# PRIVACY, SELF-REGULATION AND STATUTORY SAFE HARBORS

Ira S. Rubinstein*

*Abstract*

*According to its many critics, privacy self-regulation is a failure. It suffers from weak or incomplete realization of Fair Information Practice Principles, inadequate incentives to ensure wide scale industry participation, ineffective compliance and enforcement mechanisms, and an overall lack of transparency. Rather than attacking or defending self-regulation, this Article explores various models of self-regulation, which differ as to the role of government in setting requirements, approving guidelines, and imposing sanctions for non-compliance. Based on three case studies of a "purely" voluntary privacy code aimed at online behavioral advertising practices, a "partially mandated" safe harbor agreement that ensures data flows between Europe and the US, and a "fully mandated" or statutory safe harbor designed to protect children's privacy, this Article demonstrates that statutory safe harbor programs are more effective than other forms of privacy self-regulation. Next it conceptualizes new models for privacy safe harbors based on insights derived from "second generation" environmental policy instruments and concludes by offering specific recommendations to Congress on how best to design new safe harbor programs as an essential component of omnibus consumer privacy legislation.*

Table of Contents



* Adjunct Professor of Law and Senior Fellow, Information Law Institute, New York University School of Law. For their comments on an earlier draft of this paper, I am grateful to Chris Hoofnagle and Dennis Hirsch and to the participants in the Workshop on Federal Privacy Legislation, NYU School of Law, October 2, 2009. I also want to thank Malcolm Crompton for his guidance regarding Australian privacy codes.

# INTRODUCTION

Privacy policy in the US has long relied on a combination of sectoral law, market forces and self-regulation. Over the years, the Department of Commerce (DOC) and the Federal Trade Commission (FTC) have expressly favored a self-regulatory approach. Their chief argument has been that self-regulation can protect privacy in a more flexible and cost-effective manner than direct regulation without impeding the rapid pace of innovation in Internet-related businesses.

Privacy self-regulation generally involves a trade association or group of firms establishing a set of substantive rules concerning the collection, use and transfer of personal information along with procedures for applying these rules to member firms. More specifically, the self-regulatory model has three components: (1) an industry group issuing guidelines or a code of conduct governing members' privacy practices; (2) enforcement by the industry group, or perhaps a dispute resolution mechanism administered by an independent third party, but no enforceable legal remedies (other than the FTC's inherent power to prosecute firms for unfair and deceptive trade practices, including misrepresentation of their privacy policies); and (3) procedural rules related to amending existing guidelines and related internal matters.[1]

According to its many critics, however, self-regulation is a failure.[2] It suffers from weak or incomplete realization of Fair Information Practice Principles (FIPPs),[3] inadequate incentives to ensure wide scale industry participation, ineffective compliance and enforcement mechanisms, and an overall lack of transparency. Indeed, privacy self-regulation has been derided as chimera whose real purpose is to avoid government regulation.[4] More often than not, these same critics call upon Congress to intervene in the online marketplace by enacting comprehensive privacy legislation. Under this enforcement model of regulation (which is also referred to as "command-and-control" regulation), Congress defines a set of privacy rules for commercial firms based on FIPPs and authorizes agency regulation, which is then supplemented over time by court decisions interpreting the rules. The legislation also spells out which agencies have enforcement authority (such as the FTC and/or state Attorneys General), what remedies are available (for example, penalties, damages, and/or injunctive relief) and whether individuals have a private right of action to recover damages for any injuries they might suffer when a firm violates the law. Enforcement actions would have two main goals, deterrence and—assuming the statute permits damage awards to individuals—compensation.[5]

The opposing sides in the privacy debate tend to treat self-regulation and government regulation as if they were mutually exclusive options from which policy makers have to choose, either one or the other. But this is short-sighted. As a number of environmental law scholars have observed, self-regulation is a "highly malleable term which may encompass a wider variety of instruments." Thus, it is better to think of "pure" self-regulation and "strict" command-and-control regulation as opposing ends of a regulatory continuum, with most regulatory schemes falling somewhere in the middle.[6] Rather than attacking or defending self-regulation, this Article explores a "co-regulatory" approach in which industry enjoys considerable scope in shaping self-regulatory guidelines, with government still retaining general oversight authority to approve and enforce these guidelines.[7] This hybrid approach builds on the privacy

[1] *See* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U. S. Dep't of Commerce ed., 1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm.

[2] *See infra*, Section I.B.

[3] FIPPs are the basis for modern privacy regulation but have been challenged in recent years by privacy scholars and technologists; s*ee infra* notes 186-188 and accompanying text.

[4] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461, 1524-1528 (2000).

[5] *See* Swire, *supra* note 1. A good example of a federal privacy statute in which industry self-regulation plays no role is the Video Privacy Protection Act of 1988, 18 USC. §§ 2710-2711**.**

[6] *See* Darren Sinclair, *Self-Regulation Versus Command and Control? Beyond False Dichotomies*, 19 LAW & POL'Y 529 (1997); *see also* Neil Gunningham and Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*, 19 LAW & POL'Y 363 (1997).

[7] *See* Sinclair, *id.* at 544.

safe harbor created by Congress in the Children's Online Privacy Protection Act of 1998 (COPPA), but re-designs it in several critical ways.

Although scholars and regulators have studied the uses and limitations of self-regulation in achieving information privacy,[8] there has been little systematic attention to statutorily-created privacy safe harbors. This Article argues that a privacy safe harbor is an effective and flexible policy instrument that, if properly designed, offers several advantages as compared to the false dichotomy of voluntary industry guidelines versus prescriptive government regulation. First, the existing COPPA safe harbor, without any modification, deals successfully with virtually all of the standard criticisms of self-regulation.[9] Second, by using the right combination of sticks and carrots to re-design privacy safe harbors, Congress can encourage much broader industry participation, thereby ensuring a baseline level of monitoring and dispute resolution, while allowing the FTC to devote its scarce enforcement resources to the most egregious or systemic privacy abuses.[10] Finally, by allowing greater flexibility in structuring safe harbors, Congress can better address difficult issues such as behavioral advertising and experiment with policy innovations such as accountability-based systems.[11]

Why does this matter? For the first time in 10 years, Congress seems ready to revisit comprehensive online privacy legislation. In 2009, the House Committee on Energy and Commerce held several hearings on data privacy and security issues and the Chairman of a key Subcommittee recently described his plans to introduce online privacy legislation.[12] Leading technology firms have voiced support for federal privacy legislation and are working with privacy groups to draft model legislation.[13] If Congress enacts such legislation, one might reasonably assume that self-regulatory initiatives would fade away. But this need not be the case. For example, the COPPA safe harbor provision sought to encourage participation in self-regulatory programs by treating a company that follows program guidelines as having complied with statutory requirements.[14] Nor is this an isolated example. During the 106th and 107th Congress, which is when the Senate and the House last gave serious consideration to online privacy legislation, several of the leading bills included provisions for a self-regulatory safe harbor.[15] It seems likely that such provisions will re-surface in any new bills offered in the 111th Congress or thereafter.[16] This Article argues that a safe harbor provision would strengthen whatever bill emerges from current discussions and further that consumers will enjoy a higher level of privacy protection under a well-designed safe harbor regime than if Congress relied solely on a conventional command-and-control model of regulation or enacted no law at all.

The paper has three parts. Part I begins by analyzing the rise and fall of self-regulation as the FTC's preferred approach to online privacy in the five year period ending in 2000, when it finally recommended that Congress enact a basic level of online privacy protection. It then examines the Commission's shift in 2001, under Chairman Tim Muris, to an enforcement-based agenda designed to remedy specific harms, as well as the FTC's renewed interest in self-regulation as the best way to handle the privacy concerns raised by behavioral advertising. Finally, it considers the arguments of privacy scholars and economists for and against self-regulation, but finds this debate inconclusive since both sides voice compelling objections without advancing a solution that resolves their differences. Part II shifts from a more general and abstract discussion of self-regulation to three case studies: the first of a "purely" voluntary industry effort aimed at

[8] *See* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, *supra* note 1.

[9] *See infra* II.C.

[10] *See infra* III.B.

[11] *Id.*

[12] *See* Rick Boucher, *Behavioral Ads: The Need for Privacy Protection*, THE HILL, Sept. 24, 2009 *available at* http://thehill.com/special-reports/technology-september-2009/60253-behavioral-ads-the-need-for-privacy-protection. Boucher is chairman of the Subcommittee on Communications, Technology and the Internet.

[13] Joelle Tesler, *Microsoft, Google Back Privacy Legislation*, MSNBC, July 10, 2008, http://www.msnbc.msn.com/id/25622863/.

[14] This is referred to as "deemed compliance"; *see infra*, note 111 and accompanying text.

[15] *See, e.g.*, 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); the Consumer Privacy Protection Act of 2002, H.R. 4678, 107th Cong. §106 (2002); and the Online Personal Privacy Act, S. 2201, 107th Cong. § 203 (2002).

[16] Cong. Boucher's proposed bill would also include a safe harbor; *see supra* note 12.

online behavioral advertising practices; the second of a "partially mandated" safe harbor resulting from joint government efforts to ensure data flows between Europe and the US; and the third of a "fully mandated" or statutory safe harbor under COPPA, which is designed to facilitate industry self-regulation as a vital component of protecting children's privacy. Part III argues that despite several weaknesses, statutory safe harbors such as COPPA are a superior form of self-regulation. Next, it describes a more collaborative, flexible and performance-based alternative to existing self-regulatory schemes, drawing on critical insights into a new array of policy tools addressed at environmental challenges. The Article concludes by recommending that Congress apply these new tools to regulating privacy.

## I. DOES SELF-REGULATION WORK?

From the earliest days of the Clinton Administration's work on developing a regulatory framework for electronic commerce and the Internet, the US government has promoted self-regulation as the preferred approach to protecting consumer privacy online.[17] Clinton officials generally favored the view that private sector leadership would cause electronic commerce to flourish, and specifically supported efforts to "to implement meaningful, consumer-friendly, self-regulatory privacy regimes" in combination with technology solutions.[18] Moreover, government should avoid imposing undue restrictions on this emerging sector as unnecessary regulation might distort market developments by "decreasing the supply and raising the cost of products and services" or by failing to keep pace with "the break-neck speed of change in technology." [19] At the same time, Clinton officials recognized that if industry failed to address privacy concerns through self-regulation and technology, the pressure would increase for the Administration to safeguard consumer privacy online by imposing a regulatory solution. In 2000, the FTC issued a legislative recommendation, which Congress rejected despite holding hearings on several bills and even reporting one out of Committee. The next section shows that the FTC's embrace of self-regulatory solutions has waxed and waned over the years, and is once again ascendant at least as to online behavioral advertising. A review of the economic and legal arguments for and against self-regulation suggests that the opposing viewpoints are irreconcilable. Thus, the next Part pursues a more empirical approach via three case studies.

### *A. The Rise and Fall (and Renewal) of Self-Regulatory Privacy Schemes*

In 1995, the FTC held the first in a series of public workshops examining the collection, use and transfer of consumers' personal information, the self-regulatory and technological efforts of industry to enhance consumer privacy, and the role of government in privacy protection. At an important event held in June 1996, industry representatives and privacy advocates gave voice to their opposing views. Industry cited three reasons privacy regulation would be counterproductive: First, it would stifle innovation in a developing market; second, it might drive marketing activity off the Internet entirely by adding unnecessary costs to online advertising; and third, it would interfere with the market definition of consumer privacy preferences and the appropriate industry response.[20] On the other hand, privacy advocates warned that technology was no substitute for FIPPs and that self-regulation would remain

[17] *See* WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997).

[18] *Id.* (characterizing such regimes as including mechanisms for "facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution"). The Clinton Administration used a similar approach to regulating the environment. *See* WILLIAM J. CLINTON & ALBERT GORE, JR., THE CLIMATE CHANGE ACTION PLAN (1993) and REINVENTING ENVIRONMENTAL REGULATION (1995).

[19] CLINTON & GORE, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE, *supra* note 17.

[20] FTC, STAFF REPORT: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE 27-29 (Dec. 1996) [hereinafter 1996 Public Workshop Report], *available at* www.ftc.gov/reports/privacy/Privacy1.shtm. Industry representatives also cited emerging technologies that might obviate the need for governmental regulation. The role of such Privacy-Enhancing Technologies, or PETs, in protecting online privacy is beyond the scope of this paper.

ineffective without enforceable privacy rights, which were necessary to deter bad actors and outliers, and ensure the widest possible participation in any self-regulatory schemes.[21]

The Commission's views evolved over the next several years as it held more public workshops, commissioned two large surveys of commercial Web sites' privacy practices, and issued three reports to Congress analyzing industry's progress in addressing consumer privacy concerns. In determining whether self-regulatory initiatives were succeeding, the FTC relied on its own formulation of FIPPs in terms of five (and later four) core principles of privacy protection—notice, choice, access, security and enforcement.[22] As late as 1998, the Commission still embraced the Clinton Administration's view of self-regulation as "the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[23] Yet it also began to express some doubts. For example, a 1998 report to Congress summarized the results of the Commission's first Internet privacy survey, which found that only 14% of Web sites collecting personal information from consumers had privacy notices and only 2% had a "comprehensive" privacy policy. Based on this data, the Commission concluded that "the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness)."[24] Having asked trade associations and industry groups to submit copies of their self-regulatory guidelines for review, the Commission also found that the guidelines did not reflect all five of the FIPPs and were especially weak on "the enforcement mechanisms needed for an effective self-regulatory regime."[25] While it reached no firm conclusion on what additional incentives were required to ensure more industry progress, the Commission recommended that Congress develop legislation defining the basic standards of practice for the online collection and use of information from children.[26]

In Congressional testimony a few months later, FTC Chairman Robert Pitofsky characterized industry's self-regulatory initiatives as "inadequate and disappointing" and recommended that Congress enact online privacy legislation unless industry demonstrated significant progress by the end of the year.[27] In its second report to Congress in 1999, the FTC focused on self-regulation. It commended recent industry developments such as the guidelines adopted by the Online Privacy Alliance (OPA)[28] and the creation by Truste, BBBOnline, and others of privacy seal programs.[29] The Commission also reviewed the results of two Georgetown University surveys, one of privacy practices at a random sample of heavily trafficked Web sites and the other of the hundred busiest sites. Both surveys showed improvements in the

---

[21] *Id*.

[22] FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), *available at* http://www.ftc.gov/reports/privacy3/toc.shtm. A later report removed enforcement from the list, thereby reducing the number of FIPs to four; *see infra* note 32.

[23] FTC, SELF-REGULATION AND PRIVACY ONLINE: REPORT TO CONGRESS 6 (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf.

[24] FTC, PRIVACY ONLINE: A REPORT TO CONGRESS, *supra* note 22 at 4.

[25] *Id. See also* DEP'T OF COMMERCE AND OFFICE OF MANAGEMENT AND BUDGET, ELEMENTS OF EFFECTIVE SELF-REGULATION FOR THE PROTECTION OF PRIVACY (JUNE 5, 1998), *available at* http://www.ntia.doc.gov/reports/privacydraft/198dftprin.htm (identifying nine elements of effective self-regulation including three that specifically focused on enforcement: consumer recourse; verification of privacy statements; and consequences for failure to comply with self-regulatory practices).

[26] Four months after the Commission's 1998 report, Congress enacted COPPA and the President signed it into law; *see infra* note 105 and accompanying texts.

