PRIVACY AND REGULATORY INNOVATION: MOVING BEYOND VOLUNTARY CODES

Ira S. Rubinstein*

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 co-regulatory approaches in which government plays a role in setting requirements for industry guidelines and imposing sanctions for non-compliance. Based on three case studies of a weakly mandated industry code aimed at online behavioral advertising practices, a more strongly mandated program enabling data flows between Europe and the US, and a safe harbor program designed to protect children's privacy, this Article argues that statutory safe harbors have many strengths but would benefit from being redesigned. Next it conceptualizes new models for privacy co-regulation based on insights derived from "second generation" environmental policy instruments such as environmental covenants. Finally, it offers specific recommendations— to the FTC, on how it might begin to use the covenanting approach to experiment with innovative technologies and address hard problems such as online behavioral advertising, and to Congress on how best to structure new safe harbor programs as an essential component of omnibus consumer privacy legislation. All of these approaches to regulatory innovation move beyond purely voluntary codes in favor of co-regulatory solutions.

TABLE OF CONTENTS

* Adjunct Professor of Law and Senior Fellow, Information Law Institute, New York University School of Law. For their extensive comments on an earlier draft of this paper, I am especially grateful to Dennis Hirsch, Chris Hoofnagle, and Ron Lee. For helpful comments and suggestions, I also wish to thank Malcolm Crompton, Charles Curran, Amy Mudge, Peter Shuck, and Lisa Sotto, and the participants in the Workshop on Federal Privacy Legislation, NYU School of Law, October 2, 2009.

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. They argued 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 substantive rules concerning the collection, use and transfer of personal information and procedures for applying these rules to member firms.[1] But to its many critics, 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, Congress would define substantive privacy requirements for commercial firms based on FIPPs and authorize agency regulation as supplemented over time by court decisions interpreting their requirements. The legislation would also spell 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

[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 241-243 and accompanying text. There are different formulations of FIPPs, which vary as to both the number of principles and their substantive content. The most recent government formulation includes eight principles (transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing); *see* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (Dec. 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. For earlier formulations by the FTC, *see infra* note 25 and accompanying text.

[4] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461, 1524-1528 (2000); Chris Jay Hoofnagle, Privacy Self-Regulation: A Decade of Disappointment 11 (March 4, 2005) *available at* http://epic.org/reports/decadedisappoint.html (arguing that self-regulatory privacy programs seek "to stop Congress from creating real, enforceable rights while allowing privacy-invasive activities to continue").

have a private right of action to recover damages for any injuries they might suffer when a firm violates the law.[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 voluntary self-regulation and direct government 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 idea of a privacy safe harbor, first 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 co-regulatory initiatives or safe harbors. This Article argues that co-regulation, including privacy safe harbors, 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.[9] First, the existing COPPA safe harbor, without any modification, deals successfully with virtually all of the standard criticisms of self-regulation.[10] Second, by allowing greater flexibility in structuring self-regulatory frameworks, Congress can enable the FTC to experiment with policy innovations such as Privacy-Enhancing Technologies (PETs) and new ways of implementing FIPPs and to better address difficult issues such as behavioral advertising.[11] Finally, 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.[12]

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.[13] Leading

---

[5] *See* Swire, *supra* note 1.

[6] 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.

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

[9] Gunningham and Rees, *supra* note 6 at 366 ("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"); *see also* Sinclair, *supra* note 6 at 532.

[10] *See infra* III.A.

[11] *See infra* III.C.1 and C.2.

[12] *See infra* III.C.3.

[13] *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. Rep. Boucher (D-VA) is chairman of the Subcommittee on Communications, Technology and the Internet.

technology firms have voiced support for federal privacy legislation and have joined with privacy groups to draft model legislation.[14] 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.[15] 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.[16] It seems likely that such provisions will re-surface in any new bills offered in the 111th Congress or thereafter.[17] 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 the conventional enforcement model or enacted no law at all.

