BNA

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 1639, 11/14/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Better Safe Than Sorry: Designing Effective Safe Harbor Programs for Consumer Privacy Legislation

By Dennis D. Hirsch and Ira Rubinstein

Introduction

Congress is getting ready to take an innovative, cooperative approach to regulation and make it a centerpiece of U.S. privacy law. Three bills currently before Congress would, if enacted, regulate comprehensively the commercial use of personal information. Each of these pieces of legislation—the Kerry-McCain Bill,[1] the Rush Bill,[2] and the Stearns Bill[3]—would employ a ''safe harbor'' program[4] in which the government and the private sector would collaborate on the drafting of rules to govern industry practices.

Under the safe harbor approach, Congress would legislate broad privacy requirements for commercial entities. An industry association or other nongovernmental organization (NGO) would then draft implementing rules (sometimes called a ''code of conduct'') that would spell out how these broad requirements applied to a particular sector or set of firms, and would submit these rules to a regulatory agency, which under all three of the bills would be the Federal Trade Commission. The agency would review the rules and, if it believed that they correctly embodied the statutory requirements, approve them. Firms that followed an approved set of rules would be in compliance with the statute and would enjoy a legal ''safe harbor.'' Some have referred to safe harbor programs as a form of ''co-regulation'' since governmental and private actors expressly and intentionally share responsibility for producing the rules that guide company behavior.

This is not the first time that the United States has used safe harbors in the area of privacy regulation. The

[1] Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. (2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8nfn64 (as of Oct. 31, 2011) [hereinafter Kerry-McCain Bill].

[2] Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act (''BEST PRACTICES'' Act), H.R. 611, 112th Cong. (2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8nfnb6 (as of Oct. 31, 2011) [hereinafter Rush Bill].

Dennis D. Hirsch is the Geraldine W. Howell Professor of Law, Capital University Law School, Columbus, Ohio. Ira Rubinstein is an Adjunct Professor of Law and Senior Fellow, Information Law Institute, New York University School of Law.

[3] Consumer Privacy Protection Act, H.R. 1528, 112th Cong. (2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8nfnd6 (as of Oct. 31, 2011) [hereinafter Stearns Bill].

[4] Kerry-McCain Bill tit. V, §§ 501, 502; Rush Bill tit. 4, §§ 401-404; Stearns Bill § 9. The Stearns Bill refers to the initiative as a ''Self-Regulatory Program'' but sets out a scheme that is conceptually indistinguishable from a safe harbor program. *See* Stearns Bill § 9(a)(1) (providing for a ''Presumption of Compliance''). The Department of Commerce, in its 2010 Privacy Green Paper, sets out a similar approach that it calls ''voluntary, enforceable codes of conduct.'' *See* Dept. of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* 41 (2010), *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf [hereinafter Dept. of Commerce]. We will use these three terms—''safe harbor program,'' ''self-regulatory program,'' and ''voluntary, enforceable codes of conduct''—interchangeably and will refer to them as safe harbor programs.

COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1538-3423

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 protecting personal information than traditional regulations. Moreover, by encouraging industry to come up with designs or processes for protecting personal information, the safe harbor approach can potentially yield more creative and cost-effective approaches to privacy protection. The approach can also produce other advantages. The very process of drafting safe harbor rules forces companies to examine their own data practices and so to learn how their actions affect privacy. This can enhance firms' awareness of their privacy impacts. Safe harbor programs can also give businesses a sense of ownership over rules that they or their peers helped to create and so foster better acceptance of and compliance with these rules. Finally, the safe harbor approach can yield administrative efficiencies since private sector representatives, not agency regulators, take on the task of producing the rules in the first instance.

The safe harbor approach also poses some significant risks. Private sector organizations may draft rules that favor industry interests over those of the public. Industry-government negotiations over these rules can be less transparent, and allow less public participation, than traditional, notice-and-comment rulemaking and so may not serve as a sufficient check on the process. This can lead to rules that are too lenient and that do not adequately protect personal information. Another risk is that established companies will come to dominate the drafting process and seek to craft anti-competitive rules that create barriers to entry for new firms. Another is that privacy advocates may feel excluded from the process and resist the rules that it produces. Practical difficulties can also arise. Industry associations or other NGOs may not step forward in sufficient numbers to initiate safe harbor programs. This can delay the rule-drafting process. Even where groups do come forward to draft the rules and initiate the programs, some firms may decide not to participate in them and may, instead, seek to ''free-ride'' on the efforts of their peers. Finally, regulatory agencies with limited resources may find it difficult to administer and monitor compliance with safe harbor programs.

