program turns on whether self-regulatory guidelines (1) meet or exceed statutory requirements; (2) include an effective, mandatory mechanism for the independent assessment of compliance with the guidelines (such as random or periodic review of privacy practices conducted by a seal program or third-party); and (3) contain effective incentives to ensure compliance with the guidelines (such as mandatory public reporting of disciplinary actions, consumer redress, voluntary payments to the government, or referral of violators to the FTC).

In practice, the COPPA safe harbor programs have met with success mainly in terms of complementing FTC's own enforcement efforts.¹ But the COPPA safe harbor also suffers from two serious shortcomings: First, a very low rate of participation (presumably because deemed compliance is not a strong enough incentive to persuade many firms to bear the costs of joining a safe harbor program and abiding by its guidelines when they have to comply with all but identical statutory requirements in any case);² and, second, a lack of regulatory flexibility (all of the approved self-regulatory programs have nearly identical requirements to those of the COPPA statute).

¹ See FTC, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS (2007) 24; see also Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (forthcoming Winter 2011), 22-23 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275 (describing the success of the CARU safe harbor program, which over an eight year period investigated and successfully resolved almost 200 cases).

² See Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 20-23 (noting that fewer than 100 firms have been certified under approved COPPA safe harbor programs).

One way to build on the success of the COPPA safe harbor programs while overcoming these two shortcomings would be to adopt a more “co-regulatory” approach to privacy legislation, one in which industry enjoys greater scope in shaping self-regulatory guidelines, while government sets default requirements and retains general oversight authority to approve and enforce such guidelines. This approach envisions a more collaborative, flexible and performance-based model of self-regulation and explicitly draws on critical insights from environmental regulation.³

As noted above, COPPA safe harbor participants are subject to self-regulatory guidelines that are nearly identical to statutory requirements. Their incentives for joining are limited to deemed compliance and a largely empty promise of regulatory flexibility. In other words, COPPA failed in its efforts to treat safe harbor participants more favorably than other covered entities. In contrast, a co-regulatory approach would more effectively use both sticks and carrots as incentives. In the environmental setting, for example, sticks typically include a threat of stricter regulations or imposition of higher pollution fees, whereas carrots might take the form of more flexible regulations, recognition of better performance by the government, and cost-savings such as exemptions from mandatory reporting or easier and quicker permitting.⁴ Firms that demonstrate high performance avoid these sticks and/or enjoy these carrots. How would this approach translate into the privacy arena and why it might attract industry support at much higher rates than that of the COPPA safe harbor programs?

A New Approach to Privacy Safe Harbors

Over the years, many advocacy groups and privacy scholars have favored a private right of action and liquidated damages as enforcement mechanisms in any new privacy legislation. Not surprisingly, industry has argued that such remedies are both unnecessary and ineffective. This suggests that an excellent stick might be devised around a tiered liability system. Under this new approach, privacy legislation would allow civil actions and liquidated damages awards against firms that engaged in prohibited practices and did not participate in an approved safe harbor program. In sharp contrast, compliance with approved self-regulatory guidelines would not only serve as a safe harbor in any enforcement action but exempt program participants from civil law suits and monetary penalties. Other sticks for non-participating firms might include broader opt-in requirements; external and independent audits of regulatory compliance and mandatory reporting to the FTC; and much stricter requirements for firms engaged in online behavioral advertising such as a total ban on the use of sensitive information in behavioral targeting and a data retention limit of one month.

³ *Id.* at 28-36.

⁴ *Id.* at 23

In addition to these sticks, privacy legislation might also offer safe harbor participants a number of carrots including exemptions from civil actions and liquidated damages; cost-savings such as compliance reviews based on self-assessments rather than external audits by an independent third-party; government recognition of better performing firms (e.g., an FTC “seal of approval” under which firms that meet safe harbor requirements are duly recognized); government procurement preferences for the products or services of participating firms (including perhaps contracts for cloud computing services); and regulatory flexibility in the form of tailored requirements addressed to specific business models such as online behavioral advertising (e.g., relaxed notice and consent and/or data retention requirements for firms that engage in practices similar to those described in Section 3(e) of the Boucher bill).

In summarizing this new approach to privacy safe harbors, it bears repeating that safe harbor benefits would be limited to firms demonstrating superior performance and would not be available to other covered entities that merely satisfy default statutory requirements. In other words, a safe harbor provides incentives, in the form of sticks and carrots, but only to firms that meet higher performance standards based on data governance principles, advanced privacy methodologies, and best practices. What might such standards look like?