The Article 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 involving co-regulatory solutions: the first is a "weakly mandated" industry effort aimed at online behavioral advertising practices; the second is a more "strongly mandated" safe harbor program resulting from joint government efforts to ensure data flows between Europe and the US; and the third is a statutorily mandated safe harbor under COPPA, which is designed to facilitate industry self-regulation as a vital component of protecting children's privacy.[18]

Part III begins by assessing these case studies against five criteria—completeness, free rider problems, oversight and enforcement, transparency, and formation of regulatory norms—and concludes that despite several weaknesses, statutory safe harbors such as COPPA offer a superior form of self-regulation. Next, it describes a more collaborative, flexible and performance-based approach to self-regulation, drawing on critical insights from environmental regulation. It discusses one specific set of policy tools known as environmental covenants and applies this learning to the use of privacy covenants and a revamped version of statutory safe

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

[15] This is referred to as "deemed compliance"; s*ee infra*, note 118 and accompanying text. The key European privacy law creates a similar mix by requiring member states to set out substantive standards for the protection of personal data while also encouraging member states to allow co-regulation with industry sectors; *see supra* notes 204-208 and accompanying text.

[16] *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).

[17] Cong. Boucher's proposed bill would also include a safe harbor; *see supra* note13.

[18] For a discussion of mandated self-regulation, *see infra* notes 63-68 and accompanying text.

harbors. The Article concludes by recommending that Congress adopt these new tools to help protect online consumer 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.[19] 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.[20] 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."[21] 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 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 once again appears to be ascendant at least as to online behavioral advertising.[22] 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. A year later, 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.[23] On the other hand, privacy advocates warned that technology was no substitute for FIPPs and that self-regulation would remain ineffective without enforceable privacy rights, which were

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

[20] *Id.* 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).

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

[22] For a discussion of how this may be changing, *see infra* notes 46-48 and accompanying text.

[23] *See* 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 new PETs that might obviate the need for governmental regulation.

necessary to deter bad actors and outliers, and ensure the widest possible participation in any self-regulatory schemes.[24]

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.[25] 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."[26] After reviewing the results of an Internet privacy survey[27] and studying industry guidelines,[28] however, the FTC also began to express some doubts. 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.[29]

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.[30] In its second report to Congress in 1999, the FTC focused on self-regulation. It commended recent industry developments such as the guidelines

---

[24] *Id.*

[25] 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 FIPPs to four; *see infra* note 35.

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

[27] The survey 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)"; *see* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS, *supra* note 25 at 4.

[28] The FTC asked trade associations and industry groups to submit copies of their self-regulatory guidelines for review, and 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"; *see 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).

[29] Four months after the Commission's 1998 report, Congress enacted COPPA and the President signed it into law; *see infra* note 112 and accompanying text.

[30] *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.

adopted by the Online Privacy Alliance (OPA)[31] and the creation by Truste, BBBOnline, and others of privacy seal programs.[32] The Commission also reviewed the results of two more privacy surveys, the Commission found improvements in the frequency of privacy disclosures but continued weakness in sites' implementing all four FIPPs.[33] 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.[34]

In 2000, in its third report to Congress, the Commission finally 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 law) to comply with all four FIPPs and give rulemaking authority to an implementing agency.[35] 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."[36] 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.[37]

This trend changed in 2001, with the appointment of Tim Muris as FTC Chairman. Muris ushered in a revised privacy agenda for the Commission by temporarily shelving the debate over self-regulation and instead focusing on how best to protect consumers against "real" harms such as online stalking, identity theft, telemarketing and spam.[38] He proposed a number of measures including a "do not call" list for consumers wishing to avoid telemarketing calls (which proved wildly successful); devoting more resources to prosecuting fraudulent activities (such as spam and financial scams); and assisting 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

---

[31] *See* FTC, SELF-REGULATION AND PRIVACY ONLINE, *supra* note 26 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).

[32] *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).

[33] *See* FTC, SELF-REGULATION AND PRIVACY ONLINE, *supra* note 26 at 7.

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

[35] *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.

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

[37] *See infra* note 77 and accompanying text.

[38] *See* 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.

in their online privacy statements. Finally, he suggested that the Commission gather more information about Internet security practices and other emerging issues and new privacy technologies such as the Platform for Privacy Preferences (P3P).[39]

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 as well as a lack of consensus over online security and access principles.[40] And he called attention to the lack of data regarding the cost/benefit tradeoff of online privacy legislation.[41] Over the next eight years, Muris and his successors organized the FTC's privacy agenda around combating harmful uses of personal information with an emphasis on 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 the need for comprehensive privacy legislation. The FTC continued to believe in self-regulation as part of its broader agenda, which included protecting consumers from fraudulent advertising. But it confined its work in the privacy arena to problems causing specific harms (spam, spyware, phishing, ID theft, and data breaches) and to laws that enhanced FTC's enforcement powers (such as the CAN-SPAM Act and the US SAFE Web Act).