[27] *Electronic Commerce: Privacy in Cyberspace, Hearings on H.R. 2368 Before the Subcomm. on Telecommunications, Trade and Consumer Protection of the House Comm. on Commerce*, 105th Cong., 2nd Sess., July 21, 1998 (testimony of Robert Pitofsky, Chairman of the FTC), *available at* http://www.ftc.gov/os/1998/07/privac98.htm. Interestingly, Pitofsky proposed legislation that included "a safe harbor for industries that choose to establish their own means of providing consumers privacy protections, as long as those means are subject to governmental approval." *Id.* This is one of the earliest mentions of safe harbors as an incentive for industry self-regulation.

[28] *See* FTC, SELF-REGULATION AND PRIVACY ONLINE, *supra* note 23 at 8-9 (describing OPA as an industry coalition that developed self-regulatory guidelines used by the leading privacy seal programs, but which did not itself engage in compliance monitoring or enforcement).

[29] *Id.* at 12 (noting that seal programs "require their licensees to abide by codes of online information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites). For a critique of these seal programs based on weak standards, limited enforcement powers, and weak brand recognition, *see* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1610, 1693-94 (1999).

frequency of privacy disclosures but continued weakness in sites' implementing all four of the FIPPs.[30] A majority of the Commission determined that online privacy legislation was not yet appropriate and recommended that self-regulation be given more time, while renewing its calls for further industry efforts to implement FIPPs.[31]

Finally, in 2000, in its third report to Congress, the Commission abandoned self-regulation as a preferred approach and by a 3-2 majority formally recommended that Congress enact comprehensive online privacy legislation. The proposed legislation would require consumer-oriented commercial Web sites collecting personal data from consumers (and not already covered by the children's privacy statute) to comply with all four of the FIPPs and give rulemaking authority to an implementing agency.[32] The Commission based its recommendation on a second survey of Web site privacy practices that once again demonstrated that despite progress on privacy disclosures and adoption of FIPPs, as well as the growth of industry seal programs, self-regulatory initiatives failed to achieve broad industry adoption. Commissioner Orson Swindle issued a lengthy and stinging dissent in which he stated that among the many deficiencies in the 2000 report, "there is absolutely no consideration of the costs and benefits of regulation."[33] A few months later, in July 2000, the FTC addressed the issue of network advertisers collecting personal information for profiling purposes. While commending industry efforts to formulate self-regulatory principles for behavioral advertising, the Commission repeated its recommendation that Congress enact "backstop legislation" to fully ensure that online profiling is carried out in accordance with FIPPs.[34]

In 2001, the newly appointed FTC Chairman, Tim Muris, temporarily shelved the debate over self-regulation, not by reiterating the Commission's endorsement of legislation but by deemphasizing the implementation of FIPPs as a primary goal.[35] Muris ushered in a revised privacy agenda for the Commission by shifting its focus to protecting consumers against "real" harms such as online stalking, identity theft, telemarketing and spam. He proposed a number of measures such as creating a "do not call" list for consumers who want to avoid telemarketing calls (which proved wildly successful); devoting more resources to prosecuting fraudulent activities (such as spam and "pretexting," which is the use of fraud or pretense to obtain access to consumers' financial information, telephone call records, or other sensitive information); and providing better assistance to victims of identity theft. Muris also proposed using the FTC's enforcement powers to go after Web sites that failed to abide by the privacy promises embedded in their online privacy statements, while at the same time suggesting that the Commission gather more information about Internet security practices and other emerging issues and new privacy technologies such as P3P.

But Muris was quite skeptical about the wisdom of enacting new online privacy legislation, questioning "how such legislation would work and the costs and benefits it would generate." He characterized the task of legislating broad-based privacy protections (i.e., a bill that would address both online and offline practices) as "extraordinarily difficult" citing both the severe problems with notices from financial institutions under the Gramm-Leach-Bliley Act[36] as well as a lack of consensus over online security and access principles. Finally, he called attention to the absence of sufficient data regarding the cost/benefit tradeoff of online privacy legislation.[37] Over the next eight years, Muris and his successors organized the FTC's agenda around combating harmful uses of personal information with an emphasis on

[30] FTC, SELF-REGULATION AND PRIVACY ONLINE, *supra* note 23 at 7.

[31] *Id.* at 12-14.

[32] *See* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 36 (2000) [hereinafter FAIR INFORMATION PRACTICES REPORT], *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[33] FAIR INFORMATION PRACTICES REPORT, *id.* at 16 (Dissenting Statement of Orson Swindle, FTC Commissioner).

[34] *See infra* notes 62-68 and accompanying text.

[35] Timothy J. Muris, Chairman, FTC, Remarks at the Privacy 2001 Conference: Protecting Consumers' Privacy: 2002 and Beyond (October 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm.

[36] *Id.* As Muris noted, "Acres of trees died to produce a blizzard of barely comprehensible privacy notices."

[37] *See also* Beales and Muris, *infra* note 50.

enforcement actions and consumer outreach. In its workshops, testimony and reports to Congress, however, the Commission gave little attention to self-regulatory privacy initiatives or whether they should be supplanted by legislation. In its broader agenda, which included protecting consumers from fraudulent advertising, the FTC continued to believe in the efficacy of self-regulation and generally praised the self-regulatory efforts of the advertising industry on a range of issues. But it confined its work in the privacy arena to problems causing specific harms (e.g., spam, spyware, phishing, ID theft, and data breaches) and to laws that would enhance its enforcement powers (such as the CAN-SPAM Act and the US SAFE Web Act), and, until quite recently, remained neutral or silent on the topic of self-regulation.

In 2006, and hence for first time in many years, an FTC report included among its list of goals "encouraging self-regulatory initiatives to benefit consumers." One of two areas specifically called out for self-regulatory efforts was online behavioral advertising.[38] A year later, the FTC hosted a meeting on this topic and subsequently offered proposed principles to guide the development of self-regulation in online behavioral advertising.[39] Over the next eighteen months, a leading industry group revised its previously issued self-regulatory guidelines and in December 2008 replaced them with a new industry code of conduct. In March 2009, the FTC released its own report on self-regulation in the online advertising industry.[40] Finally, in his first speech following his appointment, the new FTC Chairman, Jon Leibowitz, noted that the current approach to behavioral advertising was not working. He alluded to the recently issued staff guidelines and expressed hope "that industry will respond with concrete improvements." While reminding his audience that "Self-regulation, if it works, can be the fastest and best way to change the status quo" he warned that "if there isn't an appropriately vigorous response, my sense is that Congress and the Commission may move toward a more regulatory model."[41]

As Yogi Berra famously said, "This is déjà vu all over again." As shown above, several of Leibowitz's predecessors arrived at exactly this point only to reluctantly conclude that self-regulation would not work. It seems highly unlikely that Leibowitz is unaware of past dissatisfaction with privacy self-regulation considering his prior service as an FTC Commissioner. Nor is he likely to hold fast to the harm-based enforcement agenda championed by Tim Muris, given recent statements by David Vladeck, the new Director of the Bureau of Consumer Protection, expressing doubts about both the traditional notice and choice model and the harms-based approach.[42] So why did Leibowitz give voice to a position that Clinton officials might have expressed fifteen years ago? One possible answer is politics. Privacy legislation has never enjoyed reliable political support especially given the relatively strong opposition from industry and the jurisdictional complications that inevitably arise when multiple Committees lay claim to privacy initiatives.[43] So perhaps Leibowitz's statement is best understood as a placeholder until the Commission assesses the political prospects for omnibus privacy legislation or Vladeck and others develop a new approach to protecting consumer privacy without legislation. An equally plausible answer is a lingering concern over the unintended consequences that might result from ill-conceived regulation of

[38] FTC, PROTECTING CONSUMERS IN THE NEXT TECH-ADE (2008), 4, 9, 11 *available at* http://www.ftc.gov/bcp/workshops/techade/reports.html (the other areas was protecting minors who use social networking websites). Although the agency published this report in spring 2008, it referred to a set of public hearings held in November 2006. At these hearings, witnesses also mentioned self-regulatory efforts in the mobile device industry and by developers of RFID devices.

[39] *See infra* Part II.A.

[40] *Id.*

[41] Jon Leibowitz, Chairman, FTC, Remarks at the Center for Democracy and Technology Gala (March 10, 2009), http://www.ftc.gov/speeches/leibowitz/090310remarksforcdtdinner.pdf.

[42] *See* Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 5, 2009 at B5 and The Editors, *An Interview with David Vladeck of the F.T.C.*, N.Y. TIMES, Aug. 5, 2009, *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/.

[43] *See* Robert R. Belair, Presentation at the Harvard Symposium on Privacy and the 110th and 111th Congresses, Congressional Privacy Policy Panel (Aug. 21, 2008), *available at* http://www.ehcca.com/presentations/HIPAA16/belair_3.ppt.

online advertising.[44] The next section suggests that even though the self-regulatory model has many weaknesses, these cost-benefit arguments are difficult to overcome.

### B. *Arguments For and Against Self-Regulation*

In 2001, Chairman Muris and Commissioner Swindle were not alone in worrying about the merits of privacy regulation or questioning the related cost/benefit tradeoffs. Privacy scholars with a free-market perspective and several economists who analyzed these tradeoffs shared their skepticism as did industry. For example, in Congressional testimony and related publications, distinguished privacy scholar Fred Cate emphasized two main concerns: first, the social and economic benefits that flow from "readily accessible information about consumers" and the corresponding harm that would result from privacy law to the extent that it interfered with such open information flows;[45] and, second, the extent to which a consent requirement regarding the collection, use or transfer of personal information "burdens consumers and creates costs."[46] Referring to several studies showing that consumers tend to ignore privacy notices whatever their form, Cate argued that firms subject to consent requirements would face excessive and wasteful costs. This would be equally true for both opt-out and opt-in measures, although he concluded that opt-out rules were preferable because they at least preserved the flow of information. Other scholars pointed to additional costs associated with privacy regulation including (1) administrative costs on government and taxpayers to draft, oversee, and enforce privacy rules; and (2) compliance costs on industry due to the inevitable lack of precision and inflexibility of government rules.[47]

Neoclassical economists who have analyzed privacy regulation also find it undesirable for a second reason, namely, that the free market already provides businesses with compelling incentives to address the privacy concerns of their customers by adopting self-regulatory measures. In their 2001 monograph entitled *Privacy and the Commercial Use of Personal Information*, Paul Rubin and Thomas Lenard argued that "market forces are moving rapidly to provide the privacy desired by consumers, in part by eliminating problems of asymmetric information."[48] For support, they pointed to numerous examples of adverse publicity forcing firms accused of violating consumers' privacy expectations to modify their data collection practices or cancel their plans to combine or use data in new ways. According to Rubin and Lenard, "the principal asset that online marketers have is their reputation with consumers, and any use of information in a way that reduces the value of those reputations is counterproductive for the firm."[49] It follows that firms have a strong incentive to avoid policies inconsistent with their customers' privacy preferences. In fact, many firms have already taken positive steps to protect their reputations by participating in voluntary, third-party privacy seal programs (as discussed above) and developing privacy-enhancing technologies such as cookie management tools and the Platform for Privacy Preferences (P3P). Rubin and Lenard also noted the lack of evidence that

[44] *See* Robert E. Litan, *Law and Policy in the Internet Age*, 50 DUKE L. J. 1045, 1065 (2002)(pointing out that statutory requirements may increase "the costs of marketing leading to increased costs for products and possibly reduced choice … for consumers" if some sites are forced to cut back on the availability of free online content and services).

[45] *See Privacy in the Commercial World, Hearings Before the House Comm. on Energy and Commerce, Subcomm. on Commerce, Trade and Consumer Protection*, 107 Cong., 1st Sess., March 1, 2001 (Statement of Professor Fred H. Cate)(Cate's examples include the ready availability and low cost of consumer credit; more convenient customer services; advertising and marketed materials directed at interested consumers; and greater success at detecting and preventing fraud—all of which are reflected in lower prices for goods and services).

[46] *See Need for Internet Privacy* Legislation, *Hearings Before the Senate Comm. on Commerce, Science and Transportation*, 107 Cong., 1st Sess., July 11, 2001 (Statement of Professor Fred H. Cate). For a more detailed treatment, *see* FRED H. CATE, PRIVACY IN PERSPECTIVE (2001).

[47] *See* Swire, *supra* note 1. In making the case for the self-regulatory model, however, Swire also points out that self-regulation sometimes benefits industry while harming the public.

[48] PAUL H. RUBIN AND THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION, 49-52 (2002)

[49] *Id.* at 51.

legal uses of information for advertising and marketing purposes harm consumers and, therefore, concluded that "the potential benefits of new privacy regulations are very small."[50]

The more prevalent view among privacy scholars, however, is one of a privacy market failure resulting from the related ideas of information asymmetries and collective action problems. For example, in Jerry Kang's view, information asymmetries exist because "individuals today are largely clueless about how personal information is processed through cyberspace."[51] Moreover, consumers face a collective action problem because they find it difficult to band together to bargain for better privacy practices due to their large numbers, lack of repeat play and difficulty in locating like-minded individuals.[52] According to Paul Schwartz, a third reason for skepticism about market-based privacy standards is the "consent fallacy," that is, the lack of either informed or voluntary consumer consent to the privacy practices of Web sites.[53] Schwartz argues that the resulting market failure awards a subsidy to companies that exploit personal data, leading them to over-invest in collecting and tracking such data and to under-invest in privacy enhancing technologies. The only way to end this subsidy is to establish a new default norm of minimum data disclosure, something industry has no reason to pursue because it prefers "weak standards that ratify the current status quo or even weaken it."[54]

In questioning the market's capacity to protect privacy, Kang and Schwartz (and a great many other privacy scholars) also call attention to the invasive nature of the Internet. Kang points out that "the very technology that makes cyberspace possible also makes detailed, cumulative, invisible observation of our selves possible." This constant surveillance "leads to self-censorship" and undermines human dignity.[55] Kang therefore supports a government mandated opt-in rule that would limit the processing of personal information in cyberspace transactions only to what is "functionally necessary" to complete the transaction at hand. Nor does he shy away from the radical implications of this proposal, which virtually eliminates the secondary market in personal information.[56] For Schwartz, the creation, combination and sale of finely granulated personal data that most people are unable to control results in what he calls the "privacy horror show." Unlike Kang, his chief focus is the impact of excessive information processing on democratic deliberation and an individual's capacity for self-rule.[57] But he agrees with Kang that only federal legislation will succeed in overcoming weak standards based on maximum disclosure, limited transparency, no substantial and or procedural rights, and hollow oversight. Accordingly, he praises COPPA as well as the recent revisions to the federal driver's protection law requiring that states obtain opt-in consent before allowing the use of drivers' licenses and other motor vehicle records for marketing and surveys.[58]

In short, while Cate and the economists emphasize costs vs. benefits under a regime that limits information flows, they seem to neglect the relatively weak position of consumers in the market for information or the privacy harms caused by commercial data surveillance practices. Kang and Schwartz emphasize the latter concerns, but their work provides no estimates of what it might cost to end the

[50] RUBIN & LENARD, *supra* note 48 at 64. For additional studies at this time by economists reaching similar conclusions, s*ee* Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, 14-17 (AEI-Brookings Working Paper, 1999); Robert W. Hahn and Anne Layne Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 119-20 (2002). For an industry perspective, *see* Kent Walker, *The Costs of Privacy*, 25 HARV. J. L. & PUB. POL'Y 87 (2001). For a more recent discussion, *see* J. Howard Beales, III and Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109 (2008)( emphasizing the value of information exchange and the need to base privacy regulation not on FIPPs but on "the potential consequences for consumers of information use and misuse").

[51] S*ee* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1253 (1998).