Data governance may be defined as “a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.”⁵ A good example of a data governance practice is appointing an individual (such as a Chief Privacy Officer) with overall responsibility for setting privacy protection policy and standards within a firm, managing risks and impacts of privacy-affecting decisions, publicizing within the company who has authority and accountability for governance decisions, and creating reporting mechanisms for both internal and external stakeholders about the status within the organization of such policy and standards.

Advance privacy methodologies include development guidelines for building privacy protection into any product or service that uses personal data. This process—which is sometimes referred to as “Privacy by Design”—implies that before releasing a new product or service, firms identify and address privacy issues using well-established techniques including data minimization, anonymization, access controls, and encryption and other security measures; create a privacy statement describing how personal data will be handled in response

⁵ See Data Governance Inst., *Defining Data Governance*, available at http://www.datagovernance.com/gbg_defining_governance.html.

to identified privacy concerns; and otherwise protect consumers' privacy by applying all relevant aspects of a robust set of Fair Information Practices (FIPs).⁶

Finally, industry-wide best practices include mandatory privacy training for all staff with privacy responsibilities, providing online guidance on privacy and security issues to employees and consumers, and implementing a complaint-handling procedure. Both of the bills under consideration today require safe harbor participants to adopt best practices. (In Section 3(e) of the Boucher-Stearns draft bill, however, the safe harbor provision is limited to online advertising firms; hence the focus instead is on *industry-specific* best practices.)

It is important to note that this is a very partial list of relevant performance standards. A more comprehensive list of potential standards is available in the previously mentioned article.⁷

Public Consultation Requirement

In thinking about this new approach to privacy safe harbors, two additional caveats are necessary: First, unlike previous or existing self-regulatory schemes, it would not suffice for industry alone to develop the relevant privacy performance standards or best practices. Rather, such standards must emerge from a multi-stakeholder process in which both advocacy groups and members of the public have an opportunity to participate. This requires that interested parties engage in difficult and perhaps protracted negotiations, and stay at the table until a consensus is forged.⁸ Second, the government must reserve the final decision on whether the performance standards or best practices achieve a high enough level of privacy protection to warrant the granting of any proposed safe harbor benefits.

The COPPA safe harbor relies on a notice and comment procedure to approve proposed self-regulatory guidelines, but it is worth considering two alternative options that meet both of the above caveats. The first is negotiated rulemaking, a statutorily defined process by which agencies formally negotiate rules with regulated industry and other stakeholders as an alternative to conventional, notice and comment rulemaking.⁹ In theory, negotiated rulemaking

⁶ See, e.g., U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (identifying eight principles: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability and auditing).

⁷ See Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 49-50.

⁸ This may seem impracticable, but three leading Internet firms recently partnered with a diverse group of non-governmental actors in a voluntary effort to negotiate free speech and privacy principle. After eighteen months of work, this multi-stakeholder group reached agreement and launched the Global Network Initiative (GNI), jointly committing to a set of principles and implementation guidelines as well as an accountability system based on independent, third-party assessments. For the GNI's three core commitment documents, see <http://www.globalnetworkinitiative.org/index.php>.

⁹ See the Negotiated Rulemaking Act of 1990, codified as amended at 5 U.S.C. §§ 561-570.

reduces cost and other regulatory burdens by developing alternative or innovative means of compliance not permitted under a statute's default requirements, thereby allowing industry more flexibility as to the timing of compliance investments, and reducing regulatory uncertainty. The incentives for regulators and advocacy groups to support this approach include the prospects of a higher level of benefits than would have been obtained, as a practical matter, under the standard default requirements.¹⁰

Negotiated rulemaking is most likely to succeed when two additional conditions are present: First, the regulatory agency should understand the industry and the issues well enough to have formulated a broad view of what a good regulatory solution should look like but it should not be wedded to a particular substantive outcome. Second, the substance of the regulation should require the credible transmission of information between the regulated entities and other interest groups--i.e., industry should possess unique knowledge and expertise such that it is in the best position to understand how regulation will affect its activities. Hence, industry cooperation is needed to ensure a satisfactory regulatory outcome.

Arguably, the present case satisfies both of these conditions. On the one hand, the FTC is very knowledgeable regarding online privacy but is not yet locked-in to any one approach. On the other, Internet firms (including network advertising firms) undoubtedly possesses greater expertise and insight into the complex technology and evolving business models underlying the digital world than either privacy advocates or FTC staff. In the past, this information has been shared or elicited mostly through one-sided communications—unilateral industry codes of conduct; complaints filed with the FTC; or charges and countercharges at public forums. In a (successful) negotiated rulemaking process, however, the parties have an incentive to educate each other, pool knowledge, and cooperate in problem solving.