In 2006, this harms-based agenda showed signs of change when, for first time in many years, an FTC report listed "encouraging self-regulatory initiatives to benefit consumers" as a goal and specifically called for self-regulatory approaches to online behavioral advertising.[42] A year later, the Commission hosted a Town Hall meeting concerning online behavioral advertising followed by Staff recommending four principles to assist industry in the further development of self-regulatory guidelines.[43] The next eighteen months saw even more activity devoted to industry self-regulation.[44] Yet, as soon as the new FTC Chairman, Jon Leibowitz, took office, he began to express doubts about the efficacy of the self-regulatory approach. Noting that the current behavioral advertising guidelines did not seem to be working, he alluded to the recently issued Staff guidelines and expressed hope that industry would respond with concrete improvements. "Self-regulation, if it works, can be the fastest and best way to change the status

---

[39] For a discussion of P3P, *see infra* notes 235-240 and accompanying texts.

[40] *See* Muris, Remarks at the Privacy 2001 Conference, *supra* note 38 (observing that "Acres of trees died to produce a blizzard of barely comprehensible privacy notices").

[41] *See also* Beales and Muris, *infra* note 54.

[42] FTC, PROTECTING CONSUMERS IN THE NEXT TECH-ADE (2008), 4, 9, 11 *available at* http://www.ftc.gov/os/2008/03/P064101tech.pdf (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.

[43] *See* FTC STAFF STATEMENT, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 3-6 (Dec. 2007) *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[44] For example, in March 2009, the FTC released a lengthy report on self-regulation in the online advertising industry, which included a summary and analysis of the comments the FTC received on the staff's earlier proposal as well as revisions to the four principles *See* FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter STAFF REPORT ON SELF-REGULATORY PRINCIPLES]. This report explained that "staff supported self-regulation because it provides the necessary flexibility to address evolving online business models." *Id.* at 14.

quo," he stated, at the same time warning his audience that "if there isn't an appropriately vigorous response, my sense is that Congress and the Commission may move toward a more regulatory model."[45]

As Yogi Berra famously said, "This is déjà vu all over again." As shown above, several earlier FTC Chairs arrived at exactly this point only to reluctantly conclude that self-regulation would not work. It seems highly unlikely that Leibowitz (who served previously as an FTC Commissioner) is unaware of past dissatisfaction with privacy self-regulation. 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.[46] So why did Leibowitz give voice to a position that Clinton officials might have expressed fifteen years ago and how did he reach this point only one month after FTC Staff recommended a self-regulatory approach? One possible answer is politics. Privacy legislation has never enjoyed reliable political support especially given the relatively strong opposition from parts of industry and the jurisdictional complications that inevitably arise when multiple Committees lay claim to privacy initiatives.[47] 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 online advertising.[48] 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 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, 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;[49] and, second, the extent to which a consent requirement regarding the collection, use or

---

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

[46] *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 [hereinafter Vladeck Interview], *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (questioning both the notice-and-consent framework and the harms-based framework).

[47] *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.

[48] *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).

[49] *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

transfer of personal information "burdens consumers and creates costs."[50] 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.[51]

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."[52] 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."[53] It follows that firms have sufficient incentives to avoid policies inconsistent with their customers' privacy preferences. In fact, many firms already have taken positive steps to protect their reputations by participating in voluntary, third-party privacy seal programs (as discussed above) and developing various PETs such as cookie management tools and P3P. Rubin and Lenard also noted the lack of evidence that 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."[54]

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).

[50] *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).

[51] *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.

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

[53] *Id.* at 51. For a recent example of this phenomenon, *see* David Coursey, *Google Apologizes for Buzz Privacy Issues*, PC WORLD, Feb. 15, 2010 *available at* http://www.pcworld.com/businesscenter/article/189329/google_apologizes_for_buzz_privacy_issues.html (discussing how Google responded to privacy concerns raised by its new Buzz social network service within a week of its launch).

