http://op.bna.com/pl.nsf/r?Open=dapn-8nfn64 (as of Oct. 31, 2011) [hereinafter Kerry-McCain Bill].

Children's Online Privacy Protection Act (COPPA) authorizes safe harbors, and the EU-U.S. Safe Harbor Agreement is grounded in this approach. But the COPPA safe harbor provision is little utilized,[5] and the EU-U.S. Safe Harbor Agreement remains controversial due to questions about compliance and enforcement.[6] Should the proposed bills give such a prominent place to safe harbors? What are pros and cons of this approach? What has experience taught us about it?

The authors of this article have conducted research on privacy safe harbor programs. Professor Rubinstein has written about the COPPA Safe Harbor Program and the EU-U.S. Safe Harbor Agreement.[7] Professor Hirsch recently completed a Fulbright Professorship in the Netherlands where he studied the 20-year Dutch experiment with privacy safe harbors. Here, we draw on this knowledge to shed light on the current safe harbor proposals and to suggest how Congress can best build this approach into consumer privacy legislation. We begin with a brief review of the potential advantages, and risks, of co-regulatory safe harbors. We then explain how to design the legislation so that it maximizes the advantages, and minimizes the risks, of this approach.

The Safe Harbor Approach: Advantages and Risks

Policymakers seeking to develop privacy regulations for the information economy face a daunting challenge. Technologies, organizational processes and business models in these industries are so varied, and change so rapidly, that regulators often have a hard time keeping up with current developments or anticipating future ones. By contrast, industry has far more intimate knowledge of its current technologies, business arrangements and future plans. In order to regulate effectively—to develop rules that correspond to business reality and achieve regulatory goals—government must gain access to this industry knowledge. Yet traditional rulemaking often discourages this. It sets up an adversarial dynamic in which interested parties adopt extreme positions and suppress relevant information in an attempt to push regulators towards their own position. This is not conducive to open dialogue and the sharing of information.

The main advantage of the safe harbor approach is that it seeks to change the rule-drafting process from an adversarial, advocacy-based model, to a collaborative, cooperative one, and so to promote the vital exchange of information between industry and government. Industry itself creates the first draft of the rules that implement the statutory requirements. It then shares and negotiates this draft with government regulators. The hope is that this new dynamic will encourage regulated entities to draw on their superior knowledge and share critical information with regulators. Where this occurs, it can yield rules that are more tailored to industry realities, more workable, and more effective at pro-

Safe Harbor Programs: General Considerations

S . . . . . . Ideally, the scope of a safe harbor program should cover all of the substantive requirements in privacy legislation. This approach permits industry to share information, tailor rules to fit industry-specific needs, and devise innovative solutions across the entire range of FIPPs as expressed in the bill's privacy requirements. The Stearns Bill takes this comprehensive approach. *S* Stearns Bill § 9(c)(1). In contrast, both the Rush Bill and the Kerry-McCain Bill take a partial approach by excluding certain statutory provisions from the safe harbor.[9] We think this partial approach is mistaken and that the underlying rationale of co-regulation applies equally to all of the substantive requirements in a privacy law. Ideally, Congress would follow a more comprehensive approach although as a practical matter it may be necessary to exclude certain provisions from the ambit of a safe harbor program due to resource constraints (which are discussed further below).[10]

E . . . . . As noted above, a safe harbor program may be broad or narrow in scope. In either case, the program should incorporate privacy protections that are the same as, or at least the equivalent of, any statutory privacy protections for which safe harbor treatment is granted. This language is broadly consistent with that found in the proposed bills.

This limitation avoids inconsistent interpretations of statutory requirements and prevents companies from forum shopping. Of course, companies outside the jurisdiction of the FTC (such as many types of financial institutions, airlines, telecommunications carriers and a few others) would be ineligible for safe harbor participation, if, as expected, the FTC were the approving agency.

P . . . . Under a sectoral approach, any organization should be able to act as a program sponsor provided it submits an application on behalf of an industry sector and demonstrates that it is representative of that sector. It should also show sufficient in-

upon the program sponsor to satisfy the public consultation requirement as set forth above.

As to the timing of consultations, we recommend that industry-agency consultation occur before any stakeholder consultations. If all stakeholders are included in the first phase of discussions the risk is that industry will be less willing to openly share information with regulators, whereas if industry-agency consultations occur before stakeholder consultations, this should help preserve the information sharing function, which is a key rationale of safe harbor programs. Consultation with stakeholders would be required but would occur after the initial conversations between industry and government.