That said, negotiated rulemaking is not always appropriate and imposes heavy burdens on participants in terms of time and other resources. With these burdens in mind—and especially their impact on the FTC's relatively small Division of Privacy and Identity Protection—I would like to propose an alternative to negotiated rulemaking that both addresses potential resource concerns while ensuring that the safe harbor approval process establishes a role for advocacy groups and the public.

In a nutshell, this second alternative consists in a two-step process for approving privacy safe harbors. In Step 1, safe harbor program sponsors would have to submit to the FTC a short initial proposal showing that they have met statutorily defined criteria (see below). FTC would

¹⁰ See Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, pp. 44-46.

then have 45 days to conduct a fairly perfunctory review designed to determine if these criteria were met. If not, FTC would issue a preliminary denial and the sponsor would have to wait twelve months from the FTC decision before submitting a revised proposal; if so, FTC would issue a preliminary approval and the sponsor would then proceed to Step 2. The criteria for approving an initial proposal might include the following:

- The sponsor is representative of an industry sector. (This is intended to discourage applications from firms that wish to sponsor a safe harbor program merely as part of a business plan, rather than due to their industry role or subject matter expertise);
- The sponsor has industry support as indicated by endorsements from leading members of the industry (defined in terms of size, revenue, influence, etc.);
- The sponsor's proposed program advances broad goals such as consumer protection, cost savings, and innovation;
- The sponsor has drafted self-regulatory guidelines addressing all of the core statutory requirements of a safe harbor program.¹¹

Upon approval of an initial proposal, the sponsor would then have up to 180 days to submit a more detailed application for approval, which FTC would review and approve within 180 days using a conventional rulemaking process. Step 2 would require the sponsor to submit a more comprehensive program description demonstrating that the program meets or exceeds all relevant safe harbor requirements. In addition, the sponsor would have to show that it continues to have substantial industry support (e.g., by listing the names of the firms that have expressed an interest, in writing, in participating in the program) and that it has engaged in stakeholder consultation. This would require the sponsor to include in its formal application a statement describing who is affected by the proposed safe harbor guidelines, efforts it has taken to consult with affected groups (including consumer or advocacy groups), changes to the proposed safe harbor guidelines resulting from these consultations (if any), a summary of any issues that remain unresolved and why (including any concerns raised by the FTC), and that the public consultation remained open for at least 60 days.¹²

¹¹ This assumes that FTC would engage in a rulemaking procedure defining industry representation, consumer benefits, cost savings, and innovation.

¹² The Network Advertising Initiative recently engaged in a public consultation along these lines when it released a draft update to its original NAI Principles, solicited public comments on the proposed changes, and published both the comments and its responses. See NAI, NAI PRINCIPLES 2008: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT FOR ONLINE BEHAVIORAL ADVERTISING (Apr. 2008), available at http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf. Under the process described in the text, however, FTC would retain final approval authority if it decided the NAI guidelines were inadequate notwithstanding a satisfactory public consultation.

Step 1 of this alternative process is meant to discourage the submission of weak applications by entities lacking industry expertise or support. It also dispenses with the need for FTC to work with sponsors on improving inadequately designed programs.¹³ FTC would review the initial proposal mainly to ensure that it is approvable subject to meeting the more formal requirements of Step 2. But if the program is inadequate on its face, FTC would simply deny the initial application and impose the 12-month waiting period. Step 2 requires industry to reach a rough consensus with advocacy groups and respond to any major concerns or to explain why this is infeasible. Although FTC is not required to approve a program merely because industry demonstrates good faith efforts in the consultation process, the idea is that by requiring a rough consensus, the consultation process will result in better quality guidelines with greater legitimacy for everyone involved. The overall goal is to ensure that FTC devotes its limited resources to reviewing programs that have already demonstrated a high likelihood of success.

Comments on the Safe Harbor Provisions of the Two Bills Now Under Consideration

When Congress last seriously considered online privacy legislation about ten years ago, bills introduced by Reps. Markey, Sens. Burns and Widen, Rep. Stearns, and Sen. Hollings provided for a comprehensive, self-regulatory safe harbor modeled on COPPA.¹⁴ Like these earlier bills, both of the bills under consideration today include safe harbors but of very different scope and import. Section 3(e) of the Boucher bill creates a limited safe harbor for advertising networks that track online behavior. It exempts these networks from having to obtain explicit, opt-in consent provided they allow consumers to access and manage their profiles.¹⁵ A coalition of consumer groups has objected to this provision on the grounds that it relies on the discredited notice-and-choice model, which they consider ineffective for ensuring

¹³ The privacy safe harbor might also include a provision encouraging or requiring FTC to convene a privacy workshop at least once every 5 years, where it would consider recent developments in privacy and technology and to issue a report on how best to improve privacy regulation. One goal of these workshops (which would resemble the most recent FTC Privacy Roundtables) would be to identify industry sectors that are “ready” for safe harbor programs, thereby encouraging such groups to submit initial proposals.