The remainder of this article draws on our research on existing programs to recommend how federal privacy legislation can design safe harbor programs in a way that maximizes the advantages of this approach, and minimizes the risks. It first addresses some general issues related to the design of safe harbor programs. It then proceeds step-by-step through the safe harbor process—from drafting, to application and approval, to monitoring and enforcement—offering analysis and recommendations at each step. It assumes that Congress will pass a comprehensive privacy statute that contains broad requirements based on Fair Information Practice Principles (FIPPs).[8] It further assumes that, in such legislation, Congress will rely, at least in part, on safe harbor programs to generate the rules necessary to implement and flesh out these broad requirements.

[5] *See* Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 63 I/S: A Journal of Law and Policy for the Information Society 356, 399 (2011) [hereinafter Rubinstein].

[6] *Id.* at 392-94.

[7] *Id.*

[8] Each of the three bills mentioned above contain such requirements. This is a good thing. In the absence of a baseline privacy law, voluntary codes of conduct are often incomplete and simply omit privacy requirements that their members find overly burdensome. *See* Rubinstein, *supra* note 5 at 388-90 (discussing weaknesses in the Network Advertising Initiative's (NAI) privacy principles); Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 Seattle L. Rev. 439, 460-64 (2011) [hereinafter Hirsch] (same).

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

Safe Harbor Programs: General Considerations

Scope of safe harbor programs. 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. *See* 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]

Equivalency standard and deemed compliance. 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.[11]

The phrase ''at least the equivalent of'' is intended to provide flexibility to safe harbor programs in choosing the means by which they will meet the statutory requirements. Should a safe harbor program adopt an original approach to achieving the statutory requirements, it should include with its application for safe harbor approval a statement identifying and explaining how its approach is at least the equivalent of the protections set out in the statute.[12]

When an agency approves a safe harbor, it should make a formal equivalency finding to forestall any legal challenges to the validity of favorable treatment under any applicable deemed compliance provisions. It follows that if the agency approves a safe harbor program, and a firm complies with the terms of a safe harbor, but an individual nonetheless brings a suit against the firm for failure to comply with the privacy statute (assuming the bill allows a private right of action), the equivalency finding would serve as a defense in a motion to dismiss.

Participants and sponsors. Participation in safe harbor programs may be sectoral or open-ended—i.e., limited to firms in an industry sector or open to all firms regardless of sector.

We favor a sectoral approach for three reasons. First, the sectoral approach is more consistent with the overall advantages and justification for safe harbors. Safe harbor programs designed on a sectoral basis may draw on a sector's knowledge of its own business realities and technology—something it knows better than regulators. This includes knowledge that firms in the sector, and a sectoral NGO, bring to the table. By contrast, if a broad-based NGO can draft a code of conduct that any firm may follow regardless of sector, then there is no reason to think that the NGO will bring any particular knowledge or expertise to the process. Second, broad-based NGO's, which have little knowledge of their members' businesses, will be more likely to depend on agency expertise (thereby draining agency resources) and will not add as much value. Research on COPPA safe harbor programs supports this conclusion: Organizations with extensive experience in children's advertising issues proved to be more self-sufficient in devising and managing safe harbor programs and gaining FTC approval than organizations that lacked this particular expertise, and the latter also required more FTC resources.[13] Third, the Dutch and other European code of conduct/safe harbor programs all operate at the sectoral level. The Dutch alone have negotiated codes of conduct with more than a dozen sectors, including banking, pharmaceuticals, direct marketing, and others.[14] This experience suggests that it is both feasible and useful to design safe harbor programs at the sectoral level. However, the FTC should approve only one program per sector, which is also the Dutch practice.

---

[9] Section 403(2)(d) of the Rush Bill excludes Title III (data security, data minimization, and accountability), while Section 502(a) of the Kerry-McCain Bill excludes Title I (security, accountability and privacy-by-design).