[54] RUBIN & LENARD, *supra* note 52 at 64. For contemporaneous studies by other 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").

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."[55] 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.[56] 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.[57] 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 protection. 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."[58]

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.[59] 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.[60] 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.[61] 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.[62]

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 subsidy to information processing firms, whether by enacting an opt-in

---

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

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

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

[58] *Id*, at 847; *see* Schwartz, *supra* note 32 at 1686.

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

[60] Kang, *supra* note 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).

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

[62] *See* Schwartz, *supra* note 57 at 854-857; *but see* Fred Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 891-95 (2000)(taking issue with Schwartz's justification of opt-in privacy laws).

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 clear from the above discussion that there is an important role for regulation to play in the protection of personal data. However, it is equally clear that the costs of such regulation are at present unknown, could be very significant, and could have a deleterious effect on the success of existing business models and/or the future growth of the information technology sector. This suggests the importance of finding regulatory mechanisms that both do a good job of protecting personal data, and do so in a cost-effective and flexible way. The next section explores whether any of the forms of self-regulation could, potentially, play this role.

II. CASE STUDIES

Thus far, the discussion of self-regulation has been mainly historical or abstract. This Part begins the task identified above by presenting three case studies of self-regulatory privacy 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.[63] Regulatory scholar Joseph Rees[64] provides a simple version of this continuum as follows:

The two end points are familiar: at one extreme, direct government regulation, in which a centralized government agency handles both regulatory rulemaking and enforcement (such as the FTC's role in protecting consumer credit under the Fair Credit Reporting Act (FACA)); at the other, voluntary self-regulation, in which private firms carry out these tasks independent of direct government involvement (such as the several privacy seal programs based on the OPA Guidelines). Mandated self-regulation, which Rees describes as a hybrid of these two regulatory forms, is the more interesting case:

> At base, it is a *governmental* strategy for strengthening *private* regulatory systems….[Its] purpose is to build into the social structure of the regulated entity a sustained and effective commitment to insecure or precarious values—such as environmental protection, affirmative action, or occupational safety.[65]

---

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

[64] JOSEPH V. REES, REFORMING THE WORKPLACE: A STUDY OF SELF-REGULATION IN OCCUPATIONAL SAFETY 9 (1988). Rees' explores a regulatory experiment carried out in the early 1980s by the Occupational Safety and Health Administration (OSHA) called the Cooperative Compliance Program (CCP). This involved a three-way arrangement among unions, management, and OSHA in which the agency authorized labor-management safety committees to assume many of OSHA's regulatory responsibilities at several large construction sites, while ceasing routine compliance inspections and pursuing a more cooperative relationship with the participating firms.

[65] *Id*. at 10.

Rees distinguished two types of mandated self-regulation, which he refers to as "full" and "partial." Full mandated self-regulation privatizes both of the major regulatory functions of rulemaking and enforcement. The strategy resembles voluntary self-regulation in this respect, but differs from it chiefly in that a government agency officially sanctions and monitors the self-regulatory program to ensure its effectiveness. In contrast, mandated partial self-regulation limits privatization to one or the other regulatory function, but not both. Two basic approaches are the result: "public enforcement of privately written rules, and governmentally monitored internal enforcement of publicly written rules."[66]

For present purposes, Rees division of mandated self-regulation into full and partial forms is less important than the extent of the government's role in approving and monitoring one (or both) of the regulatory functions of rulemaking and enforcement. The government may impose this mandate *weakly* or *strongly*. In the former, a government agency might informally review and approve industry guidelines and engage in enforcement activity only if a specific violation is brought to its attention. In the latter, the agency, pursuant to statute or acting under it rulemaking authority, prescribes the minimum requirements for industry guidelines and evaluates the guidelines using a formal notice and comment procedure; in addition, the agency defines compliance requirements and supplements industry enforcement efforts on an ongoing basis.[67] This new emphasis makes Rees typology more flexible and allows it to accommodate a greater variety of hybrid schemes. Accordingly, the regulatory continuum utilized in this Article looks like this:

All three of the case studies examined below exemplify mandated self-regulation and hence fall within the middle of the continuum. The first case study focuses on the Network Advertising Initiative (NAI) Principles, which take the form of a weakly mandated self-regulatory scheme in which an ad hoc industry advertising group defines a set of governing principles (which the FTC informally approved) and also oversees members' compliance (by