¹⁴ See the Electronic Privacy Bill of Rights Act of 1999, H.R.3321, 106th Cong. § 4 (1999); the Online Privacy Protection Act of 1999, S. 809, 106th Cong. § 3 (1999); Consumer Privacy Protection Act of 2002, H.R. 4678, 107th Cong. §106 (2002); the Online Personal Privacy Act, S. 2201, 107th Cong. § 203 (2002).

¹⁵ More specifically, the requirements for “individual managed preference profiles” under Section 3(e) are as follows: (1) users must be provided with a readily accessible opt-out mechanism whereby the opt-out choice of the individual is preserved and protected from incidental or accidental deletion; (2) firm must delete or render anonymous any covered information not later than 18 months after the date the covered information is first collected; (3) firms must place a symbol or seal in a prominent location on both its website and on or near any ads it delivers based on a user’s preference profile that enables an individual to connect to additional information regarding advertising practices and allows individuals to review and modify, or completely opt out of having, a preference profile created and maintained by the firm or a an ad network; and (4) any ad network to which a firm discloses covered information must avoid further disclosure to any other entity except with the user’s express affirmative consent.

online privacy.¹⁶ In my view, the more fundamental problem with this approach is its narrowness and inflexibility. Section 3(e) enshrines a single program already adopted by several companies engaged in targeted advertising (including Google and Yahoo, both of whom already allow users to access and revise their profiles). But the Boucher bill lacks a more general safe harbor provision that would encourage other companies (and other sectors) to offer innovative privacy protections or adopt industry-specific best practices.

In contrast, Title V of the Rush bill provides a full-fledged safe harbor under which any self-regulatory program (referred to as a “Choice Program”) may qualify for certain exemptions provided the programs meet the following five requirements:

- A “universal” opt-out mechanism and preference management tool that applies an individual’s choices to all firms participating in the Choice Program;
- Guidelines and procedures that offer equivalent or greater protections than those required in Title I (transparency, notice and individual choice) and Title II (accuracy, access and dispute resolution);
- Approval procedures for participating firms;
- Procedures for periodic self-assessment and random compliance testing; and
- Consequences for failure to comply with program requirements.

Firms that participate in and comply with an approved Choice Program meeting these requirements are exempted from (1) the express affirmative consent requirements under subsection 104(a); (2) the access requirement under section 202(b); and (3) liability in a private right of action brought under section 604.

In my opinion, the Choice Program is preferable to the limited exemption for individual managed preference profiles for several reasons. First, and obviously, it is more comprehensive and therefore allows companies in any sector to develop innovative privacy protections or adopt industry-specific best practices. Second, it relies on a good mix of carrots and sticks including tiered liability. However, in order to meet the basic test of any safe harbor--which is that program participants are entitled to better treatment based on superior performance--the Choice Program needs strengthening in several areas. To begin with, it needs to clarify that safe harbor approval depends on compliance not only with Titles I and II but also with Title III (security, data minimization and accountability). I would also support the addition of several new elements to the list of requirements for self-regulatory programs including (a) procedures for handling and reporting on consumer complaints; and (b) guidelines for requiring

¹⁶ See Letter from Jeff Chester, Center for Digital Democracy, et al., to Reps. Rick Boucher and Cliff Stearns (June 4, 2010), available at <http://www.democraticmedia.org/files/u1/2010-06-letter-to-boucher.pdf>.

participating firms to build privacy protection into their products or services using “privacy by design” or related methods and techniques.

Recommendations and Conclusion

First, Congress needs to enact comprehensive privacy legislation incorporating the full range of Fair Information Practices.

Second, this legislation should include a broad-based safe harbor program based on a co-regulatory approach that provides flexibility to industry in shaping self-regulatory guidelines in exchange for superior performance, while ensuring that the FTC retains general oversight authority to approve and enforce such guidelines.

Finally, this safe harbor program should be amended to include a complaint handling process and privacy by design requirement; it should also require public consultation as part of the safe harbor approval process, which might consist in negotiated rulemaking or the two-step application process as described above.

Section 3(e) of the Boucher-Stearns discussion draft and the Choice Program as set out in Title IV of H. R. 5777 are important first steps in developing a new approach to safe harbors but should be expanded in various ways as discussed above.

I want to thank you again for the opportunity to appear before the Committee today. I will be pleased to answer your questions and would be happy to provide any further assistance as appropriate.