[10] While some of the bills are more comprehensive than others, all of them seek to apply the safe harbor approach to the sharing of personal information with third parties for online behavioral advertising (OBA) and other purposes. This raises the question of whether a statute should treat advertising or marketing safe harbor programs separately from safe harbor programs for other sectors. There are two ways a bill might approach this. First, Congress could set out the requirements for establishing sectoral safe harbors in general terms. It could then identify, or authorize a regulatory agency to identify, those sectors (such as the online advertising sector) that would benefit from a code of conduct. If an identified sector failed to act or develop a code that the agency rejected, Congress would authorize the agency itself to develop default rules applying the statute to the sector in question. Both the United Kingdom and Ireland provide this authority in their own code of conduct/safe harbor programs. *See* Hirsch, *supra* note 8, at 477-78 & nn. 267-68 (describing these two approaches). Second, Congress could mandate that a specific sector (such as online advertising) draft a code of conduct. It would not only define sectoral safe harbors in broad terms, but would also identify the statutory requirements that this particular sector would have to address to win approval of a code of conduct. Either of these approaches would allow a variety of sectors (gaming sites, mobile application providers, social media services, etc.) to develop codes. We do not recommend that Congress limit its safe harbor program solely to online advertising as this would severely reduce the coverage of safe harbor programs and thereby sacrifice the opportunity to apply the co-regulatory approach more broadly.

[11] *See* Kerry-McCain Bill § 501(b)(3) (providing that safe harbor program rules must provide protection that is ''substantially equivalent to or superior to the protection otherwise provided under this Act''); Stearns Bill § 9(c)(1) (requiring that a program provide ''substantially equivalent or greater protections'' than those that the statute imposes).

[12] This equivalency standard implies that any deemed compliance provisions benefiting safe harbor participants must match the scope of the industry code of conduct. In other words, if the code of conduct only addresses substantive requirements in Title I and Title II of a bill but not in Title III, then deemed compliance would extend only to Title I and Title II, but not to Title III.

[13] *See* Rubinstein, *supra* note 5.

[14] *See* http://www.dutchdpa.nl/Pages/en_ind_cbp_taken_gedrag.aspx; (describing the sector-based code of conduct approach); *see also* http://www.cbpweb.nl/Pages/ind_wetten_zelfr_gedr.aspx; (providing links to codes for particular sectors).

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.

Program sponsorship. 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 industry interest in the form of firms that have indicated preliminary support for drafting a code of conduct and participating in a safe harbor program. These criteria may be defined more precisely as part of any agency rulemaking needed to implement a statutory safe harbor. The purpose of these qualifying criteria is two-fold: first, to allow both existing trade associations and newly formed NGOs to qualify as sponsors provided they have sufficient support; and, second, to create a gatekeeping mechanism that would limit the number of potential program sponsors and thereby preserve agency resources. The Dutch code of conduct program follows this approach. It requires that the drafters of a code of conduct be ''sufficiently representative'' of the sector.[15] As a result, trade associations and other experienced sectoral organizations have drafted and submitted most of the codes. This contrasts with COPPA, which did not restrict sponsors and thereby attracted applications from newly formed businesses with limited expertise or industry support.

Incentives to participate. Prior safe harbor programs have found it difficult to attract sufficient participation, e.g., fewer than 100 firms have signed up for the four approved programs under COPPA. This weak participation may be overcome by designing appropriate incentives, which may be divided into carrots and sticks. *Carrots* might benefit participating firms by allowing them to:

- display a seal indicating membership in a safe harbor program (*See* Stearns Bill § 9(c)(4));
- have an opportunity to cure potential violations and enjoy reduced civil penalties (*See* Rush Bill § 603(b)(4));
- not be subject to any private right of action (*See* Rush Bill § 401(3)); and
- enjoy beneficial treatment under any monitoring and/or audit requirements (For example, in deciding which entities to inspect the agency could find that a participant's membership in a safe harbor program makes it less of a compliance risk and so give it a lower inspection priority. Alternatively, participants in safe harbor programs could be subject to less frequent third-party audits than non-participants.).

On the other hand, *sticks* might burden non-participating firms by subjecting them to:

- the uncertainty of FTC enforcement of broadly written statutory requirements without the benefit of more detailed, industry-tailored codes;
- an agency determination that a given sector should develop a code and that if it fails to do so, the agency would develop applicable rules and impose them on that sector (*See supra* note 10);
- increased inspection and compliance burdens, such as more frequent third-party audits, and higher risk of enforcement actions;
- higher civil penalties and vulnerability to a private right of action (if this remedy is included in the bill); and
- ineligibility for any of the above-listed carrots.