[52] Kang *Id.* at 1254-56; s*ee* Swire, *supra* note 1.

[53] Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 833 (2000).

[54] *Id.*, at 847; *see* Schwartz, *supra* note 29 at 1686.

[55] Kang, *supra* note 52 at 1198 and 1260. For a more recent discussion of this point, *see* DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, Chap. 3 (2004).

[56] Kang, *supra* note 52 at 1271-1273 (arguing that both advertising and any other secondary use of personal information would require opt-in consent because neither is functionally necessary).

[57] Schwartz, *supra* note 29 at 1621-32, 1647-67.

[58] Schwartz, *supra* note 53 at 854-857; *but see* Fred Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877891-95 (2000)(taking issue with Schwartz's justification of opt-in privacy laws).

subsidy to information processing firms, whether by enacting an opt-in regime or otherwise, or who would pay for these changes. In particular, neither addresses the risk of unintended consequences if Congress enacts strong privacy legislation (in the form of an opt-in rule for data transfers), nor the likely impact of such a rule on the availability of free Internet contents and services.

It is beyond the scope of this paper to attempt to resolve the differences between these two perspectives, which may be irreconcilable. Rather, the point of this section has been to provide some context for the alternating cycles of enthusiasm and disappointment that have marked the US government's support for the self-regulatory approach to privacy. One thing seems clear, however. *If* Congress enacts a new privacy law, and this legislation includes provisions that seek to facilitate industry self-regulation as one element of a broader solution, then it behooves us to understand the shortcomings of self-regulation at a practical level and to consider how they might be fixed.

## II. CASE STUDIES

Thus far, the discussion of self-regulation has been historical or abstract. This Part begins the task identified just now by presenting three case studies of self-regulatory industry programs. The case studies have been chosen to exemplify different forms of self-regulation, all of which fall on a continuum based on what role the government plays in setting requirements, approving guidelines, or imposing sanctions for non-compliance.[59] The two ends of this continuum consist in "pure" voluntary self-regulation at one end and "pure" government regulation at the other. As often is the case with continuums, these end points are ideal types; the actual case studies all fall somewhere in the middle.

The first case study focuses on the Network Advertising Initiative (NAI) Principles, which take the form of *voluntary self-regulation*, in which an industry group defines a set of governing principles and monitors members' compliance (or assigns this task to an independent third-party) without any direct government involvement.[60] This is the prevalent form of privacy self-regulation in the US; other examples include the Privacy Promise of the Direct Marketing Association (DMA), the Individual Reference Service Group (IRSG) Principles (which apply to data brokers), the privacy seal programs of Truste and BBBOnline, and, most recently, the Self-Regulatory Principles for Online Behavioral Advertising, a cross-industry alternative to the NAI Principles.

The second case study looks at a safe harbor solution for US firms needing to transfer data from the EU to the US without running afoul of EU data protection requirements. To benefit from the safe harbor, firms must certify that they will comply with privacy principles negotiated by the US and EU but administered by industry seal programs created for this purpose by DMA, Truste, BBBOnline, and others. This exemplifies what Joseph Rees calls *mandated partial self-regulation*, in which industry handles the enforcement of government-sanctioned rules but subject to government oversight.[61] Finally, the third case study deals with FTC-approved safe harbor programs under COPPA, and that of the Children's Advertising Unit (CARU), in particular, which exemplifies what Rees calls *mandated full self-regulation*, where industry is responsible for both rule making and enforcement, but under (close) government supervision. After completing these case studies, this Article turns an assessment of self-regulatory programs and how to improve them; it then concludes with specific recommendations aimed at redesigning statutory safe harbors based on lessons learned from "second generation" environmental regulations.

### A. *The Network Advertising Initiative*

[59] *See* Gunningham and Rees, *supra* note 6 at 365.

[60] For a broad overview of non-governmental, voluntary initiatives and standards, *see* VOLUNTARY CODES: PRIVATE GOVERNANCE, THE PUBLIC INTEREST AND INNOVATION (Kernaghan Webb, ed. 2004).

[61] JOSEPH V. REES, REFORMING THE WORKPLACE: A STUDY OF SELF-REGULATION IN OCCUPATIONAL SAFETY 11 (1988)

On November 8, 1999, the DOC and the FTC held a public workshop on online profiling, which the FTC defined as the collection of data about consumers using cookies and Web bugs to track their activities across the Web.[62] Although much of this information is anonymous in the narrow sense of not including a user's name, profiling data may include both personally identifiable information (PII) and non- personally identifiable information (non-PII).[63] This data may also be "combined with 'demographic' and 'psychographic' data from third-party sources, data on the consumer's offline purchases, or information collected directly from consumers through surveys and registration forms."[64] The resulting profiles often are highly detailed and revealing yet remain largely invisible to consumers, many of whom react negatively when informed that their online activities are monitored.[65]

The FTC recognized several benefits in the use of cookies and other technologies to create targeted ads, such as providing information about products and services in which consumers are interested and reducing the number or unwanted ads. More importantly, targeted ads increase ad revenues, which subsidize free online content and services.[66] On the other hand, the report also acknowledged several major privacy concerns raised by online profiling such as the lack of consumer awareness; the scope of the monitoring activities, which occurs across multiple Web sites for an indefinite period of time; the potential for associating anonymous profiles with particular individuals, which may discourage "valuable uses of the Web fostered by its perceived anonymity;" the possibility that companies might unilaterally change their policies and begin associating PII with previously collected non-PII; and the risk of companies using profiles to engage in price discrimination.[67] Despite these concerns, the Commission "encouraged the network advertising industry … to craft an industry-wide" self-regulatory program.[68]

A group of eight leading companies responded by announcing the formation of the NAI. Their key tenets included notice to consumers of what information network advertising firms collect and how that information is used, the ability to opt-out of receiving tailored ads, and consumer outreach and education.[69] Less than a year later, the NAI completed a code of conduct and its member firms won praise from the FTC "for the innovative aspects of their proposal" and for adopting self-regulatory principles that "address the privacy concerns consumers have about online profiling and are consistent with fair information practices."[70]

---

[62] *See* FTC, ONLINE PROFILING: A REPORT TO CONGRESS (June 2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf.

[63] *Id.* at 3-4. PII is data that can be linked to specific individuals such as name and address, phone number, e-mail address, and social security and driver's license numbers. Non-PII consists mainly in page views, search query terms, purchases, and click-through responses to ads. Although network advertisers link the profiles that result from tracking such consumer activity to a unique identifier, they generally do not know the name of a specific consumer; hence profiles are considered "anonymous."

[64] *Id*. at 5.

[65] *Id*. at 14; *see* Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES, Sept. 30, 2009 at B3 (discussing new survey of consumer attitudes to online tracking by advertisers).

[66] FTC, ONLINE PROFILING: A REPORT TO CONGRESS, *supra* note 62 at 10.

[67] *Id.* at 10-14. *See also* Deirdre Mulligan, Comments at the FTC Public Workshop on Online Profiling (Nov. 30, 1999), *available at* http://www.ftc.gov/bcp/workshops/profiling/comments/mulligan.pdf (also noting the failure of network advertisers to follow the four FIPPs as identified by the FTC (notice, choice, access security and enforcement).

[68] *Id.* at 1.

[69] *See* Network Advertising Initiative (NAI), Comments at the FTC Public Workshop on Online Profiling (Nov. 30, 1999), *available at* http://www.ftc.gov/bcp/workshops/profiling/comments/nai.htm. By the time this workshop took place, the eight NAI firms had ample reason to fear that their business practices might soon be restricted or even regulated unless they banded together to formulate self-regulatory principles. Privacy complaints about the use of cookies for advertising purposes were growing and only intensified when DoubleClick announced plans to combine the profiling data it collected online with offline data obtained from a merger with a leading data marketing firm, Abacus. This led to investigations by the FTC and several state Attorney Generals, a class action consumer lawsuit, Congressional hearings on online profiling, and massively bad publicity; *see* Evan Hansen, *Double-click Postpones Data Merging Plan*, CNET, March 2, 2000 http://news.cnet.com/DoubleClick-postpones-data-merging-plan/2100-1023_3-237532.html?tag=mnco.

[70] FTC, ONLINE PROFILING: A REPORT TO CONGRESS PART 2 RECOMMENDATIONS 9 (July 2000) [hereinafter ONLINE PROFILING REPORT], *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf. The report also recommended that Congress enact "backstop legislation" establishing a basic level of privacy protection for all consumers since self-regulation cannot address "recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program" whereas legislation "guarantees that notice and choice are

Under the NAI Principles, network advertisers engaging in online preference marketing (OPM) are required to offer consumers notice and choice, both of which vary depending on whether the data collected is non-PII or a combination of PII and non-PII.[71] The use of non-PII requires member firms to post on their Web sites "clear and conspicuous" notice of profiling activities including what type of data is collected and how it is used; procedures for opting-out of such uses; and the retention period for such data.[72] The opportunity to opt-out must be accessible on the firm's or the NAI's Web site. Moreover, NAI firms that enter into a contract with a publisher for OPM services must require that they offer similar privacy protections to consumers.[73] The merger of PII and non-PII for OPM purposes are subject to substantially similar notice requirements but the choice options are more complex. Network advertisers merging PII with previously collected non-PII must first obtain a consumer's affirmative (opt-in) consent, whereas mergers of PII and non-PII collected on a going forward basis must afford consumers "robust notice" and an opt-out choice; the latter rule also applies to using PII collected offline when merged with PII collected online.[74]

The third substantive requirement that applies to all NAI members is enforcement. The NAI Principles offer two options: either participation in a seal program that includes "typical" elements such as random third-party audits, a complaint process, and sanctions including revocation of the seal accompanied by public notice;[75] or independent audits of a member's practices that would be made publicly available on the NAI's Web site.[76] Finally, the NAI offers a number of additional protections to consumers including a prohibition on the use of "sensitive data" (defined as PII about "sensitive medical or financial data, sexual behavior or sexual orientation, [and] social security numbers") for OPM purposes; an opt-in requirement for using any previously collected data (non-PII or PII) under a materially different data collection and use policy;[77] a set of rather limited pledges regarding security and access;[78] and an agreement by NAI members to abide by the principles of notice, choice, access and security as defined by the OPA Guidelines.

Do the NAI principles live up to their promise of protecting consumer privacy or do they merely serve industry's objective of avoiding government regulation? When the principles were first issued, privacy and consumer groups responded quite negatively. They complained about the NAI's lack of transparency[79] and raised significant substantive concerns as well. For example, the 2000 report by EPIC and Junkbusters claimed that the notice provided under the NAI principles would be "complex and confusing;" that opt-out was an "insufficient standard" given the invisible nature of online tracking; that robust opt-out for the merging of personal and anonymous information was not much better unless Internet users were given "the ability to view the information in question" and "to update and delete data"

---

always provided." *Id.* One Commissioner dissented on the grounds that "we do not have a market failure here that requires a legislative solution." *See* ONLINE PROFILING REPORT, *id.* at 2 (Dissenting Statement of Orson Swindle, FTC Commissioner).

[71] OPM is NAI's term for online profiling. *See* NETWORK ADVERTISING INITIATIVE, SELF-REGULATORY PRINCIPLES FOR ONLINE PREFERENCE MARKETING BY NETWORK ADVERTISERS 22 (2000) [hereinafter NAI PRINCIPLES], *available at* http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf (defining OPM as "a process used by network advertisers whereby data is typically collected over time and across Web pages to determine or predict consumer characteristics or preferences for use in ad deliver on the Web").

[72] *Id.* at 3-4.

[73] *Id.* at 4. Similar requirements (excluding the opportunity to opt-out) apply to the collection of data for Ad Delivery and Reporting purposes; *id.* at 5.

[74] *Id.* at 6-7. "Robust notice" is defined as "clear and conspicuous notice about the scope of the non-PII that would be made personally identifiable and how the non-PII will used as a result of such merger." *Id.* at 7. It is not at all obvious how robust notice differs from ordinary notice, which also must be "clear and conspicuous."

[75] *Id.* at 3.

[76] *Id.* at 9-10.

[77] *Id.* at 5 and 8.

[78] *Id.* at 3 and 7.

[79] *See* ELECTRIC PRIVACY INFORMATION CENTER (EPIC) & JUNKBUSTERS, NETWORK ADVERTISING INITIATIVE: PRINCIPLES NOT PRIVACY (2000) *available at* http://epic.org/privacy/internet/nai_analysis.html#note1 (noting that privacy and consumer groups were all but excluded from the NAI-FTC discussions with the exception of a single meeting held ten days prior to the issuance of the ONLINE PROFILING REPORT).

at their discretion; that access might not be provided at all; and that seal programs were reluctant to go after member firms and provided no consumer remedies when violations occurred.[80]

The NAI principles remained unchanged during the next seven years until two highly publicized incidents sparked renewed concerns over profiling practices, not only of the network advertisers but of search firms such as Google, AOL, Microsoft and Yahoo!.[81] In August 2005, the Department of Justice served a subpoena on Google demanding disclosure of search queries during a two month period along with all the URLs in Google's index.[82] The following year, AOL inadvertently disclosed about 20 million search queries with random identifiers in lieu of user ID's but the queries were sufficiently revealing to allow reporters to identify an individual user by name.[83] Press reports of both incidents suggest that consumers were very surprised to learn that Google retained search records at all and could be forced to hand them over to the government or that AOL would voluntarily share such records even with researchers.[84] The next two years saw new complaints by consumer privacy organizations regarding online advertising practices as well as objections to proposed mergers between industry giants such as Google and DoubleClick. Both the EU data protection agencies and the FTC became actively engaged in reviewing these activities, while industry responded to the regulatory pressure by proposing new practices and technologies for improving search privacy and addressing online profiling practices.[85]

In 2007, the FTC held a two-day workshop to revisit the issue of online behavioral advertising. In connection with this workshop, the World Privacy Forum (WPF) prepared a report on the effectiveness of the NAI's self-regulatory scheme during the previous seven years.[86] The report was extremely critical of the NAI Principles on three main grounds. First, WPF characterized the NAI opt-out mechanism as a failure (because it often didn't work, consumers sometimes deleted the opt-out cookie inadvertently, and this technology was ineffective against newer tracking technologies). Second, WPF pointed to a severe and rapid drop-off in NAI membership following the initial release of the principles (from twelve members in 2000 to just two members in 2003) and questioned NAI's decision to sign up so-called "Associate Members" even thought they were not required to fully comply with the NAI Principles. Finally, WPF disparaged NAI's compliance program (which had been outsourced to Truste) for having a weak consumer complaint mechanism and for neglecting random audits, which was one of four key elements identified in NAI's own Enforcement Principle. (There is no indication that Truste conducted any audits at all).[87]

In April 2008, responding to these and other criticisms, and at the urging of the FTC, the NAI released a draft update to its original NAI Principles (and this time solicited public comment on the proposed changes).[88] At the end of 2008, the trade association (which in the wake of renewed public

---

[80] *Id.* at notes 1-7 and accompanying text.

[81] All of these firms offer free search and a host of related services in exchange for serving targeted ads that are based on search queries and other data that users disclose in the course of using a search engine or the related services.

[82] *See* Verne Kopytoff, *Google Says No to Data Demand: Government Wants Records of Searches*, S.F. CHRON., Jan. 20, 2006 at A1. The DOJ hoped that the search records would assist the government in proving the constitutionality of the Child Online Protection Act by showing that it was "more effective than filtering software in protecting minors from exposure to harmful materials on the Internet." A district court eventually approved a narrower DOJ request that Google turn over a random sample of 50,000 URLs for use in the DOJ study. See *Gonzalez v. Google*, 234 F.R.D. 674 (N.D. Cal. 2006).