[66] *Id.* at 11. Rees offers no examples of this first prong of partial self-regulation in which a government agency would enforce a purely private rule, i.e., one that no branch of government has formally adopted or approved. Arguably, this first prong should have an additional condition: "public enforcement of privately written *and publicly ratified* rules." There are indeed numerous examples of this approach such as municipal building codes, which are drafted by the International Code Council and adopted by local municipalities; professional codes of practice, such as the American Bar Association (ABA) Model Rules of Professional Conduct, which are created by the ABA and then adopted in whole or in part by state legislatures; and financial industry regulations, which are developed by the Financial Industry Regulatory Authority (the largest independent regulator for all security firms doing business in the US) and approved by the Security and Exchange Commission under a notice and comment procedure.

[67] *See* IAN AYRES & JOHN BRAITHWAITE, RESPONSVIE REGULATION: TRANSCENDING THE DEREGULATION DEBATE, 101-138 (1992) (describing a variation on mandated self-regulation, which they refer to as "enforced self-regulation," a model under which "the government would compel each company to write a set of rules tailored to the unique set of contingencies facing that firm"). What's unique about their model is that negotiations occur between a government agency and an *individual firm* and result in regulations that are *specific* to each firm.

assigning this task to an independent third-party).[68] 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 had to certify that they would comply with privacy principles negotiated between the US and EU but administered by industry seal programs created for this purpose by DMA, Truste, BBBOnline, and others. Thus, industry manages the enforcement of publicly-written rules but subject to weak government oversight. 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 strongly mandated self-regulation, where industry is responsible for both rule making and enforcement, but under close government supervision.

A. The Network Advertising Initiative

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.[69] 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).[70] 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."[71] 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.[72]

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

[68] The most prevalent form of privacy self-regulation in the US is purely voluntary self-regulation, including familiar examples such as the Privacy Promise of the Direct Marketing Association (DMA), the Individual Reference Service Group (IRSG) Principles (which apply to data brokers), and the privacy seal programs of Truste and BBBOnline (which originally were based on the OPA Guidelines). Arguably, the NAI Principles fit in this category too but for the fact that under threat of various law suits and investigations, NAI engaged in informal negotiations with FTC, and the agency concluded that the NAI Principles were consistent with FIPPs; *see infra* notes 76-77 and accompanying text. Thus, the NAI Principles represent a transitional form of self-regulation at the point on the continuum at which voluntary self-regulation shades over into weakly mandated self-regulation.

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

[70] *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." The FTC now rejects this distinction, at least in the context of online behavioral advertising; *see* STAFF REPORT ON SELF-REGULATORY PRINCIPLES, *supra* note 44 at 21-22 (stating that "the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data").

[71] *Id*. at 5.

[72] *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).

ads increase ad revenues, which subsidize free online content and services.[73] 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.[74] Despite these concerns, the Commission "encouraged the network advertising industry … to craft an industry-wide" self-regulatory program.[75]

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.[76] 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."[77] This nominal approval by FTC arguably converts the NAI principles from a purely voluntary regime into a (very) weakly mandated self-regulatory scheme.

Under the original 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.[78] The

---

[73] *See* FTC, ONLINE PROFILING: A REPORT TO CONGRESS, *supra* note 69 at 10. For a more recent analysis of the economic impact of online advertising, *see* David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSPECTIVES 37 (2009)(noting that online advertising benefits consumers by increasing the likelihood of their receiving relevant ads and reducing the costs of advertising to businesses, which may result in lower consumer prices, but also creates a privacy dilemma).

[74] *Id.* at 10-14.

[75] *Id.* at 1.

[76] *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.

[77] 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 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).

[78] OPM was NAI's original term for online profiling. *See* NAI, 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

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.[79] 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.[80] 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.[81]

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;[82] or independent audits of a member's practices that would be made publicly available on the NAI's Web site.[83] 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;[84] a set of rather limited pledges regarding security and access;[85] 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[86] and raised significant substantive concerns as well.[87]

---

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").

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

[80] *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.

[81] *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 obvious how robust notice differs from ordinary notice, which also must be "clear and conspicuous."

[82] *Id.* at 3.

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

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

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

[86] *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 very late in the process).

[87] *Id.* (arguing 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" 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).