Agency and public consultations. The agency should encourage program sponsors to meet informally with agency personnel in advance of preparing an application, both to discuss the process and to identify key issues. The main purpose of these meetings would be a candid exchange of information and views. In addition, the safe harbor approval criteria would include a requirement that industry demonstrate that it consulted with public stakeholders. Although this has not been the norm in the United States (e.g., COPPA requires only industry-government consultation), a public consultation requirement strongly reinforces the credibility and integrity of the safe harbor approach and increases the likelihood that industry codes of conduct will enjoy the widespread support and acceptance of consumers, consumer advocates, and the general public.

The agency should define public stakeholders very broadly to include members of the public, consumer advocacy groups, and academics. Indeed, as part of their applications, program sponsors should be required to submit a statement showing that they allowed at least twelve weeks for consultation and describing who is affected by the code, efforts to consult with affected groups, the groups' comments on the proposed code, changes to the proposed code, a summary of any remaining issues and why they are unresolved, and a list of organizations likely to adopt the code.[16] This statement should be publicly available.[17] One way to ensure that such consultations occur would be for a newly formed ''Privacy Policy Office'' in the Department of Commerce to convene relevant multi-stakeholder groups as suggested in the recent Commerce Privacy Green Paper.[18] Alternatively, program sponsors and industry might arrange for informal meetings with relevant stakeholders.[19] In either case, it is incumbent

[15] Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(3), Stb. 2000, 302 (Neth.), *available and translated at* http://www.dutchdpa.nl/downloads_wetten/wbp.pdf.

[16] This approach is based on an Australian model, which is described at length in Office of the Federal Privacy Commissioner, Guidelines on Privacy Code Development (2001), *available at* http://www.privacy.gov.au/materials/types/download/8634/6482.

[17] The NAI followed a similar approach when it revised its code of conduct for OBA in 2008. Indeed, NAI published draft principles for public comment, and then issued revised principles and simultaneously published a fifty-page summary of these comments along with its own responses, which in many cases consisted in changing the draft principles. *See* Network Advertising Initiative, *Response to Public Comments Received on the 2008 NAI Principles Draft* (2008), *available at* http://www.networkadvertising.org/networks/NAI%20Response%20to%20Public%20Comments_Final%20for%20Website.pdf.

[18] *See* Dept. of Commerce, *supra* note 4, at 45-50.

[19] A good example is how Yahoo!, Google and Microsoft responded to accusations of censoring the internet in China by sitting down with a cross-section of human rights organizations, socially responsible investment firms, and academics, and developing voluntary guidelines for protecting freedom of

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

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.

Form of application. 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.'' *See* Stearns Bill § 9(b)(2).

Criteria for approval. 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.

Threshold criteria. 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.

Substantive criteria. 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 (*See* 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.

Approval process. 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). *See* Rubinstein, *supra* note 5, at 402-04.

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

[21] *See* Rubinstein, *supra* 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. *See* 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 ideas about how it wants to regulate the OBA sector and may want the agency to establish specific approval criteria for this industry. We recommend that, if Congress directs the agency to issue specific criteria for the OBA sector safe harbor, it *not* do so for other sectors. Instead, the statutory requirements for other sectors should remain broad so as not to stifle tailoring and innovation.

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 (*See* Kerry-McCain Bill § 501(b)(4));
- issue its written decision pursuant to a notice-and-comment rulemaking processes (*See* 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 (*See* Stearns Bill § 9(b)(4)).

Judicial review. Congress should give federal district courts jurisdiction to review final agency action rejecting, or approving, a safe harbor program application. See Rush Bill § 402(d). This will allow applicants to seek recourse in the courts if they believe that the agency has improperly rejected their application. It will also allow stakeholders to challenge an agency approval of a program that they believe does not correctly embody the statutory requirements. The courts should uphold the agency decision so long as it is reasonable.

Renewal and amendment. Amendment and renewal of safe harbor programs can serve as effective mechanisms for keeping program rules current in an area of rapidly changing technology and privacy challenges. It is therefore important that safe harbor program approvals expire after a certain period, and that the safe harbor organizations have an opportunity to amend their programs during any given approval period. To achieve this, the statute should provide that:

- Agency approval of a safe harbor program ends after five years. After five years, the applicant may seek, and the agency may approve, a renewal of the program.[24]
- Applicants seeking program renewal must consult with stakeholders as set out in the public consultation requirement (above).
- Prior to renewing a safe harbor program, the agency should audit the program to confirm that it continues to meet the approval criteria and has properly been carrying out its responsibilities.
- Safe harbor organizations may amend their programs prior to renewal.
- The agency should follow notice-and-comment rulemaking procedures in assessing any proposed renewal or amendment.
- An agency decision on an application to renew or amend a safe harbor program is final agency action that is subject to judicial review in the federal district courts.