[83] *See* Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006 at A1 (as a woman identified in a front page *New York Times* article on the AOL leak told reporters, "My goodness, it's my whole personal life. . . .I had no idea somebody was looking over my shoulder").

[84] *Id.*

[85] *See, e.g.*, Stefanie Olsen, *Privacy Concerns Dog Google-DoubleClick Deal*, CNET, April 17, 2007 http://news.cnet.com/Privacy-concerns-dog-Google-DoubleClick-deal/2100-1024_3-6177029.html?tag=mncol; Kevin J. O'Brien and Thomas Crampton, *E.U. Probes Google Over Data Retention Policy*, N.Y. TIMES, May 26, 2007.

[86] *See* PAM DIXON, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND SELF-REGULATION (2007), *available at* http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

[87] *Id.* at 14-27, 28-30 and 32-38.

[88] NAI, NAI PRINCIPLES 2008: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT FOR ONLINE BEHAVIORAL ADVERTISING (Apr. 2008), http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf.

scrutiny now numbered twenty-five members) published its revised code of conduct to mixed reviews.[89] For example, the FTC commended NAI for extending the scope of its access and security principles to data used not only for behavioral targeting but for practices such as ad delivery and reporting on a single domain or across multiple domains site (so-called "multi-site advertising"). But the Commission criticized NAI's failure to develop more effective and innovative disclosure and choice options beyond mere inclusion in the text of a posted privacy policy.[90] Similarly, the Center for Democracy and Technology (CDT)[91] noted "areas of progress" such as greater transparency in the revision process and a potentially broader definition of sensitive information as well as "areas in need of improvement" including those mentioned by the FTC and several others: use of in-house rather than third-party compliance reviews; a failure to address new forms of behavioral advertising based on ISP traffic content;[92] no choice requirement for multi-site advertising; a weak data retention principle; and a failure to take a leadership role in developing innovative mechanisms that would allow users to view, edit and control their behavioral profiles.[93]

### B. *The US-EU Safe Harbor Agreement*

The European Union Data Protection Directive (EU Directive) limits the transfers of personal data to a third country unless it provides an "adequate" level of privacy protection.[94] Unlike the EU Directive, which is an omnibus statute protecting all personal information of European citizens, US privacy protection relies on a combination of sectoral laws addressing privacy in specific contexts, FTC enforcement powers, and self-regulation. As a result of these differences, US firms were uncertain about the legality of data flows from the EU to the US under the Article 25 adequacy standard. After several years of discussion, the European Commission (EC) and the DOC entered into a Safe Harbor Agreement (SHA) spelling out Privacy Principles that would apply to US companies and other organizations receiving personal data from the EU.[95]

The SHA creates a voluntary mechanism enabling US organizations to demonstrate their compliance with the EU Directive for purposes of data transfers from the EU by self-certifying to DOC that they adhere to the Privacy Principles (which mirror the core requirements of the EU Directive) and repeating this assertion in their posted privacy policy.[96] Although the FTC has agreed to treat any violation of the Privacy Principles as an unfair or deceptive practice, the SHA also defines the mechanism that firms should use to ensure compliance with these principles. These include (a) readily available and affordable independent recourse mechanisms for investigating and resolving individual complaints and

---

[89] *See* NAI, NAI'S SELF-REGULATORY CODE OF CONDUCT (Dec. 2008), http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf.

[90] FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 14 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[91] CDT, Response to the 2008 NAI Principles (Dec. 16, 2008), http://cdt.org/press/20081216press.php.

[92] ISPs have the ability to mine data from *all* of a consumer's Internet traffic streams (without exception) using a new technique known as "deep packet inspection," a prospect that has raised serious privacy concerns; *see* Grant Gross, *US Lawmakers Target Deep Packet Inspection in Privacy Bill*, PC World (Apr. 23, 2009) *available at* http://www.pcworld.com/article/163740/us_lawmakers_target_deep_packet_inspection_in_privacy_bill.html.

[93] For a discussion of Google's new "Ad-Preference Manager, which "allows users to express preferences about what sort of advertisements will result from that tracking," s*ee* Kurt Opsahl, *Google Begins Behavioral Targeting Ad Program*, EFF DEEPLINKS BLOG, Mar. 11, 2009, http://www.eff.org/deeplinks/2009/03/google-begins-behavioral-targeting-ad-program; s*ee also* Miguel Helft, *Google to Offer Ads Based on Interests, With Privacy Rights*, N.Y. TIMES, Mar. 11, 2009 at B3.

[94] Council Directive 95/46, art. 25(1), 1995 O.J. (L 281) 31 [hereinafter Council Directive 95/46/EC].

[95] On July 17, 2000, DOC formally issued the Safe Harbor Privacy Principles and other supplementary documents explaining how US enforcement mechanisms would apply and addressing related issues of interpretation, with the understanding that the Commission would then determine that this safe harbor framework provides adequate protection for purpose of data transfer to participating companies. The Privacy Principles included notice, choice, onward transfer, security, data integrity, access and enforcement; s*ee* DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (2000), *available at* http://www.export.gov/safeharbor/eg_main_018247.asp.

[96] Note that there are other ways of meeting the adequacy requirement such as individual consent, standard contractual clauses, binding corporate rules, and approved codes of conduct.

disputes;[97] (b) verification procedures regarding the attestations and assertions businesses make about their privacy practices, which may include self-assessments (which must be signed by a corporate officer and made available upon request) *or* outside compliance reviews;[98] and (c) remedies for failure to comply with the Privacy Principles including not only correction of any problems but various sanctions such as publicizing violations, suspension or removal from a seal program, and compensation for any harm caused by the violation.[99] Truste, BBBOnline, and several other self-regulatory privacy programs already in operation when the SHA took effect then developed Safe Harbor programs specifically designed to satisfy (a) and (c). The verification requirement is satisfied by self-assessment or third-party compliance reviews.

The SHA has been rightly described as an "uneasy compromise" between the comprehensive regulatory approach of the EU and the self-regulatory approach preferred by the US.[100] This partly reflects the fact that in providing the Privacy Principles and related documents that form the SHA, the DOC lacked any direct statutory authority to regulate online privacy and therefore had to rely solely on its enabling statute, which only grants authority to foster, promote, and develop international commerce. Although DOC considers the resulting privacy framework a success,[101] commentators have called attention to several weaknesses. For example, a 2004 report, prepared at the request of the EC and based primarily on a survey of publicly available privacy policies of participating US companies, found numerous deficiencies. These included inadequate representation of various Privacy Principles; misrepresentation of company memberships in self-regulatory programs; Safe Harbor programs that did not incorporate all of the Privacy Principles; and weak implementation of the Enforcement Principle. Moreover, the EC report noted that no complaints have been received and treated "despite frequent and even flagrant inconsistencies and violations in implementation."[102] Indeed, it was not until the summer of 2009 that the FTC announced its first ever enforcement action against a US company for violation of the SHA.[103]

A 2008 report by an independent consulting firm called Galexia reached very similar conclusions.[104] It found that some participants failed to meet even basic requirements of the SHA such as posting a public statement of adherence to the principles; that relatively few participants published privacy policies reflecting all of the Principles as required by the SHA; that a large number of firms failed to provide an independent recourse mechanism or selected a mechanism that was not affordable (such as arbitration); and that many firms claimed to be participants and continue to be accredited by self-regulatory SHA programs even though they no longer appeared on the Safe Harbor List maintained by DOC.

### C. *The COPPA Safe Harbor*

[97] *See* Dep't of Commerce, Issuance of Safe Harbor Principles and Transmission to European Commission, Part III, FAQ 11, 65 Fed. Reg. 45,666, 45,673-674 (July 24, 2000).

[98] *Id.*, FAQ 7, 65 Fed. Reg. at 45,670-671.

[99] *Id.*, FAQ 11, 65 Fed. Reg. at 45,673-674.

[100] *See* Chris Connolly, *The US Safe Harbor - Fact or Fiction?*, 96 PRIVACY LAWS AND BUSINESS INTERNATIONAL 1, (2008) 4, *available at* http://www.galexia.com/public/research/articles/research_articles-pa08.html.

[101] *See* Damon Greer, The US-E.U. Safe Harbor Framework, Presentation at the Conference on Cross-Border Data Flows, Data Protection, and Privacy (October 2007), *available at* http://www.SafeHarbor.govtools.us/documents/1A_DOC_Greer.ppt.

[102] *See* J. Dhont et. al., Safe Harbour Agreement Implementation Study 105-7 (2004), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf. For the EC's own summary of the study, *see* European Commission, The Implementation of Commission Decision on the Adequate Protection of Personal Data Provided by the Safe Harbor Privacy Principles (2004), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf.

[103] *See* Press Release, FTC, Court Halts US Internet Seller Deceptively Posing as U.K. Home Electronics Site, August 6, 2009 (the FTC brought suit against a California company, inter alia, for falsely claiming in its privacy policy that it was certified under the SHA when it fact it was not). A few months later, the FTC announced proposed settlements in six more false claims cases, suggesting that the Commission is stepping up its Safe Harbor enforcement activity; *see* Press Release, FTC, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework (October 6, 2009).

[104] Galexia is a British management consulting firm that performed its own study based on the approximately 1,600 firms then listed on the Safe Harbor List. For a summary of the results, s*ee* Connolly, *supra* note 100.

Congress enacted the Children's Online Privacy Protection Act of 1998 (COPPA) to prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personal information from and about children on the Internet.[105] The statute and Final Rule[106] require an operator of a of web site directed at children, and of general audience web sites with actual knowledge that a user is a child, to meet the following five requirements: 1) notice of data collection and use practices; 2) "verifiable parental consent" prior to the collection, use, and/or disclosure of personal information from a child; 3) a "reasonable means for a parent to review" such information and to refuse to permit its further use or require its deletion; 4) a prohibition on conditioning a child's online activity "on the child disclosing more personal information than is reasonably necessary to participate in such activity"; and 5) establishing and maintaining adequate policies and procedures to protect the "confidentiality, security, and integrity of personal information collected from children."[107]

COPPA provides both federal and state enforcement mechanisms and penalties against operators who violate the provisions of the implementing regulations.[108] The statute by its terms also establishes an alternative means of compliance for operators that follow self-regulatory guidelines if issued by an industry representative or others and approved by the FTC under a notice and comment procedure.[109] There are three key criteria for safe harbor approval. Self-regulatory guidelines must: (a) meet or exceed the five statutory requirements set forth above; (b) 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 (c) 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.[110]

The avowed purpose of the COPPA safe harbor is to facilitate industry self-regulation and it does so in two ways. First, operators that comply with approved self-regulatory guidelines are "deemed to be in compliance" with all regulatory requirements.[111] To benefit from safe harbor treatment, operators need not individually apply for approval as long as they in fact fully comply with approved guidelines that are applicable to their business. According to the COPPA Final Rule, such compliance serves "as a safe harbor in any enforcement action" under COPPA unless the guidelines were approved based on false or incomplete information.[112] Second, the safe harbor allows "flexibility in the development of self-regulatory guidelines" in a manner that "takes into account industry-specific concerns and technological developments."[113] Industry groups interested in providing safe harbors must submit their self-regulatory guidelines to the FTC for approval. The FTC will then act on the application within 180 days of the filing

[105] Pub. L.105-277, Div C, Title XIII, § 1302, 112 Stat. 2681-728 (codified at 15 U.S.C. §§ 6501-6506 (1998)).

[106] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999)(codified at 16 C.F.R. pt. 312 (1999))[hereinafter, COPPA Final Rule].

[107] *See* COPPA, 15 U.S.C. § 6502, 16 C.F.R. § 312.3(a)-(e).

[108] COPPA, 15 U.S.C. §§ 6502(c) and 6504.In April 2002, the FTC conducted a survey of the information collection practices of 144 children's websites and found that that the general trend of the sites is one of increased compliance, even though some COPPA provisions, such as requirements about specific disclosures, have been followed less consistently. *See* FTC, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE (2002), *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf. The Commission has also settled nine cases for violation of the COPPA Rule, including two that each resulted in civil penalties of $1 million; *see* FTC, Children's Privacy-Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.

[109] COPPA, 15 U.S.C. § 6503; *see generally* 16 C.F.R. § 312.10.

[110] *See* 16 C.F.R. § 312.10(b)(2).

[111] COPPA, 15 U.S.C. § 6503(a)(2).

[112] COPPA Final Rule, 64 Fed. Reg. at 59,906.

[113] *Id.* According to the FTC, self-regulatory program are desirable because they "often can respond more quickly and flexibly than traditional statutory regulation to consumer needs, industry needs and a dynamic marketplace." *See* FTC, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS (2007) 22-23, *available at* http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf [hereinafter, FTC COPPA REPORT]. Similarly, the Final Rule emphasizes the flexibility of industry guidelines by making explicit that required assessment mechanisms and compliance incentives are not considered as mandatory practices but rather as "performance standards" and that the listed methods are only "suggested means for meeting these standards." See COPPA Final Rule, 64 Fed. Reg. at 59,907.

and after the proposed guidelines have been subject to notice and comment.[114] To date, the FTC has reviewed five safe harbor programs and approved four of them after requiring that three of the applicants revise or clarify certain program requirements in response to public comments.[115]

Critics of COPPA complain that the parental consent mechanism is ineffective and that even though the law offers certain protections, it does not prevent marketing firms and list brokers from profiling children.[116] Despite these criticisms, when the FTC submitted to Congress its review of the effectiveness of the COPPA implementing rule, it concluded that the COPPA safe harbor program "has been successful in complementing the FTC's enforcement of COPPA and should be given continued support."[117]

A brief assessment of CARU's monitoring and complaint-handling system further confirms the success of the safe harbor program from an enforcement standpoint.[118] Between 2000 and 2008, CARU reported on almost 200 cases; a few originated in consumer complaints and the rest resulted from CARU's routine monitoring of web sites that may be reasonably expected to attract children or teen users.[119] Issues ranged from inadequate privacy policies to the lack of a neutral age-screening process to collection or disclosure of PII from children without parental consent. All of the cases were resolved by the company in question agreeing to change its practices as directed by CARU. In addition, CARU referred one case to the FTC that resulted in a $400,000 settlement;[120] in a second case, the respondent entered into a consent decree with the FTC that included signing up for the CARU safe harbor;[121] and in a third case, the FTC initiated a COPPA law suit based in part on CARU's determination of compliance shortcomings.[122] This is an impressive record considering that since 2000, the FTC has brought a total of only fourteen COPPA enforcement cases. In short, it seems clear that CARU's compliance review and disciplinary procedures have been successful in complementing FTC's enforcement of COPPA and allowing the Commission to focus its resources on high profile matters.[123]

There are two serious weaknesses with the COPPA safe harbor programs, however. The first is that very few firms have signed up. CARU has the fewest members (about 10) while Privo has 22 and ESRB and Truste have about 30 each.[124] All told, fewer than 100 firms have been certified under approved safe harbor programs (although some of the ESRB and Truste certifications cover multiple web

[114] *See* 16 C.F.R. §§ 312.10(c)(1) and (2).

[115] The approved industry groups are the Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus (CBBB), the Entertainment Software Rating Board (ESRB), Truste and Privo, Inc. The FTC received seven public comments in response to CARU's application; two in response to ESRB's; two in response to Truste's; and seven in response to Privo's, which was approved without revision. For application materials, public comments and FTC approval letters, *see* FTC, Children's Privacy-Safe Harbor Program, http://www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.