For the next seven years, the NAI principles remained unchanged 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!.[88] 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.[89] 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.[90] 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.[91] 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 started 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.[92]

In 2007, the FTC held a two-day workshop to revisit the issue surrounding online profiling/OPM, or what it now referred to as Online Behavioral Advertising (OBA). In connection with this workshop, the World Privacy Forum (WPF) prepared a highly critical report attacking the effectiveness of the NAI's self-regulatory scheme during the previous seven years.[93] NAI responded to these and other criticisms by releasing a draft update to its original NAI Principles (this time soliciting public comments on the proposed changes).[94] The newly

---

[88] 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 while using a search engine or the related services.

[89] *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 requiring Google to 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).

[90] *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").

[91] *Id.*

[92] *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.

[93] *See* PAM DIXON, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND SELF-REGULATION 14-27, 28-30 and 32-38 (2007), *available at* http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (arguing that the NAI opt-out mechanism was 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; that there was a severe and rapid drop-off in NAI membership from twelve members in 2000 to just two members in 2003 (although this may have been due in part to the dot.com collapse); questioning NAI's decision to sign up so-called "Associate Members" even thought they were not required to fully comply with the NAI Principles; raising doubts about NAI's compliance program (which had been outsourced to Truste) for having a weak consumer complaint mechanism and for neglecting random audits.

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

expanded organization then published its revised code of conduct but to mixed reviews.[95] 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").[96] But the Commission also 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.[97] Similarly, the Center for Democracy and Technology (CDT)[98] 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;[99] 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.[100]

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.[101] 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.[102]

---

[95] *See* NAI, NAI'S SELF-REGULATORY CODE OF CONDUCT (Dec. 2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf (in the wake of renewed public scrutiny,t he NAI grew to twenty-five members.

[96] STAFF REPORT ON SELF-REGULATORY PRINCIPLES, *supra* note 44 at 14.

[97] *Id.*

[98] *See* CDT, Response to the 2008 NAI Principles (Dec. 16, 2008), *available at* http://cdt.org/press/20081216press.php.

[99] 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.

[100] In recent Congressional testimony, NAI supported new methods for enhancing consumer notice mechanisms and improving the durability of cookie-based opt-outs; *see Behavioral Advertising: Industry Practices and Consumers' Expectations, Hearings before the House Comm. on Energy and Commerce, Subcomms. on Commerce, Trade and Consumer Protection and Communications, Technology and the Internet*, 111 Cong., 1st Sess., June 18, 2009 (Statement of Charles Curran, Exec. Dir., NAI).

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

[102] 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,

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. They must self-certify to DOC that they adhere to the Privacy Principles (which mirror the core requirements of the EU Directive) and repeat this assertion in their posted privacy policy.[103] 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 disputes;[104] (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;[105] 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.[106] 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 described as an "uneasy compromise" between the comprehensive regulatory approach of the EU and the self-regulatory approach preferred by the US.[107] 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,[108] commentators have called attention to several major 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."[109] Indeed, it was not until the

---

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.

[103] 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.

[104] *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).

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

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

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

[108] *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.

[109] 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

summer of 2009 that the FTC announced its *first* enforcement action against a US company for violation of the SHA.[110] A 2008 report by an independent consulting firm called Galexia reached very similar conclusions.[111] 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. In sum, while in theory the SHA is a strongly mandated self-regulatory program (because the government sets the requirements both for rulemaking and enforcement), in practice the government monitoring of both functions is so weak as to render the SHA more like a purely voluntary program.

C. The COPPA Safe Harbor

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. The statute[112] and Final Rule[113] 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" before 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."[114]

COPPA provides both federal and state enforcement mechanisms and penalties against operators who violate the provisions of the implementing regulations.[115] The statute by its terms

---

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.

[110] *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 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).

[111] 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 107.

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

[113] 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].

[114] *See* COPPA, 15 U.S.C. § 6502, 16 C.F.R. § 312.3(a)-(e). COPPA combines the enforcement model of regulation with a self-regulatory option in the form of an optional safe harbor program.

[115] *See* 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

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.[116] 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.[117]

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.[118] 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.[119] 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."[120] 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 and after the proposed guidelines have been subject to notice and comment.[121] 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.[122] All of the approved safe harbor programs must satisfy the three criteria set out in the preceding paragraph. Accordingly, COPPA safe harbors exemplify the strongly mandated self-regulation category because they assign industry groups the responsibility both for rule making and compliance.