[23] The agency should also comply with time limits for the issuance of the proposed rule (180 days), comment period (60 days), and issuance of the final rule (1 year).

[24] The Dutch also employ a five-year renewal period.

Accountability and Enforcement

Accountability is critical to the credibility and success of the safe harbor approach. For this approach to be successful, Congress will need to create effective monitoring and enforcement mechanisms. At the same time, experience shows that monitoring, inspection and enforcement can be time-consuming and costly. For example, in the Netherlands the large number of firms that utilize personal information, combined with limited agency enforcement resources, have made it difficult for the Data Protection Authority to carry out monitoring and enforcement while also meeting its other responsibilities. American regulators would likely face similar resource constraints. It is therefore vital that Congress design a monitoring and enforcement system that does not rely exclusively on limited agency enforcement resources. To achieve effective monitoring, accountability and enforcement at a reasonable cost, we recommend that the safe harbor system rely on a mix of self-audits, agency inspection, and third-party audits, as described below.

Self-audits and self-certification. Each covered entity under any newly enacted privacy statute should annually audit its own compliance with the requirements of its safe harbor program. *See* Stearns Bill § 9(c)(2). Covered entities that are not participating in a safe harbor program should assess whether they are in compliance with the statute itself. Following its self-audit, each covered entity should annually certify that it is in compliance with the relevant requirements. *See* Stearns Bill § 9(c)(2). Congress should establish an easy mechanism for making this certification such as ''checking a box'' on an agency website. If an entity identifies compliance problems during the course of a self-audit, discloses them to the agency, and resolves them within a reasonable time, it should face reduced or no penalties for such violations, although the agency should publicly disclose the compliance problem and its resolution. Any entity that incorrectly certifies its compliance with the relevant requirements should face substantial penalties.

Agency inspection. Congress should give the agency authority to inspect covered entities to assess compliance. *See* Stearns Bill § 9 (c)(2)(E). Resource constraints will limit the number of such inspections. Accordingly, the agency should use a risk-based approach to determine which entities it will inspect, and should issue a rule that specifies how it will assess risk. The Dutch Data Protection Authority follows this approach. It draws on citizen complaints and other information to assess the risk that a given entity is violating the data protection law. Based on this risk analysis, it then determines where to target its enforcement resources. The statute should authorize the agency to take a similar approach and should instruct the agency to treat an entity's participation in a safe harbor program as a factor that reduces its risk level. Safe harbor participants will therefore have a lower inspection priority than nonparticipants.

Third-party audits and certification. Periodically, each covered entity (whether or not it participates in a safe harbor program) should employ an independent, third-party auditor to evaluate its policies and practices and assess its compliance with the relevant requirements. Entities below a certain size—perhaps as measured by web subscribers or visitors—would be exempt from this audit requirement. Where a covered entity participates in a safe harbor program, the auditor will

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

assess the entity's compliance with that program's rules. Where a covered entity does not participate in a safe harbor program, the auditor will assess the entity's compliance with the statute itself. The third-party auditor will review the covered entity's annual self-audits as well as its policies, practices and records. If the auditor finds the entity to be in compliance with the relevant requirements, it will ''certify'' the entity—a seal of approval that the particular company or organization can publicize. If the auditor finds that the entity is not in compliance, it will communicate this to the agency. The auditor's evaluation should be an important factor in the agency's risk analysis for the purposes of inspection priority.

The NAI, a self-regulatory privacy program for the behavioral advertising industry, called for random, third-party audits of participating companies. A study of this initiative suggested that, during the initial years of the program, the auditor did not remain sufficiently independent and did not carry out its work in a transparent manner.[25] While the NAI has significantly revised and has re-launched its program since the time of this study, the initial phase of the initiative suggests that a third-party audit requirement must be correctly structured in order to be effective.[26]

We suggest that Congress require the agency to review all third-party auditors to ensure that they satisfy basic eligibility criteria related to competence in applying appropriate privacy standards. The agency should publish these eligibility criteria and also indicate what constitutes an acceptable audit. Organizations or individuals wishing to serve as third-party auditors should then apply to the agency with evidence of their qualifications, and the agency should maintain a list of those that demonstrate that they meet these criteria. Only auditors on this list should be allowed to perform third-party audits. The agency should not allow the safe harbor organizations themselves to serve as auditors for their own members, and it should periodically evaluate the listed auditors. If it finds that an auditor is consistently submitting inadequate audits or is otherwise not adequately performing its responsibilities, it should remove it from the list.