[116] Parental verification mechanisms are considered costly and inconvenient for parents yet ineffective in achieving their broader purpose since Internet savvy children learn how to evade the requirement by claiming that they are over 13. Moreover, none of the available consent mechanisms establish that the adult granting consent is indeed the parent of the child in question. For a discussion of these and related points, s*ee* EPIC, CRITICISMS OF COPPA, http://epic.org/privacy/kids/default.html. For a discussion of weaknesses of COPPA from a family law perspective, *see* Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751 (Fall, 2001).

[117] FTC COPPA REPORT, *supra* note 113 at 24.

[118] CARU was established in 1974 by the National Advertising Division (NAD) of the CBBB, and has long experience in advertising review and dispute resolution. NAD maintains an archive of publicly available case reports of all formally opened cases involving the failure of a participating web site to voluntarily comply with the CARU guidelines, which makes this assessment possible. *See* National Advertising Division, Case Reports and Procedures, http://www.nadreview.org/search/search.aspx?doctype=1&casetype=2.

[119] All four safe harbor programs periodically monitor their member web sites, whereas CARU also monitors non-member web sites.

[120] *See* FTC, Press Release, UMG Recordings, Inc. to Pay $400,000 to Settle COPPA Civil Penalty Charges (Sept. 13, 2006).

[121] *See* FTC, Press Release, Imbee.com Settles FTC Charges Social Networking Site for Kids Violated the Children's Online Privacy Protection Act (Jan. 30, 2008).

[122] *See* FTC, Press Release, Web Site Targeting Girls Settles FTC Privacy Charges (Oct. 21, 2001).

[123] *See* FTC COPPA REPORT, *supra* note 113 at 23-24.

[124] Email from Joanne Furtsch, Senior Privacy Architect, Truste to Ira Rubinstein, Adjunct Professor of Law, New York University School of Law (Sept. 17, 2009)(on file with author); telephone Interview with Phyllis B. Spaeth, Associate Director, CARU (Sept. 23, 2009); telephone Interview with Dona J. Fraser, Director, Privacy Online, ESRB (Sept. 28, 2009); email from Stephen Kline, Vice President, Public Affairs, Privo to Ira Rubinstein (Sept. 29, 2009)(on file with author).

sites). The most likely explanation for this low rate of participation is that deemed compliance is not a strong enough incentive to persuade a firm to bear the costs of joining a safe harbor program and abiding by its guidelines when it has to comply with all but identical statutory requirements in any case. (Moreover, the COPPA Rule permits a firm to claim safe harbor benefits even though it has not joined a program but instead relies on internal processes for compliance and enforcement.) A second serious weakness is that contrary to the FTC's intent, the COPPA regulations are neither very flexible nor do they take into account "industry-specific concerns and technological developments." Although the Commission expressly characterized the assessment mechanisms and compliance incentives described in the Final Rule as "performance standards" that may be satisfied by equally effective alternatives,[125] a review of the self-regulatory guidelines of CARU, Truste, ESRB and Privo shows relatively little differentiation by sector, technology, or innovative methods of assessment or compliance.[126] Rather, the reason firms participate in safe harbor programs is probably due to a desire to share in the brand recognition of the program seal; to develop a closer working relationship with FTC staff; and to draw on the additional expertise of program staff.

## III. ARE SAFE HARBORS THE ANSWER?

This Article began with an historical review of the self-regulatory approach as a sometimes favored policy tool of the FTC and then analyzed the arguments for and against self-regulation from the perspective of privacy scholarship and law and economics. Next, it presented three case studies of voluntary, partially mandated and fully mandated self-regulatory programs. This Part shifts gears from the descriptive to the normative, first by arguing that statutory safe harbors are more effective than any other form of privacy self-regulation and, second, by conceptualizing new models for privacy safe harbors based on insights derived from advances in environmental regulation. Finally, the Article sketches in a few details of safe harbors designed to (a) combine the best elements of law and self-regulation to address hard issues such as behavioral targeting and (b) allow companies to experiment with privacy guidelines that go "beyond FIPPs" in various ways or that even supplant the traditional emphasis on FIPPs in favor of new approaches to privacy protection.

### *A. Advantages of Safe Harbors*

This section proceeds in a very straightforward manner. First, it crystallizes the various objections to privacy self-regulation that were highlighted in Parts I and II. Second, it argues that statutory safe harbors such as CARU overcome all of these objections largely due to the fact that they consist in a self-regulatory mechanism reinforced by state intervention. Third, it suggests that statutory safe harbors may achieve further advantages by drawing on what environmental law scholars Neil Gunningham and Joseph Rees call "industry morality."

The criticisms of self-regulatory privacy programs boil down to four points: first, that program guidelines are incomplete because they incorporate FIPPs in a selective and self-interested manner; second, that market incentives are insufficient to overcome free rider problems resulting in low industry adoption rates; third, that programs rely on weak oversight and enforcement mechanisms; and, fourth, that programs suffer from a lack of transparency, both during their formation and in their ongoing operations.

*1. Completeness.* - The FTC reports and published reviews of the NAI guidelines and the SHA seal programs persistently note the failure of self-regulatory programs to address *all* of the FIPPs or to do so in a sufficiently robust manner. For example, the original NAI Principles were considered weak on

[125] COPPA Final Rule, 64 Fed. Reg. at 59,906-907.

[126] ESRB is a trade association for the gaming industry and draws all of its members from this sector, but this seems to be have little to do with any differences between its guidelines and those of the other three COPPA safe harbor programs. In addition, although Privo is unique in offering its own turnkey identity solution, which handles children's registration and parental consent under COPPA, this seems more like a business decision than a direct response to COPPA's "flexible" regulations.

notice, choice and access (we address enforcement separately below) and critics were not much happier with the retrograde forms of notice, choice and access permitted under the 2009 revised principles. The SHA seal programs fare better in terms of formulating program guidelines that adhere to all of the Privacy Principles. However, both the EU study and the report by Galexia found that a high percentage of participating firms did not incorporate all seven of the agreed upon Privacy Principles in their own posted privacy policies.[127] Only the COPPA safe harbor programs achieve full coverage of substantive privacy requirements as might be expected given the FTC's mandatory review of program guidelines, all of which must offer principles that "meet or exceed" statutory requirements. This is equally true of CARU and the other three approved safe harbor programs. Indeed, the COPPA Rule requires that applicants submit a comparison of the requirements of the COPPA Rule with the corresponding provision of the proposed guidelines and the FTC acts on their request for approval only after subjecting the proposal to a formal notice and comment procedure. This is not to say that every firm that participates in an approved COPPA safe harbor program is in full compliance with the Rule. Rather, the point is that unlike industry guidelines, which often establish weak standards that fall short of FIPPs, a statutory safe harbor has mechanisms designed to overcome this problem by evaluating proposed guidelines against the privacy standards defined by statute and requiring complete convergence as a condition of approval.

*2. Free Rider Problems.* – Gunningham and Rees identify two main versions of the free rider problem as it affects companies deciding whether to participate in a self-regulatory program: first, some firms may agree to join a program but merely feign compliance; second, certain firms in the relevant sector may simply refuse to join at all. Both versions are potentially fatal to self-regulatory schemes because they create a competitive disadvantage for legitimate participants. The first version may be counteracted by "peer group, shaming or more formal sanctions" while the second may require that "government intervenes directly to curb the activities of non-participants."[128]

Both versions of the problem seem to have applied to the NAI in its early years. As the WPF study observed, the FTC was unsuccessful in maintaining a serious threat of government regulation and NAI membership rapidly deteriorated once Muris announced his new agenda and Congress failed to enact privacy legislation. Moreover, by creating a category for "Associate Members" (who were not required to abide by the NAI Principles), NAI institutionalized the problem of half-hearted participation. This improved only after FTC re-engaged on behavioral advertising with new workshops and reports and advocacy groups began filing complaints with the Commission objecting to both the profiling practices of network advertising and search firms, and to proposed mergers involving the leading players. It remains to be seen whether this cycle will repeat itself now that the FTC is again encouraging self-regulation. The SHA also suffers from both problems: many firms self-certify their adherence to the Privacy Principles without even revising their posted privacy policies in accordance with SHA requirements, and the roughly 2,000 companies on the DOC's Safe Harbor List represent only a small fraction of firms that transfer data from the EU to US, even if one excludes those that rely on alternative methods for demonstrating adequacy. Of course, the near absence of SHA enforcement over the past eight years only intensifies the free rider problems, since firms that join but feign compliance or simply refuse to comply generally suffer no adverse consequences. Once again, only the COPPA safe harbor programs are successful at curbing free rider problems. The number of CARU investigations seems high enough to discourage feigned compliance, especially given CARU's willingness to refer cases to the Commission and the FTC's aggressive enforcement stance with respect to children's privacy issues. Finally, firms that refuse to join an approved safe harbor program gain little competitive advantage since they remain subject to the legal requirements of COPPA and the FTC's specific regulatory authority under the COPPA Rule.

*3. Oversight and Enforcement.* – At an early stage of the US government's support for self-regulatory privacy guidelines, the DOC commissioned a study of the criteria for effective self-regulation. In addition to substantive criteria based on FIPPs, the DOC study identified three criteria addressing

[127] For example, according to the report by Galexia, only 348 of the total 1,597 companies registered for safe harbor were in compliance with the Enforcement Principle and only 209 offered an affordable dispute resolution process; *supra* note 100 at 7.

[128] Gunningham and Rees, *supra* note 6 at 393-96.

oversight and enforcement. They are: (1) consumer recourse, or the availability of affordable mechanisms for resolving complaints and perhaps awarding some compensation to an injured party; (2) verification, or the nature and extent of audits or more cost-effective ways to verify that a companies' assertions about its privacy practices are true and to monitor compliance with a program's requirements; and (3) consequences for failure to comply with program requirements, such as cancellation of the right to use a seal, public notice of a company's non-compliance, or suspension or expulsion from the program.[129]

With respect to consumer recourse, the NAI Principles make formal provision for consumers to file complaints (which are now handled in-house) but are silent on remedies. Given how little consumers understand about profiling practices, it seems unlikely that they will be able to determine which NAI firm might be misusing their data or whether any violation of the principles has occurred. Studies of the SHA suggest that no consumer complaints have been filed, either with safe harbor seal programs or EU data protection officials. The complaint record of CARU is somewhat better although still disappointing—only a small number of almost 200 investigations originated in consumer complaints (but all were resolved satisfactorily).

The NAI is no more successful on verification. Its track record on compliance audits is extremely poor—it is not clear whether any have occurred during its nine years in operation. The SHA relies on self-assessment or outside compliance reviews to meet the verification requirement but neither of the two studies discussed above had access to any relevant data regarding audit performance, so it is difficult to reach a firm conclusion. On the other hand, any misrepresentation of a firm's preferred method of verification is actionable by the FTC under its Section 5 enforcement powers, and this may provide sufficient incentives for firms to fulfill this requirement. COPPA requires that approved safe harbor programs engage in ongoing monitoring of their members' practices to ensure compliance with program guidelines and the participant's own privacy notices. CARU's strong record of investigating compliance issues identified in complaints or as a result of routine monitoring (coupled with FTC's higher profile enforcement actions) rebuts the usual charge that self-regulatory programs are weak on enforcement. To the contrary, the COPPA safe harbor programs, like other well-organized and committed industry groups, "help free up scarce government regulatory resources to address the recalcitrant few rather than the compliant majority."[130]

As for consequences for failure to comply, the NAI, the SHA seal programs and the COPPA safe harbors all rely on a similar mix of revocation, public suspension of membership and referral to the FTC. The SHA permits (but does not require) compensation to individuals for losses incurred as a result of non-compliance. Additionally, the DOC maintains a searchable, online list of organizations that adhere to the SHA principles and their certification and compliance status.[131] The CARU program stands out both for publishing case reports on non-member compliance issues and for having, in fact, referred several cases to the FTC.

*4. Transparency.* – As Gunningham and Rees observe, the effectiveness of self-regulation depends enormously on transparency and, in particular, "on the system's ability to produce and promulgate two kinds of information: (1) about the normative standards the industry has set for itself; and (2) about the performance of member companies in terms of those standards."[132] The public announcement of privacy principles has never been a problem for organizations that develop voluntary guidelines; they simply post the guidelines on their websites. In the case of the NAI, the FTC also published the NAI Principles as an Appendix to its July 2000 Online Profiling Report. That said, the

[129] *See* DEP'T OF COMMERCE, ELEMENTS OF EFFECTIVE SELF-REGULATION, *supra* note 25.

[130] *See* Sinclair, *supra* note 6 at 537; IAN AYRES & JOHN BRAITHWAITE, RESPONSVIE REGULATION 129 (1992)("A fundamental principle for the allocation of scare regulatory resources ought to be that they are directed away from companies with demonstrably effective self-regulatory systems and concentrated on companies that play fast and loose").

[131] Almost 2000 organizations have self-certified; *see* Dep't of Commerce, Safe Harbor List, *available at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Sept. 2, 2009). Many of the listed firms are shown as "non-current" under certifications status but there is not a single entry under compliance status.

[132] Gunningham and Rees, *supra* note 6 at 383.

preliminary discussion of these principles between the NAI firms and the FTC was far less transparent—the talks took place largely behind closed doors. In 2009, NAI decided on a very different approach: it not only published draft principles for public comment but then issued revised principles and simultaneously published a 50-page summary of these comments along with its own responses to this feedback, which in many cases consisted in changing the draft principles.[133] Of course, the SHA Privacy Principles were announced in the Federal Register, while the FTC followed a notice and comment procedure in developing the COPPA Rule.[134] Although the NAI's approach in 2009 resembled the FTC's notice and comment procedure and was highly transparent, there was a decisive difference: in one case, an industry trade group held the pen and made final decisions on how to balance public comments against industry goals; in the other, a government agency balanced public comments against the requirements of a law duly enacted by Congress with the participation of the marketing and online industries, the FTC, privacy groups, and First Amendment organizations.[135]

The creation and use of systems of performance monitoring have proven far more difficult, regardless of whether a firm participates in a voluntary or government-defined safe harbor program. Thus, the NAI initially promised random audits by seal programs but it is unclear whether these ever occurred; in any case, the results were never published. Under the NAI's newly announced Compliance Program, NAI staff will conduct annual compliance reviews of member companies and post a summary of the results on the web site.[136] The SHA allows firms to meet the verification requirements of the Enforcement Principle either through self-assessment *or* outside compliance reviews. Under the former, the firm must have in place "internal procedures for periodically conducting objective reviews" and must retain any relevant records and make them available upon request in the context of an investigation or a complaint but has no obligation to share this information with third parties. The same record keeping requirement applies in the case of outside reviews subject to the same limitation. Thus, both internal and external compliance reviews remain opaque. As noted above, the COPPA Rule requires periodic compliance reviews or other effective assessment mechanisms but makes no provision for publishing these reviews or any underlying data.

*5. Other Advantages.* – This section has so far focused on the advantages of safe harbors as compared to voluntary and partially mandated forms of self-regulation when assessed against the four criteria of completeness, free rider problems, oversight and enforcement, and transparency. This final section starts from a more general observation about all self-regulatory programs in which member firms cooperate with each other to establish a code of practice, namely, that this activity entails the development of an industry-wide normative framework. Gunningham and Rees refer to this framework as an "industrial morality" and identify seven common features which, for the sake of brevity, may be reduced to two key points.[137]

The first point is that industrial morality is a form of "moral discourse capable of challenging conventional industry practices." As the two authors note, self-regulatory guidelines require that firms come together and engage in a deliberate and normative discussion of the principles that should guide their activities with respect to a public policy goal such as privacy protection. This inevitably involves candid reflections on how a company *should* handle information processing challenges both in terms of its own business model and as compared to other firms in the industry. Moreover, as cooperation and trust increase among the participating firms, so too do candor and critical thinking. The two authors describe a process of collective soul-searching "where industry officials question their customary ways of doing

[133] *See* NAI, Response to Public Comments Received on the 2008 NAI Principles Draft (Dec. 16, 2008), http://www.networkadvertising.org/networks/NAI%20Response%20to%20Public%20Comments_Final%20for%20Website.pdf (summarizing the public comments received on its draft principles and its responses to that feedback).