Application and Approval

In designing its application and approval criteria, Congress should take into account the COPPA safe harbor experience. Under COPPA, the FTC issued specific application and approval criteria.[20] The Commission described these criteria as ''guidelines'' and ''performance standards'' that allowed programs to come up with their own, equally protective, alternatives. But the safe harbor programs did not treat them this way. Instead, most of them adopted the Commission's template. They produced rules that contained little individuality, largely failed to account for particular industry realities, and provided few innovations.[21] The COPPA experience demonstrates the difficulty in designing application and approval criteria. On the one hand, Congress needs to create a structure that will allow only those safe harbor programs that correctly embody statutory requirements to gain approval. On the other, it needs to avoid imposing, or having an agency impose, the kind of detailed application and approval criteria that will stifle tailoring and innovation. In this section, we recommend how Congress can achieve this balance.

F . Congress should not prescribe the specific form of a safe harbor application. It should adopt language similar to that currently found in the Stearns Bill, which provides that an agency should accept applications in ''any reasonable form.'' *S* Stearns Bill § 9(b)(2).

C . Congress should specify two types of approval criteria: threshold criteria that every safe harbor program must meet before the agency will even consider it for approval; and substantive criteria that will inform the agency's substantive evaluation of a given application. The threshold criteria should be more tightly worded. The substantive criteria should be written in broad language that allows for individual program differentiation and innovation.[22] Congress should instruct the agency first to evaluate the threshold criteria and, only if the applicant meets them, to move on to the more substantive evaluation. This will conserve agency resources and make sure that only bona fide safe harbor applications receive full consideration.

T . Each applicant must demonstrate that:

- It represents a sufficient number of the companies in its sector, and the companies it represents have expressed their support for the proposed safe harbor program rules.
- Both larger established companies, and smaller and newer firms, were involved in the drafting of the safe harbor program rules and are represented in the program's leadership.
- The applicant has consulted with stakeholders and has reported on the results in accordance with the public consultation requirement set out above (The Network Advertising Initiative (NAI) followed a similar approach when it revised its code of conduct for online behavioral advertising (OBA) in 2008.).
- The safe harbor program includes a process for handling individual complaints.
- The safe harbor program possesses sufficient resources to carry out its duties and observes basic corporate formalities such as the passage of bylaws and the appointment of a Board of Directors.
- The program will allow firms to participate only if they agree to remain in the program for a substantial period of time.

S . If the applicant meets the threshold criteria, then the agency should further consider the substantive merits of the program. The agency should approve the application if the safe harbor program rules:

- offer protection that is ''at least the equivalent of'' statutory requirements (This language will allow a degree of innovation while still ensuring that program rules provide Congress's desired level of protection.);
- do not violate any statutory requirement;
- incorporate industry knowledge about business practices and emerging technologies and use this knowledge to tailor the rules to industry realities;
- contain and/or promote continued innovation in the protection of personal information and consumer control over such information (*S* Rush Bill § 404(4));
- allow for and promote cost-effective compliance;
- incorporate stakeholder comments made during the public consultation process or offer a reasonable explanation as to why they are not doing so; and
- do not create unnecessary barriers to entry for new firms. The agency may consult with competition authorities in assessing this.

A . Congress should establish a formal process by which the agency will consider safe harbor

---

expression and privacy on the internet under the banner of Global Network Initiative (GNI). *S* Rubinstein, note 5, at 402-04.

[20] Children's Online Privacy Protection Rule § 312.10, 64 Fed. Reg. 59,888, 59915 (Nov. 3, 1999).

[21] *S* Rubinstein, note 5 at 398-99.

[22] The Kerry-McCain and Rush Bills pay particular attention to the online behavioral advertising sector. They direct the FTC to issue regulations that spell out what a safe harbor program for this sector must contain. *S* Kerry-McCain Bill, § 501(a)(2)(A); Rush Bill, § 404(2). We believe that Congress should not direct an agency to issue detailed safe harbor program approval criteria. However, in light of the proposed bills, we recognize that Congress may have more defined ideas20

program applications. This process should require the agency to:

- respond to applications by issuing a written decision that sets out the agency's reasons for approving or disapproving the application (*S* Kerry-McCain Bill § 501(b)(4));
- issue its written decision pursuant to a notice-and-comment rulemaking processes (*S* Rush Bill § 402(a));
- comply with time limits for the review of applications and issuance of approvals or denials;[23]
- before rejecting an application, communicate any deficiencies to the applicant and give it a period of time (30 days) to submit a revised application; and
- revoke its approval upon a finding that the safe harbor was approved based on false or incomplete information or that the safe harbor organization has materially failed to meet its obligations as specified in its application, the statute, or in agency rules (*S* Stearns Bill § 9(b)(4)).