In addition Congress, after assessing the costs involved, should establish the frequency with which safe harbor participants and non-participants must undergo third-party audits. In setting this time period, Congress should require safe harbor participants to undergo third-party audits *less frequently* than non-participants. This reduced frequency recognizes that firms demonstrate responsibility when they voluntarily agree to participate in a safe harbor program and so require less outside supervision. The reduced frequency will also serve as an incentive that encourages participation in safe harbor programs. The covered entity will bear the cost of the third-party audit. This will allow for wider and more effective compliance auditing without overtaxing limited agency budgets.

Finally, Congress should design the third-party audit process so that firms that comply with it also meet the requirements for the Asia Pacific Economic Cooperation (APEC) Accountability Agent certification.[27] This will support global interoperability of compliance and accountability programs.

Claims handling and dispute resolution. A safe harbor program should establish a mechanism for receiving consumer complaints about its own practices or about the practices of its participants, and for handling these complaints and resolving disputes. This could include the establishment of an independent dispute resolution committee charged with receiving complaints and resolving disputes. The Dutch codes of conduct typically include such a body. For example, the Code of Conduct for Financial Institutions provides that individuals should first present their complaints to an independent Complaints Institute. If they are not satisfied with the Complaints Institute's decision, they may then bring their complaint to the Data Protection Authority or to the courts. As with the Dutch approach, we recommend that Congress require individuals to exhaust their remedies under the safe harbor program's dispute resolution process before filing a complaint with the agency. *See* Stearns Bill § 9(d). If, upon consideration of a complaint, the safe harbor program finds that a participant has failed to comply with program requirements, the program should:

- issue a formal finding of noncompliance and provide public notice of this finding;
- give the participant an opportunity to address and cure the compliance issue;
- if the participant does not cure the compliance issue within 60 days of the formal finding, report this to the agency and suspend the participant's membership in the program until such time as the participant proves that it has cured the issue and achieved compliance; and
- if the participant does not cure the compliance issue within 120 days of the formal finding or, at minimum, make a binding commitment to correct the issue within a mutually agreeable time frame, expel the participant from the safe harbor program and refer the matter to the agency for further enforcement as the agency may deem appropriate.

The agency should establish a similar mechanism to handle complaints against those companies that are not participating in a safe harbor program.

Enforcement. Congress should grant the agency express authority to enforce the statute against all covered entities and to issue civil penalties for non-compliance. Congress should also consider creating a private right

[25] Pam Dixon, World Privacy Forum, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* 39 (2007) (calling the NAI audits ''neither independent nor transparent'').

[26] Hirsch, *supra* note 8, at 460-64.

[27] The APEC Cross-Border Privacy Rules program seeks to facilitate cross-border data flows among APEC countries while protecting individual privacy. The program allows individual companies to develop a set of rules that satisfy the APEC Privacy Framework. Specially designated accountability agents would certify that a given company's rules comply with the Framework. Companies that follow certified rules would have some confidence, although not complete assurance, that they were in compliance with the relevant member state laws. *See generally, Asia-Pacific Economic Cooperation (APEC) Data Privacy Pathfinder Projects Implementation Plan–Revised* (Feb. 2009), *available at* http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group [hereinafter APEC Plan]; Justin Brookman, *Can Cross-Border Privacy Rules ''Trump'' Divergent Data Protection Laws?*, *available at* http://www.cdt.org/blogs/justin-brookman/410can-%E2%80%9Ccross-border-privacy-rules%E2%80%9D-trump-divergent-data-protection-laws.

of action against covered entities for non-compliance with the statute. Where a covered entity *participates* 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 *does not participate* 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. *Indeed, an underfunded safe harbor program with lax oversight and enforcement would be worse than no safe harbor program at all*. 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. *See* 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. *See* http://ftc.gov/opa/2009/08/bestpriced.shtm. A few months later, the FTC announced proposed settlements in six more false claims cases. *See* 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, *supra* note 5, at 392-93.

[30] The FTC has been slow to take action in these false claims cases. *See* Rubinstein, *supra* 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] *See supra* note 27.

[33] *See generally* APEC Plan, *supra* note 27.

 COPYRIGHT © 2011 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423