[134] The agency received 132 comments in response to its Notice of Proposed Rulemaking and held a public workshop to obtain additional information on the issue of how to obtain parental verification; *see* COPPA Final Rule, 64 Fed. Reg. at 59,888.

[135] *See* 144 Cong. Rec. S11657 (Statement of Sen. Bryan).

[136] *See* NAI Compliance Program Attestation Review Process (2009), www.networkadvertising.org/.../NAI_COMPLIANCE_AND_ENFORCEMENT_PROGRAM_Attestation_Review_detail.pdf.

[137] Gunningham and Rees, *supra* note 6 at 376-80.

business, including their taken-for-granted economic assumptions, weigh the alternatives, and think through the consequences of their choices."[138] Thus, the very act of participating in the drafting of self-regulatory principles provides company representatives with a highly relevant basis for questioning how their own firms do business. At the same time, achieving consensus as to industry principles lays the foundation for future compliance by forming an "expectation of obedience." Certainly, legal norms contribute to this expectation since agreement to industry principles may result in legally enforceable obligations (for example, online advertising firms that agree to abide by the NAI Principles are legally accountable for any misstatements of company practices). But Gunningham and Rees explain obedience more in terms of moral and social norms, noting that "it becomes harder for a member company to reject a norm after treating it seriously and at length in industry deliberations."[139] In effect, the process of creating or even signing up for industry principles presupposes that someone in a firm champions these principles internally and lobbies internally for their approval by executives. This, in turn, empowers these champions to use moral suasion with firm management to ensure that the company satisfies its industry-wide commitments.[140]

This moral discourse leads directly to a second point, which is that industrial morality creates a "normative framework that defines and upholds a special organizational competence." For members of the self-regulatory groups under consideration here, this translates into the capacity to manage privacy within a complex business organization, and coincides with the rise (over the past decade) of the Chief Privacy Officer (CPO) and the increasingly strategic role of this position within leading IT firms.[141] This trend coincides with the growing professionalization of the role.[142] While employment of a CPO is no guarantee of improved levels of privacy protection, it does seem to help.[143]

In sum, based on this analysis of the three case studies, it seems fair to conclude that a hybrid approach, combining complementary components of self-regulation and prescriptive law improves both the efficiency and effectiveness of industry guidelines. In the words of Gunningham and Rees, "there is reason to believe that self-regulatory mechanisms underpinned by some form of state intervention are more resilient and effective than self-regulation in isolation."[144]

### *B. "Second Generation" Strategies For Privacy Safe Harbors*

Having established the superiority of statutory safe harbors over self-regulatory programs lacking any basis in law, we now turn to ideas for making safe harbors even better. In a path breaking article published in 2006, legal scholar Dennis Hirsch discussed the possibilities of developing a new model for privacy regulation based on a number of innovative environmental policy tools that have emerged over the past thirty years. Hirsch contrasts the older, command-and-control model with a "second generation" of environmental regulations that "encouraged the regulated parties themselves to choose the means by which they will achieve environmental performance goals" resulting in "more cost-effective and

---

[138] *Id.* at 377.

[139] *Id.* at 379.

[140] *See* Gunningham, *supra* note 6 at 69.

[141] *See* Christopher Brown, *Privacy Officers: Survey Finds Increasing Number of Firms Appointing Officers with Institutional Clout*, 1 PRIV. & SEC. L. REP. 78 (2002); *see also* Deirdre Mulligan and Kenneth Bamberger, *From Privacy on the Books to Privacy on the Ground: The Evolution of a New American Metric* (unpublished paper on file with author)("Within many Fortune 500 companies CPOs are directors or … executives, signaling that privacy is viewed as a strategic matter").

[142] The International Association of Privacy Professionals (IAPP) boasts 6,000 members and offers a certification program in corporate privacy compliance; *see* IAPP Membership, https://www.privacyassociation.org.

[143] *See* Peter Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 Minn. L. Rev. 1263, 1316 (2002) (noting with respect to CPOs that "…having a person visibly responsible for privacy is a helpful way to ensure that privacy issues are considered in the organization's actions. Privacy concerns may or may not win out in the eventual decisions, but having a person expert in privacy in the process means that the other participants at least have to articulate why the proposed actions are consistent with the organization's announced privacy policies").

[144] Gunningham and Rees, *supra* note 6 at 366; *see also* Sinclair, *supra* note 6 at 532.

adaptable" strategies.[145] The defining characteristic of second generation strategies is that they "allow these self-directed actions to count towards regulatory compliance." This radical departure from a command-and-control regime spurs regulatory innovation by harnessing a firm's own ingenuity in devising environmental solutions that meet or exceed legal requirements yet fit a firm's business model and the needs of its customers. As Hirsch points out, this strength of second generation strategies is also a source of weakness insofar as enforcement becomes more challenging when firms choose how and when to achieve regulatory goals as opposed to following a uniform national standard. Thus, these innovative strategies work best where reliable monitoring technologies exist as is the case in controlling air pollution by reducing emissions of specific hazardous pollutants.[146]

### *1. Privacy Covenants*

Hirsch argues that privacy regulation has much to learn from these second generation environmental strategies and he proposes several ideas for adapting them to protecting information privacy without deterring innovation. His most relevant idea for present purposes is the use of environmental covenants. Under this approach, "government officials sit down with the regulated industry and hammer out an agreement" on a disputed issue such as pollution reduction. The negotiations often take place in the context of a credible threat of tougher regulation if no agreement is reached and may include other stakeholders at the bargaining table such as environmental advocacy groups. Industry finds these covenants attractive because they have more input into the final agreement than with conventional rulemaking efforts, the covenants take the form of performance goals rather than technology mandates, and their longer time frame "fits with the normal cycles of business planning and investment." Government and society benefit from this approach by achieving better results (such as steeper pollution reductions) than might otherwise be politically achievable. Finally, the proof that all parties view these results as superior is that they entered into the covenants voluntarily.[147]

In the US, there is at least one precedent for privacy covenants in the form of a negotiated agreement. In the winter of 2006, Yahoo, Google and Microsoft had to contend with highly unfavorable publicity and Congressional hearings over their roles in cooperating with Chinese government efforts to monitor and censor the Internet.[148] A few months later, Rep. Chris Smith introduced a bill that would've rendered such assistance illegal and forced US companies to confront a Hobson's choice between disregarding a raft of licensing requirements imposed by Chinese authorities as a condition of providing Internet services in the local market or obeying Chinese censorship rules in violation of US law.[149] The companies then sat down with a cross-section of human rights organizations, academics, and socially

[145] *See* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law*, 41 GEORGIA L. REV. 1, 8 (2006). For a book length discussion of second generation environmental strategies, *see* DANIEL J. FIORINO, THE NEW ENVIRONMENTAL REGULATION (2006).

[146] *Id.* at 37-39; *see* Fiorino, *id.* at 139.

[147] Hirsch, *id.* at 51-53. Fiorino and Hirsch discuss Project XL as an example of environmental covenants. The Clinton Administration announced this initiative in May 1995 as part of its program for reinventing environmental regulation. Project XL provided a limited number of responsible companies "the flexibility to replace the requirements of the current system at specific facilities with an alternative strategy developed by the company" provided that the alternative strategy met five conditions: (1) superior performance superior as compared to that which would be achieved by full compliance with current laws and regulations; (2) transparency; (3) avoidance of "worker safety or environmental justice problems"; (4) support from the community surrounding the facility; and (5) enforceability. *See* CLINTON & GORE,, REINVENTING ENVIRONMENTAL REGULATION, *supra* note 17. The Environmental Protection Agency set a goal of implementing 50 pilot projects in several different program areas including both facilities-based and industry-wide or sector-based programs; *see* Regulatory Reinvention (XL) Pilot Projects, 60 Fed. Reg. 27282 (May 23, 1995). For a discussion of how Project XL implemented the covenanting approach, *see also* Fiorino, *id.* at 140-44; Dennis D. Hirsch, *Project XL and the Special Case: The EPA's Untold Success Story*, 26 COLUM. J. ENVTL. L. 219, 224-27 (2001). For a broader analysis of the technique of negotiated rulemaking (informally known as "reg-neg," see PETER SCHUCK, FOUNDATIONS OF ADMINISTRATIVE LAW 367-70 (2003).

[148] Tom M. Zeller, Jr., *Online Firms Facing Questions About Censoring Internet Searches in China*, N.Y. TIMES, Feb. 15, 2006.

[149] Carrie Kirby, *Chinese Internet vs. Free speech: Hard Choices for US Tech Giants*, S. F. CHRONICLE, Sept. 18, 2005.

responsible investment firms to work on voluntary guidelines to protect freedom of expression and privacy on the Internet. After two years of negotiations, a multi-stakeholder group launched the Global Network Initiative (GNI) and jointly committed to principles, implementation guidelines, and an accountability system based on independent, third-party assessments.[150]

Although spurred by a combination of negative publicity and a threat of government intervention, the GNI negotiations were an entirely voluntary effort, with no legal mandate as to process or substance. Instead, the parties proceeded on an ad hoc basis and agreed to principles that—while based on international human rights instruments—were not subject to any formal approval criteria or government oversight. (The US State Department supported the GNI initiative but did not participate in any stakeholder meetings.) For examples of privacy codes that have been negotiated on a statutory basis, it is necessary to look overseas, principally to the Netherlands and Australia (and New Zealand, in passing) and, by analogy, to a covenanting approach called "enforced self-regulation" in which individual firms draft their own set of corporate rules, subject to public ratification by an administrative agency.[151]

Dutch data protection law allows industry sectors to draw up codes of conduct for processing of personal data, which are submitted to the Dutch Data Protection Authority (DPA) for review and approval.[152] According to Hirsch, the Dutch have approved twelve such codes covering various industry sectors, each with its own tailored compliance plan that is nevertheless consistent with the broader requirements of the Dutch data protection law.[153] This Dutch approach, which is generally consistent with that of the EU Data Directive,[154] resembles the COPPA safe harbor and has many of the same advantages: It allows a more expansive role for industry in shaping the final regulatory outcome against a backdrop of enforceable privacy rights; addresses free rider problems given that firms remain subject to Dutch privacy mandates irrespective of their decision to abide by an industry code; and ensures that the government has a clear right to enforce the code of conduct.

Australia also follows a co-regulatory approach by permitting organisations to develop specialized codes for the handling of personal information. According to the Australian Privacy Commissioner, these codes were "designed to allow for flexibility in an organisation's approach to privacy, but at the same time, guarantees consumers that their personal information is subject to minimum standards that are enforceable in law."[155] The relevant sections of the Australian Privacy Act impose detailed requirements that a privacy code must satisfy to win approval. In particular, a code must incorporate all of the relevant FIPPs (which Australian law refers to as National Privacy Principles or NPPs) or set forth obligations that are "at least the equivalent of" the NPPs; specify the organizations to which NPPs apply; and permit organizations to develop their own complaint-handling procedures, such as appointing the Commissioner or a third party as an independent adjudicator to whom complaints may be

---

[150] For the three core commitment documents of the GNI, *see* http://www.globalnetworkinitiative.org/index.php. There are several other examples of multi-stakeholder processes designed to achieve basic human rights including the Fair Labor Association Workplace Code of Conduct, the Equator Principles, the Voluntary Principles on Security and Human Rights, and the Extractive Industries Transparency Initiative. For a discussion of multi-stakeholder agreements in the context of the intersection of business and human rights, *see* John Ruggie, *Protect, Respect and Remedy: A Framework for Business and Human Rights*, A/HRC/8/5 (2008), *available at* http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf.

[151] *See* Ayres & Braithwaite *supra*, note 130, Chap. 4.

[152] *See* the Dutch Personal Data Protection Act (PDPA), Chap. 3, art. 25(1), *available and translated at* http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml. This provision requires the Dutch DPA to issue an opinion as to whether the rules in a code "properly implement" Dutch law; if so, this declaration is deemed to be the equivalent of a binding administrative decision. This declaration is similar in effect to FTC approval of COPPA safe harbor guidelines such that Dutch firms that comply with an industry code are deemed to be compliance with the Dutch PDPA.

[153] Hirsch, *supra* note 145 at 54-56.

[154] *See* Council Directive 95/46/EC, Article 27(1), which states that "Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors." Ireland also has approved three codes of practices under its data protection law; *see* Irish Data Protection Commissioner, Self Regulation and Codes of Practice, *available at* http://www.dataprotection.ie/viewdoc.asp?DocID=98.

[155] *See* Office of the Federal Privacy Commissioner, Guidelines on Privacy Code Development 16 (2001) (hereinafter Code Guidelines*), available at* http://www.privacy.gov.au/materials/types/download/8634/6482.

made.[156] In addition, the Commissioner must be satisfied "that members of the public have been given an adequate opportunity to comment on a draft of the code."[157] Although codes are voluntary, approved codes are legally binding on any company that consents to be bound.[158] Not surprisingly, privacy codes in Australia have met with limited success; only three codes have been approved to date. According to one observer, the effect of the legislation was to give industry the option of complying with the NPPs with the Privacy Commissioner handling complaints as prescribed by statute, or developing and implementing its own privacy codes, which offered few advantages since the codes had to be at least as strong as the NPPs, and potentially shifted the costs of complaint handling to industry.[159]

In view of the complex and costly nature of the code approval process and the lack of interest by Australian industry, the Australian Law Reform Commission (ALRC) suggested various reforms of privacy codes such as specifying that approved codes operate in addition to the privacy principles, rather than replacing them, thereby promoting national consistency and reducing fragmentation and confusion. Under this approach, codes would provide specific and binding guidance on how the principles should be applied in particular sectors.[160] In response, the Australian Government largely adopted the first recommendation but noted that organisations may offer protections "in excess of those offered by the privacy principle but only to the extent that these protections do not derogate from the principles."[161] It also supported the idea of the Privacy Commissioner having the power to request the development of a privacy code by a defined group and, where an adequate code is not developed or approved, to not only devise a code but to make it mandatory for these groups, subject to a public consultation process.[162] The Government concluded that "This would result in a three tiered model for code development: codes voluntarily developed by organisations; mandatory codes developed at the request of the Privacy Commissioner; and where such a request is not complied with, a mandatory code developed by the Privacy Commissioner."[163]

Finally, Ayres and Braithwaite describe a variation on the co-regulatory model in which firms are "required to write their own set of corporate rules, which are then publicly ratified [and] publicly enforced."[164] What's unique about this model is that negotiations occur between a government agency and an *individual firm* and result in regulations that are *specific* to each firm. Under this model, "each firm in an industry is required to propose its own regulatory standards if it is to avoid harsher (and less tailored) standards imposed by the state." A regulatory agency would then review the proposal and seek comments from public interest groups (PIGs). Once approved, the rules would become binding on the individual firm and any violation of them would be punishable by law. In addition, companies would handle most enforcement duties by establishing independent, internal compliance groups to monitor company practices and recommend disciplinary action if violations occur. (And, where feasible, PIGs might be represented on this inspection group.) If management fails to rectify reported violations or fails to act on

[156] *See* Privacy Act, 1988, §§ 18BB(2) and (3).