---

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.

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

[117] 16 C.F.R. § 312.10(b)(2).

[118] COPPA, 15 U.S.C. § 6503(a)(2).

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

[120] *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*.

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

[122] 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.

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.[123] 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."[124] A brief assessment of CARU's monitoring and complaint-handling system further confirms the success of the safe harbor program from an enforcement standpoint.

CARU is a self-regulatory program dedicated to promoting responsible children's advertising. Established in 1974 by the National Advertising Division (NAD) of the Council of Better Business Bureaus (CBBB), it is administered by the CBBB and funded by members of the children's advertising industry. The primary role of CARU is to monitor and review child-directed advertising in all media as well as online privacy practices as they affect children. In January 2001, the FTC approved CARU as a COPPA safe harbor program. Because the NAD maintains a publicly available archive of case reports of all formally opened cases involving a web site's failure to comply voluntarily with the CARU guidelines, it is possible to evaluate CARU's track record on compliance.[125]

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 any web site that may be reasonably expected to attract children or teen users.[126] 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;[127] in a second case, the respondent entered into a consent decree with the FTC that included signing up for the CARU safe harbor;[128] and in a third case, the FTC initiated a COPPA law suit based in part on CARU's determination of compliance shortcomings.[129] This is an impressive record considering that since 2000, the FTC has brought a total of only fifteen COPPA enforcement cases. In short, CARU's compliance review and disciplinary procedures clearly have been successful in complementing FTC's enforcement of COPPA, due in no small measure to their policy of engaging in wide-spread

[123] *See* EPIC, CRITICISMS OF COPPA, http://epic.org/privacy/kids/default.html (observing that parental verification mechanisms are costly and inconvenient for parents yet ineffective since Internet savvy children learn how to evade them by claiming that they are over 13 and that none of the available consent mechanisms establish that the adult granting consent is indeed the parent of the child in question).

[124] FTC COPPA REPORT, *supra* note 120 at 24.

[125] For CARU's purpose and organization, *see* About the Children's Advertising Review Unit (CARU), http://www.caru.org/about/index.aspx. The case reports are available upon request; *see* National Advertising Division, Case Reports and Procedures, http://www.nadreview.org/search/search.aspx?doctype=1&casetype=2.

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

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

[128] *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).

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

monitoring of child-oriented web sites as opposed to member's sites only.[130] This, in turn, allows the Commission to focus its resources on higher profile matters.[131]

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 ten) while Privo has twenty-two and ESRB and Truste have about thirty each.[132] 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 sites). The most likely explanation for this low rate of participation is that deemed compliance is not a strong enough incentive to persuade firms to bear the costs of joining a safe harbor program and abiding by its guidelines when they have to comply with all but identical statutory requirements in any case. (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,[133] 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.[134] This is at least partly the result of the safe harbor approval process, which requires a side-by-side comparison of the substantive provisions of the COPPA rule with the corresponding provisions of the guidelines. The reason firms participate in safe harbor programs is probably due less to regulatory flexibility than 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 weakly and strongly 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

[130] The monitoring and complaint-handling records of the other three safe harbor programs are more difficult to assess given the dearth of public documentation.

[131] *See* FTC COPPA REPORT, *supra* note 120 at 23-24.

[132] 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).

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

[134] Although ESRB is a trade association for the gaming industry and draws all of its members from this sector, this does not seems to reflect 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.

models of privacy covenants based on insights derived from advances in environmental regulation.

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 harbor such as CARU overcomes all of these objections largely due to the fact that it consists in a self-regulatory mechanism reinforced by state intervention (making it strongly mandated). The criticisms of self-regulatory privacy programs boil down to five 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; fourth, that programs suffer from a lack of transparency, both during their formation and in their ongoing operations; and, finally that self-regulatory programs are motivated by a desire to avoid stricter regulation and hence are unreliable.

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 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.[135] 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, as noted above, the COPPA Rule requires that applicants submit a comparison of substantive requirements of the rule with 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 the degree of completeness is directly related to the strength of the government's mandate over the applicable self-regulatory scheme. Clearly, the CARU guidelines are strongly mandated given that they must implement "substantially similar requirements" that provide the same or greater protections for children as those contained in the COPPA Rule.