J . . . . . CongrKerryitsCong9(b)t03sew.

of action against covered entities for non-compliance with the statute. Where a covered entity in a safe harbor program then the agency would not directly enforce the statute. Instead, it would enforce the statute as interpreted by the relevant, approved safe harbor program. Firms that complied with such programs would be deemed to be in compliance with the statute. This is necessary for the program or code to serve as a legal ''safe harbor.'' Where a covered entity in a safe harbor program, the agency would enforce the statute directly against the non-participant. It is important that the agency have this power. Without it, covered entities will be able to ''free-ride'' on the responsible practices of others.[28]

During the implementation of the EU-U.S. Safe Harbor Agreement a number of firms falsely represented that they were members of a safe harbor program when, in fact, they were not.[29] This kind of misrepresentation can severely damage the credibility and effectiveness of a safe harbor program. Congress should provide that those who falsely represent that they are members of safe harbor program will be subject to enforcement and civil penalties. See Stearns Bill § 9(f).[30]

Global Interoperability

Congress may be able to use safe harbors as a way to harmonize U.S. privacy law with the European Union and APEC regimes. Both the EU and APEC systems allow industry to generate a set of rules that will satisfy all national governments in the region. In the European Union, this is known as a Community Code (a code of conduct that applies throughout the European Community). It must be approved by the Article 29 Working Group.[31] Under the APEC system, a firm develops ''cross-border rules'' that must be consistent with the APEC privacy principles.[32] An Accountability Agent (third-party certifier) must certify the firm's cross-border rules and its compliance with them.[33]

To achieve global interoperability, a U.S. sector could develop a safe harbor program (or code of conduct) that satisfied not only the U.S. statutory requirements but also the requirements of the EU's 1995 Data Protection Directive and the APEC Privacy Principles. It would then, simultaneously, submit the program/code to the U.S. agency for approval; to the Article 29 Working Group for approval; and to an APEC Accountability Agent for certification. Assuming that it received all three approvals, the sector's program/code would constitute a set of rules that were accepted in the United States, the European Union, and the APEC member economies. Firms that followed such rules could enjoy an international, and nearly global, safe harbor.

Agency Resources

There is no denying that privacy safe harbor programs require additional agency staff and resources to handle additional tasks such as a rulemaking, addressing program requirements and procedures (including both audits and establishing the criteria for approving third parties as auditors), review and approval of proposed safe harbor programs and proposed auditors, and review and responses to both self-certifications and complaints, quite possibly resulting in additional enforcement activity. All of this new activity will require new funding. In these times of severe budget cuts and fiscal constraints, it would be highly desirable if a new privacy law required no additional expenditures. But this goal seems unattainable, especially when the safe harbor provisions we have described in this article require FTC and Commerce to assume new responsibilities. We believe the benefits of the safe harbor approach more than justify such expenditures. On the other hand, it would be highly undesirable to enact a safe harbor program without appropriating the necessary funds to establish new procedures, oversee third-party audits, and engage in enforcement activities as required. *I* - . It would encourage abuses ranging from inadequate and self-interested codes of conduct, to participating firms ignoring their responsibilities under industry codes without penalty.

Conclusion

This article has recommended how Congress can best incorporate the safe harbor approach into its current legislative proposals. These recommendations draw from, and are grounded in, our research on prior initiatives of this type. They seek to maximize the advantages, and minimize the risks, associated with safe harbors. We recognize that there are many ways to design a successful safe harbor program. We invite reactions to this article and welcome opportunities to discuss it with others interested in this important topic.

---

[28] The accountability and enforcement program should focus on covered entities, not on the organizations that establish and administer the safe harbor programs. Still, the agency should conduct some supervision of the safe harbor programs. *S* Kerry-McCain Bill § 501(d). If it finds that the safe harbor program sponsor is not adequately performing its statutory responsibilities, it should withdraw its approval of that program.

[29] In 2009, the FTC brought suit against a California company for falsely claiming, in its privacy policy, that it was certified under the SHA when in fact it was not. *S* http://ftc.gov/opa/2009/08/bestpriced.shtm. A few months later, the FTC announced proposed settlements in six more false claims cases. *S* http://www.ftc.gov/opa/2009/10/safeharbor.shtm. Moreover, two independent studies of the SHA found that many participating firms did not incorporate all seven of the agreed-upon SHA privacy principles in their own posted privacy policies. See Rubinstein, note 5, at 392-93.

[30] The FTC has been slow to take action in these false claims cases. *S* Rubinstein, note 5 (noting that the FTC waited nine years before bringing any enforcement actions against firms participating in the SHA). The current legislation should not allow for this experience to be repeated. It should instruct the FTC to take the steps necessary to detect and enforce against misrepresentations, and should provide it with the resources to do so. It could also specify liquidated damages for firms that misrepresent their membership in a safe harbor program.

[31] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31, art. 27(3).

[32] *S* note 27.

[33] *S* APEC Plan, note 27.