[157] *Id.* at § 18BB(2)(f). The Code Guidelines describe the public consultation requirement in greater detail. Code proponents are required to submit a statement showing that they allowed at least six weeks for consultation and describing who is affected by the code, efforts to consult with affected groups, changes to the proposed code, a summary of any issues that remain unresolved and why, and a list of organizations likely to adopt the code; *supra* note 157 at 5-6.

[158] *Id.* at § 16A. New Zealand privacy law also treats approved codes of conduct as instruments of law with binding effect; *see* Privacy Act, 1993, § 46.

[159] Email from Malcolm Crompton, former Australian Privacy Commissioner (1999-2004), to Ira Rubinstein, Adjunct Professor of Law, New York University School of Law (Nov. 1, 2009) (on file with author).

[160] *See* Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC 108), Recommendation 48-1 *(*2008), *available at* http://www.austlii.edu.au/au/other/alrc/publications/reports/108/.

[161] Australian Government, First Stage Government Response to the ALRC Report, No. 48, Privacy Codes (2009), *available at* http://www.pmc.gov.au/privacy/alrc.cfm.

[162] *Id.* As the ALRC 108 Report noted, "the New Zealand Privacy Commissioner has the power to issue binding codes of practice that become part of the law. The codes may modify the application of one or more of the information privacy principles by prescribing: standards that are more or less stringent than the standards prescribed by the principle; or how any one or more of the principles are to be applied, or are to be complied with" (citations omitted); *see supra* note 160 at § 48.22.

[163] *Supra* note 161, No. 48, Privacy Codes.

[164] *Supra* note 130 at 4.

disciplinary recommendations, the director of the compliance group would be statutorily required to report such failures to the relevant agency, which would have enforcement powers. The agency would also share these reports with PIGs.[165]

According to Ayres and Braithwaite, this model has many strengths including *flexibility* (in the form of well-tailored rules that exactly match the unique contingencies of an individual firm and that could be rapidly adjusted to reflect changing conditions without affecting every firm in the industry); *innovation* (because firms may tap into their own ingenuity to devise custom-made, least-cost solutions); greater *commitment* (because companies write their own rules rather than having them imposed externally); and more effective *compliance* (because internal discipline is likely to be more extensive and cheaper for everyone than government investigations and prosecutions). On the other hand, the model has several obvious weaknesses including much higher administrative costs to approve a vastly larger number of rules each year (although this might be mitigated by allowing companies to adopt approved rules from other companies or even model rules suggested by a trade association); concerns that the independence of internal compliance groups could never be fully guaranteed; and a bias against small firms, which typically lack the resources necessary to negotiate differentiated standards or to stand up an independent compliance team.[166]

In sum, there are a number of subtly different models for privacy covenants depending on whether negations between the state and the private sector occur (1) under a threat of government intervention or under statutory guidelines; (2) at the sectoral or firm level; (3) in consultation with advocacy groups or with their participation at the table under a consensus model requiring their approval. The models also vary depending on whether codes (4) are legally binding or merely precatory; (5) may derogate from applicable legal standards by being both more or less stringent; and (6) may be initiated only by the private sector or may be requested by the government or even imposed on a recalcitrant sector or firm. The various combinations of these six factors in the previously discussed models are summarized below in Table 1:

| | *GNI* | *Dutch* | *Australian* | *New Zealand* | *Enforced Self-Regulation* |
|---|---|---|---|---|---|
| *Government oversight* | N | Y | Y | Y | Y |
| *Industry level* | Firm | Sector | Sector | Sector | Firm |
| *Role of Advocates* | At the table | Consultation | Consultation | Consultation | Consultation |
| *Legally Binding?* | N | Y | Y | Y | Y |
| *Derogation Allowed?* | Y | N | N | Y | N |
| *Who Initiates?* | Industry | Industry | Industry & Government (if reforms are enacted) | Industry & Government | Industry |

Table 1

If Congress wishes to include privacy covenants in future legislation, therefore, it has many models to choose from. A conservative approach to experimenting with covenants would be to modify the COPPA safe harbor provisions by adding several new elements based on the models discussed above. For example, Congress might grant the FTC broad discretion to approve self-regulatory guidelines for

[165] *Id. at* 101-10.

[166] *Id. at* 110-16, 120-28.

different industry sectors provided that (1) the organization seeking approval is sufficiently representative of the sector; (2) industry members and other interested parties, including privacy and consumer advocacy groups, attempt to reach consensus on a proposed code of conduct; (3) derogation is permitted to ensure maximum flexibility; (4) the Commission reviews the privacy code conduct under a notice and review process prior to approval; and (5) approved code bind only those companies who chose to be bound. Of course, this brief description raises more questions than it answers: Which trade associations should FTC negotiate with, especially if there are competing organizations with overlapping membership? How are firms and NGOs selected and how many should participate? May a large firm that has several different divisions and belongs to several trade groups participate in multiple negotiations and assume obligations under multiple codes? What about smaller firms that may not belong to any trade association—how do they ensure proper representation in negotiations that might affect them? If NGOs lack the necessary resources to staff negotiation sessions (which seems very likely), should government or industry help fund their participation? Should there be a specified period for completion of negotiations and/or submission of a draft code? Should negotiations occur in open sessions or behind closed doors with only stakeholders in attendance? If a firm or NGO walks out on the negotiating process, does the FTC retain discretion to commence a notice and comment process for a code that it nevertheless considers satisfactory?

For the covenanting approach to have any likelihood of success, Congress would also need to ensure that industry did not view the code-making process as requiring a high expenditure of resources while offering too few tangible benefits (as seems to be the case with both COPPA and the Australian codes). This requires not only well-designed legislation but far more deliberate attention than existing schemes give to developing the right combination of incentives.

As to the design issue, new federal privacy legislation would have to be expressed in terms of broadly stated principles that allow differentiation by sector in the form of more detailed codes of conduct. This in turn requires that Congress resist the temptation to set forth privacy principles in highly detailed or prescriptive terms that apply across the board.[167] For its part, the FTC would need to pay more than lip service to allowing flexibility in the development of industry guidelines and taking into account industry-specific concerns and technological developments.

As to incentives, Daniel Fiorino points out that government leverage in "getting participation, commitments and performance from industry … may come from either sticks or carrots."[168] In the environmental setting, 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. Firms that commit to achieving certain goals or that demonstrate high performance avoid these sticks and/or enjoy these carrots. What sticks and carrots might be devised to enhance the COPPA safe harbor, which relied almost solely on deemed compliance and a largely empty promise of regulatory flexibility?

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 a tiered liability system might make an excellent stick. Under this approach, new privacy legislation would allow civil actions and liquidated damages awards against firms that did not participate in an approved safe harbor program. Whereas compliance with approved self-regulatory guidelines would not only serve as a

[167] For example, a statute might include short provisions that encapsulate the core FIPPs of notice, choice, access, security and enforcement as well as more detailed provisions that articulate comprehensive requirements for each separate principle. In reviewing proposed codes of conduct, the FTC would evaluate them against these broadly stated principles and the approved codes would be binding on participating companies, even if they differ from the more detailed provisions of the statute. On the other hand, regulated entities that do not participate in an approved safe harbor program would have to comply with both the broad principles and the more prescriptive requirements, including any privacy regulations issued by the FTC.

[168] Fiorino, *supra* note 145 at 124.

safe harbor in any enforcement action but exempt program participants from civil law suits and monetary penalties.[169]

Just as harsher legal sanctions may induce companies to join a privacy safe harbor program, so too might lighter regulatory burdens. Thus, new privacy legislation would establish broad privacy protections based on FIPPs but might also include provisions allowing (1) industry groups to decide how best to meet these requirements (while non-participating firms would be subject to uniform FTC implementing regulations); (2) compliance based on self-assessments by participants and supervised by program sponsors, whose board might include representatives of advocacy groups (while non-participating firms would be subject to third-party compliance audits with the results reported to the FTC); (3) official, government recognition of superior performance by top tier performers in safe harbor programs (while non-participating firms would be ineligible for such recognition); and (4) purchase preferences if applicable. (The federal government gives a preference to Energy Star products; why not also give a preference to email, search or other Web technologies or services acquired from safe harbor firms?)

The last few paragraphs describe a proposed regulatory strategy in which federal privacy law would formally recognize differences in performance by treating safe harbor participants differently from non-participants. This is true of all safe harbor schemes; their function is to shield or reward regulated firms if they engage in desirable behavior as defined by statute. A few safe harbor provisions, like the small business exemption under Title VII, leave no doubt as to whether a regulated firm qualifies for differential treatment. But this is unusual; more often than not, the conditions for eligibility are sufficiently complex that litigation is required to sort them out and even then the courts often disagree.[170]

Under the covenanting approach as described above, the main eligibility requirement for safe harbor treatment is agreement to abide by a code of conduct that emerges by consensus from a multi-stakeholder process and is approved by the FTC under a notice and comment process. The assumption here is that when industry groups sit down with their advocacy counterparts "in the shadow of the law" and weigh the benefits their members may become eligible for if they agree to go "beyond" compliance, they may well reach consensus with advocates and other stakeholders, even though the latter may insist upon rigorous privacy protections in some areas while making concessions in others.[171]

The current controversy over online behavioral advertising seems ready made as a test case of the covenanting approach. If Congress today was ready to enact omnibus privacy legislation based on FIPPs,

---

[169] While tiered liability is a novel concept in privacy law, it is worth pointing out that *Black's Law Dictionary* defines safe harbor as a "provision (as in a statute or regulation) that affords protection from liability or penalty" and that such safe harbors are extremely common statutory devices. For example, the Private Securities Litigation Reform Act (PSLRA) of 1995 provides a safe harbor for projections of future economic performance if they meet a (much litigated) standard of good faith. Similarly, the safe harbor under § 512 of the Digital Millennium Copyright Act (DMCA) seeks to immunize online service providers from copyright liability if they adhere to certain guidelines designed to protect the rights of authors. In contrast, the § 230 safe harbor in the Communications Decency Act of 1996 provides complete immunity from liability for providers and users of an "interactive computer service" who publish information provided by others. Safe harbors may also take the form of exemptions from statutory requirements. For example, Title VII of the Civil Rights Act of 1964 does not apply to private sector employers with 14 or fewer employees, while the California security breach notification law (Ca. Civ. Code. 1798.82) only imposes notice requirement on "unencrypted data." Finally, some safe harbors permit regulated entities to engage in certain desired behavior provided they meet certain conditions. For example, the SHA treats US firms that self-certify as providing an adequate level of privacy protection and thereby permits transfers of EU data to the US; and the Federal Election Commission regulations allow a "corporation, labor organization, or qualified nonprofit corporation" to make an "electioneering communication" if they meet certain conditions set out in the safe harbor provisions of 11 C.F.R. 114.15(b), such as avoiding appeals to vote for or against a clearly identified Federal candidate.

[170] For example, courts have disagreed on whether the PLSRA safe harbor immunizes forward-looking statements that are accompanied by "meaningful cautionary statements" if the statements were false and made with actual knowledge of their falsity; c*ompare Freeland v. Iridium World Comm.*, 545 F.Supp.2d 59 (D.D.C. 2008) *with Beaver County Ret. Bd. v. LCA-Vision Inc.*, No. 1:07-CV-750, 2009 WL 806714 (S.D. Ohio Mar. 25, 2009); denied safe harbor protection under DMCA § 512 to firms that use peer-to-peer networking systems to facilitate file sharing over the Internet, *see A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); *In re Aimster Copyright Litigation*, 35 252 F. Supp. 2d 634, 648 (N.D. Ill. 2002), *aff'd,* 334 F.3d 643 (7th Cir. 2003); and denied § 230 immunity to an online roommate matching service that was potentially liable under the Fair Housing Act for requiring members to answer questions that potentially enabled other members to discriminate for or against them, *see Fair Housing Council of San Fernando Valley v. Roommate.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (*en banc*).

[171] For a discussion of industry self-regulatory programs that often go beyond compliance in achieving environmental goals, s*ee* Fiorino, *supra* note 145 at 139-52.

it might well reach an impasse over explicitly regulating firms engaged in targeted advertising. Some Members might insist on giving industry more time to adopt the FTC's proposed self-regulatory principles, while other Members might argue that the time for self-regulation has come and gone and that advocacy groups are right in demanding government enforced rules limiting the collection and use of both personal and behavioral data for online advertising purposes.[172] One way to break this impasse might be to create a pilot program based on the covenanting approach as described above. In a nutshell, Congress would authorize the FTC to approve a code of conduct for the online advertising industry provided it meets the five conditions identified above as the "conservative approach."

The pilot program could be modeled on § 6503 of COPPA but with several notable differences. For starters, it would apply second generation regulatory strategies to proposed codes of conduct such as greater regulatory flexibility and attractive incentives such as tiered liability as well as various other benefits. Additionally, the pilot program might include a provision suspending FTC rulemaking for a fixed period of time during which a multi-stakeholder process could be organized and reach a conclusion, along with a triggering device that would authorize the FTC to issue prescriptive regulations binding all firms if no codes were submitted and approved prior to the expiration of this suspension period. [173] During this time, the Commission would facilitate self-regulatory efforts by soliciting further public comments on the existing NAI Principles and IAB Principles, holding new public workshops to evaluate their success and failure in practice, encouraging industry to meet with advocacy groups and other stakeholders to hammer out a consensus, and even publishing its own views on what constitutes measures that go beyond compliance as well as reviewing appropriate incentives for participating firms.

### *2. A Performance-Based Approach*

The fate of any multi-stakeholder process largely depends on how the players assess their strategic options: are they better off cooperating with each other and reaching agreement on a code of conduct or trying to influence the FTC rulemaking process directly to achieve a more desirable outcome? Given the FTC's recent work on self-regulatory guidelines for targeted advertising, the somewhat skeptical remarks of Leibowitz and Vladeck regarding industry efforts, and the Commission's on-again off-again history with self-regulatory solutions, it is at least an open question as to which side (industry or the advocacy groups) would prosper if the stakeholders failed to reach consensus and the Commission issued a final rule. However, a covenanting approach is not the only way that Congress might experiment with second generation regulatory strategies. Recall the underlying premise of such strategies, which is to distinguish good performers from bad performers and treat them accordingly. Obviously, this requires reliable methods for measuring performance such as—in the environmental context—meeting targeted goals for reducing pollution or emissions.[174] Although privacy is much less susceptible to objective

---

[172] This roughly describes the current state of affairs. For the FTC staff report on self-regulatory guidelines in the online advertising industry, *see supra* note 90 and accompanying text. In a clear effort to fend off regulation, a consortium of advertising trade groups issued a set of privacy principles that closely tracked the FTC's recommendations; *see* Stephanie Clifford, *Industry Tightens Its Standards for Tracking Web Surfers*, N.Y. TIMES, July 1, 2009. The industry consortium included the Interactive Advertising Bureau (IAB), the American Association of Advertising Agencies (AAAA), the Association of National Advertisers (ANA), and the DMA. For the consortium's document, *see* SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, *available at* http://www.bbb.org/us/article/principles-on-collection-and-use-of-behavioral-advertising-data-released-11287. A privacy coalition responded by urging Congress to enact privacy legislation protecting consumers against the growing threat of online behavioral tracking and targeting; *see* Stephanie Clifford, *Privacy Advocates Push for New Legislation*, N.Y. TIMES, *Sept. 1*, 2009. For the coalition's document, *see* CENTER FOR DIGITAL DEMOCRACY, ONLINE BEHAVIORAL TRACKING AND TARGETING: LEGISLATIVE PRIMER SEPTEMBER 2009, *available at* http://www.democraticmedia.org/doc/privacy-legislative-primer.

[173] *See* Sinclair, *supra* note 6 at 536 (describing a trigger device in a somewhat different setting as "a classic example of self-regulation operating in the shadow of the law").

[174] Recall that Project XL offered flexibility from existing regulations in exchange for attaining environmental results that go beyond compliance. EPA considered eight criteria in evaluating pilot projects: environmental results; cost savings; stakeholder support; innovation; transferability; feasibility; monitoring, reporting and evaluation; and shifting of the risk burden. Four of these criteria (results, savings, innovation and monitoring) presuppose the availability of objective performance measurements. *See supra* note 147, 60 Fed. Reg. at 27287.

measurement than air or water quality, it is still possible to identify steps that should result in higher levels of privacy protection for consumers, thus qualifying firms for safe harbor treatment if they take these steps on a consistent basis.[175] This section concludes by briefly considering a holistic approach to assessing good privacy performance. It has three major sub-components: governance, methodologies, and practices.[176] Under this approach, Congress would authorize the FTC to identify specific measures under each heading that firms would need to implement in order to qualify for safe harbor treatment.

A brief summary of the argument so far is in order here. Any privacy legislation that Congress is likely to enact is bound to address the core FIPPs: notice, consent, access, security and enforcement. Under such a statute, firms would be obliged to provide notice via a privacy statement, offer relevant consent choices depending on their data collection and use practices, provide reasonable access to personal data and a limited ability to correct or amend that data, and implement reasonable security practices. Mere compliance with these legal requirements *should not* entitle a firm to safe harbor treatment. Rather, the point of second generation strategies like those described above is to reserve safe harbors benefits for top tier firms that go beyond compliance as determined by suitable performance measures. Congress needs to devise appropriate incentives to achieve this policy goal. But the focus here is with selection criteria for identifying firms that provide customers with a higher level of privacy protection and hence merit safe harbor treatment. To be clear, this is an alternative method of qualifying firms for a safe harbor and those that satisfy these selection criteria would *not* have to participate in a multi stakeholder process that achieves consensus.

In devising the selection criteria that fit this task, Congress should begin by addressing data governance, 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."[177] Firms that implement data governance systems typically meet one or more of the following criteria: (1) designation of a Chief Privacy Officer (CPO) or similar executive level position with overall responsibility for setting privacy protection policy and standards within a firm and managing risks and impacts of privacy-affecting decisions;[178] (2) publicizing within the company who has authority and accountability for governance decisions; (3) deployment of sufficient staff and budget throughout the company to ensure that appropriate governance arrangements are established and acted on; and (4) creation of reporting mechanisms for both internal and external stakeholders about the status of privacy protection within the organization.

Privacy staff also needs to follow suitable methodologies to ensure the implementation of privacy protection measures into all information-related processes that collect or use personal data. (This staff may consist in members of the CPO group or extend to other staff with privacy responsibilities; in a large IT firm, this may include any employee who runs internal systems, develops products or services, or operates these services.) Firms that employ appropriate privacy methodologies usually meet one or more of the following, additional criteria: (5) formal processes for the development of company-wide policies,

---

[175] In contemplating relevant performance measures, it is worth comparing the state of the art in privacy versus security. ISO 27001 and ISO 27002 are widely used security standards, which thousands of companies rely upon in implementing information security management systems and thereby establishing their compliance with corporate accountability laws such as the Sarbanes-Oxley Act of 2002; *see* ALAN CALDER & STEVE WATKINS, IT GOVERNANCE: A MANAGER'S GUIDE TO DATA SECURITY AND ISO 27001/ISO 27002 (2008). Although the British Standards Institute recently introduced BS 10012, the Data Protection: Specification for a Personal Information Management System, this brand new standard is not yet well-established. *See* Outlaw.com, *Code for Handling Personal Data is Muddled, Says Lawyer*, THE REGISTER, June 3, 2009 http://www.theregister.co.uk/2009/06/03/code_adds_confusion/.

[176] For the ideas in the following paragraph, I am indebted to a Discussion Document prepared at the behest of the U.K. Information Commissioner's Office; *see* John Leach and Colin Watson, *The Business Case for Investing in Proactive Privacy Protection* (2009), *available at* http://www.watsonhall.com/resources/downloads/pp-discussion-document-12.pdf. I also relied on the following texts: George O. M. Yee, *Estimating the Privacy Protection Capability of a Web Service Provider*, 6 INTL. J. WEB SERVICES RES. 20 (2009); Colin J. Bennett & Charles Raab, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2006)*;* David Flaherty, *Privacy Impact Assessment: An Essential Tool for Data Protection*, 7/5 Privacy Law & Policy Reporter 85 (2000).

[177] *See* Data Governance Inst., Defining Data Governance, http://www.datagovernance.com/gbg_defining_governance.html.

[178] *See* Bennett and Raab, *supra* note 176 at 267 (noting that CPOs help ensure that data governance issues are debated at the top level of the organization); Swire, *supra* note 143.

standards, and procedures related to privacy protection; (6) periodic assessments of both internal systems and a company's products and services to ensure that they adhere to established privacy standards; (7) a risk-based approach to privacy and security decisions;[179] (8) use of leading edge development process such as privacy by design;[180] (9) use of privacy impact assessments (PIAs) for new products or initiatives;[181] (10) use of methods for addressing privacy issues with third-parties such as suppliers, outsourcing partners and agency workers;[182] and (11) use of a privacy incident handling process.

Finally, most organizations that implement data governance systems and appropriate privacy methodologies also use best practices to achieve desired outcomes. Firms that use best privacy practices usually meet one or more of these additional, and final, criteria: (12) adherence to well-established industry-wide codes of conduct; (13) privacy certifications of products and services by accredited certification bodies;[183] (14) use of specific privacy-protective techniques such as layered notice, data minimization, deletion of data when no longer used or required, data anonymization, and other PETs; (15) mandatory privacy training for all staff with privacy responsibilities; (16) employee and consumer guidance on privacy and security issues; (17) customer complaint procedures; (18) a policy addressing access to personal information in criminal and civil cases, which requires notice and/or exigent circumstances or appropriate legal process before revealing customer information; and (19) sharing of best practices through industry or government collaboration, participation in trade organizations and government forums, and public dissemination.

It is beyond the scope of this discussion to justify these nineteen criteria or comment on whether this is the right number or mix of selection criteria, if they should be weighted and if so how, or if there is a minimum number of criteria that must be satisfied to achieve safe harbor eligibility. Rather, they are provided for illustrative purposes only and to demonstrate that even in the absence of the objective measures on which environmental regulators typically rely, it is possible to identify which firms are most likely to deliver a high level of privacy protection as compared to their peers.[184]

## IV. CONCLUSION AND RECOMMENDATIONS

Despite its shortcoming and many critics, self-regulation is a recurrent theme in the US approach to online privacy and perhaps a permanent aspect of the regulatory landscape. This Article's goal has been to consider new strategies for overcoming observed weaknesses in self-regulatory privacy programs. It began by examining the FTC's intermittent embrace of self-regulation, and found that the Commission's most recent foray into self-regulatory guidelines for online behavioral advertising is not very different from earlier efforts, which ended in frustration and a call for legislation. It also reviewed briefly the more theoretical arguments of privacy scholars for and against self-regulation, but concluded that the market-oriented views of those who favor open information flows clashed with the highly critical views of those who detect a market failure and worry about the damaging consequences of profiling and surveillance not only to individuals, but to society and to democratic self-determination. These views seem irreconcilable and do not pave the way for any practical solutions.

---

[179] *See* Press Release, FTC, Eli Lilly Settles FTC Charges Concerning Security Breach (June 18, 2002) (describing a four-stage, risk-based approach to information security). For a general discussion of security design methods, *see* Michael Howard and Steve Lipner, THE SECURITY DEVELOPMENT LIFECYCLE (2006); GARY MCGRAW, SOFTWARE SECURITY: BUILDING SECURITY IN (2006).

[180] For discussion of privacy by design, *see* Sarah Spiekermann and Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 67, 72 (2009); UK Information Commissioner's Office, PRIVACY BY DESIGN REPORT (2008); Elizabeth Montalbano, *Microsoft Releases Guidelines for Customer Privac*y, COMPUTERWORLD (Oct. 16, 2006).

[181] *See* Bennett & Raab, *supra* note 176 at 204-10.

[182] *See* Press Release, FTC, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data, (March 27, 2008) *available at* http://www.ftc.gov/opa/2008/03/datasec.shtm (requiring both firms to "develop reasonable steps to select and oversee service providers that handle the personal information they receive from the companies").

[183] *See* Kirsten Bock, *EuroPrise Trust Certification: An Approach to Strengthen User Confidence Through Privacy Certification*, 32 Datenschutz und Datensicherheit 610 (2008)(discussing the European privacy seal for IT products and IT-based services).

[184] *See* Yee, *supra* note 176.

Next, this Article presented three case studies of self-regulatory programs that spanned the continuum from voluntary to partially mandated to fully mandated. This included an empirical analysis of the CARU safe harbor program, especially its case reports of compliance issues and their intersection with FTC enforcement actions. Finally, this article turned to an evaluation of the case studies in terms of completeness, free rider problems, oversight and enforcement, and transparency, and concluded that self-regulation undergirded by law—in other words, a *statutory safe harbor*—is a more effective and efficient instrument than any self-regulatory guidelines in which industry alone is responsible for developing principles and/or enforcing them. In a nutshell, well-designed safe harbors enable policy makers to imagine new forms of self-regulation that "build on its strengths … while compensating for its weaknesses."[185] This embrace of statutory safe harbors led to a discussion of how to improve them by importing second-generation strategies from environmental law. Rather than summarizing these strategies and how they translate into the privacy domain, we conclude with a set of specific recommendations based on the discussion in Part III.B.

*If* Congress enacts comprehensive privacy legislation based on FIPPs, we recommend, first, that the new law include a safe harbor program that resembles the COPPA safe harbor, in that it allows groups to submit self-regulatory guidelines to the FTC for approval and treats compliance with these guidelines as deemed compliance with statutory requirements. The FTC should be authorized to draft an implementing rule addressing the safe harbor among other things. Beyond that, the design of the COPPA safe harbor program should be overhauled to reflect second-generation strategies. Specifically, the statute should articulate core substantive requirements in general terms and grant FTC much greater discretion in determining whether proposed guidelines achieve desired outcomes, without having to match detailed regulatory requirements on a point by point basis. Second, the enforcement provision should include new incentives such as tiered liability and lighter regulatory burdens for firms that qualify for safe harbor treatment.

Third, the safe harbor provision should describe not only the approval process but the eligibility requirements for such treatment. There should be at least two ways for firms to qualify, both of which reflect the idea that safe harbor treatment requires that firms go beyond mere legal compliance with notice, choice, access, security and enforcement requirements. One way for a firm to qualify would be to agree to abide by a code of conduct, which is drafted by a group of representative firms together with other stakeholders using the covenanting approach as described above, and which is approved by the FTC; an alternative way is join a safe harbor program that has two components: self-regulatory guidelines that achieve the purpose of the statute as described in its general provisions, and criteria designed to demonstrate superior performance in protecting privacy in keeping with the nineteen criteria enumerated at the end of Section III.B. The FTC would need to approve both components.

Fourth, because performance measures for privacy is an undeveloped area of privacy regulation with scant literature describing these measures or their usefulness in predicting superior performance, the FTC should be directed to prepare a report to Congress within twelve months of enactment of the new legislation. This report should examine relevant technological, market and regulatory developments, including the growing use of PIAs by government agencies, and make recommendations concerning options for measuring privacy performance for purposes of safe harbor eligibility. It should also consider the need (if any) for Congress to modify any safe harbor provisions that presuppose the effectiveness of specific performance measures.

Fifth, the new law should authorize the FTC to issue regulations addressing online behavioral advertising but not until twenty-four months after enactment of the new legislation. During this suspension period, the FTC should encourage industry to develop self-regulatory guidelines that go beyond compliance (either by participating in a multi-stakeholder process using the covenanting approach or refining their own code of conduct while also developing criteria for demonstrating superior performance). If the FTC approves the proposed guidelines, companies that sign up for the resulting safe

[185] *See* Gunningham and Rees, *supra* note 6 at 389.

harbor program would be deemed in compliance with any relevant regulatory requirements and enjoy additional benefits as described above if approved by the FTC.

Before turning to the final point, it is worth noting that all of the preceding safe harbor recommendations presuppose a comprehensive privacy law premised on FIPPs. But nothing in the structure of a re-designed safe harbor ties it exclusively to this foundational understanding of privacy protection. This is important, for in the past few years, a diverse group of privacy scholars, technologists, and business leaders have each begun to explore new approaches to privacy protection that refocus or even supplant FIPPs and instead emphasize tangible harms,[186] the transparency and accountability of data uses,[187] and data use (as opposed to collection) and the obligations it imposes on organizations (as opposed to individuals).[188] Thus, the sixth and final recommendation is that the statute should authorize the FTC to conduct a study of these and other alternative approaches to privacy to determine if they offer as good—or better—privacy protections as systems based on FIPPs and, if so, to recommend that Congress grant the FTC authority to approve self-regulatory guidelines premised on these new approaches.

[186] *See* Fred H. Cate, *The Failure of Fair Information Practice Principles* in CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' (Jane K, Winn, ed., 2006). Cate argues that despite their lofty goals, FIPPS fail in practice by "maximizing consumer choice" rather than "protecting privacy while permitting data flows." *Id.* at 369. He proposes a revised version of FIPPs with new principles emphasizing the prevention of harm, the maximization of individual and public benefits through the balancing of the value of accessible personal information and information privacy, and more consistent privacy protection across types of data, settings, and jurisdictions. In shifting attention from notice and choice to tangible harms, Cate's proposed principles also emphasize substantive rather than procedural protections.

[187] *See* Daniel J. Weitzner et al, *Information Accountability*, 51 COMM. OF THE ACM 82 (2008). Weitzner and his colleagues argue that a privacy regime premised on controlling and preventing access to information no longer works given the ease of sharing data and the large-scale aggregation and searching of data across multiple sources. Their new approach is based on transparency and accountability of data *use* and their work describes a new technical architecture for promoting informational accountability. In a related article, they illustrate this new architecture by showing how it would apply to data mining scenarios such as passenger airline screening systems. *See* Weitzner et al, *Transparent Accountable Data Mining: New Strategies for Privacy Protection*, MIT CSAIL Technical Report (Jan. 27, 2006), *available at* http://www.w3.org/2006/01/tami-privacy-strategies-aaai.pdf (describing how the new architecture prevents certain privacy failures).

[188] *See* The Business Forum for Consumer Privacy, *A New Approach to Protecting Privacy in the Evolving Digital Economy* (2009), *available at* https://www.privacyassociation.org/images/stories/pdfs/a%20new%20approach%20to%20protecting%20privacy%20-%20final.pdf. Influenced by the work of both Cate and Weitzner, the Business Forum begins with a critique of FIPPs based on the observation that FIPPs expect the consumer "to serve as the controller of his or her information and carries much of the responsibility for policing its appropriate use," *id. at 5*, a task for which consumers are ill-suited given the complexity and lack of transparency of information flows in today's networked world. Their alternative approach takes off from a belief that "the use of data, rather than its collection, serves as a better starting point for defining the obligations related to personal information." *Id.* This "use-and-obligations" model deemphasizes notice and choice in favor of a data governance approach that "places obligations for responsible data use squarely on the organization." *Id.* at 6.