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

[135] 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 107 at 7.

sanctions" while the second may require that "government intervenes directly to curb the activities of non-participants."[136]

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 both to 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, although current policy may change depending on whether or not Congress enacts new privacy legislation. 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—even if one excludes firms that rely on alternative methods for demonstrating adequacy—the roughly 2,000 participants on the DOC's Safe Harbor List represent only a tiny fraction of firms that transfer data from the EU to US. 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.

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 oversight and enforcement criteria. 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.[137]

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 would 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).

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

[137] DEP'T OF COMMERCE, ELEMENTS OF EFFECTIVE SELF-REGULATION, *supra* note 28.

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 previous nine years of operation, although this is changing for the better.[138] 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 could result in an FTC investigation, and this may provide sufficient incentives for firms to fulfill this requirement, especially if FTC persists in bringing enforcement actions. 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. (The enforcement records of other safe harbor programs are more difficult to assess.) 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."[139]

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.[140] 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.

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."[141] 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 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 fifty page summary of these comments along with its own responses, which in many cases consisted in changing the draft

[138] *See* NAI, 2009 ANNUNAL COMPLIANCE REPORT (2009), *available at* www.networkadvertising.org/.../2009_NAI_Compliance_Report_12-30-09.pdf (summarizing the annual review by NAI Staff of member companies' compliance with the requirements of the new NAI Principles).

[139] *See* Sinclair, *supra* note 6 at 537; AYRES & BRAITHWAITE, *supra* note 67 at 129 ("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").

[140] 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.

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

principles.[142] 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.[143] Although the NAI's approach in 2009 resembled the FTC's notice and comment procedure and was highly transparent, there is 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.[144]

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 conducted its first annual compliance reviews of member companies and posted a summary of the results on the web site.[145] 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.

Regulatory Norms. – When critics of privacy self-regulation question whether all that motivates these codes is a desire to delay Congressional action on a new privacy law, they ignore the fact that even in weak self-regulatory programs, firms must cooperate with each other, an activity that 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; for brevity's sake, they may be reduced to two key points.[146]

The first is that industrial morality is a form of "moral discourse capable of challenging conventional industry practices." 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."[147] Thus, the very act of

---

[142] *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).

[143] 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*.

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

[145] *See supra* note 138.

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

[147] *Id.* at 377 (describing a process of collective soul-searching "where industry officials question their customary ways of doing business, including their taken-for-granted economic assumptions, weigh the alternatives, and think through the consequences of their choices").

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." Legal norms contribute to this expectation since agreement to industry principles creates legally enforceable obligations. 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."[148] In effect, creating industry principles requires that someone in a firm support them enough to lobby for their approval by executives, which then empowers this internal champion to use moral suasion with firm management to ensure that the company satisfies its industry-wide commitments.[149]

This moral discourse leads directly to a second point: 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.[150] This trend coincides with the growing professionalization of the role.[151] While employment of a CPO is no guarantee of improved levels of privacy protection, it does seem to help.[152]

B. "Second Generation" Strategies For Privacy Regulation

Having established the superiority of statutory safe harbors over self-regulatory programs lacking any statutory basis, we now turn to ideas for alternative regulatory strategies, including privacy covenants and revamped statutory safe harbors. 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 of environmental regulation (in which regulators both *command* the level of required performance and *control* the means of achieving it) with "second generation" regulations that encourage "the regulated parties themselves to choose the means by which they will achieve environmental performance goals" resulting in "more cost-effective and adaptable" strategies.[153] The defining

---

[148] *Id.* at 379.

[149] *Id.* at 369.

[150] *See* Christopher Brown, *Privacy Officers: Survey Finds Increasing Number of Firms Appointing Officers with Institutional Clout*, 1 PRIV. & SEC. L. REP. 78 (2002).

[151] 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.

[152] *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").

[153] *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 comprehensive analysis of second generation environmental strategies, *see generally* Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 CAP. U. L. REV. 21, 38-151 (2001); DANIEL J. FIORINO, THE NEW ENVIRONMENTAL REGULATION (2006).

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.[154]

Hirsch contends 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 stringent 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 better fits the normal business planning and investment cycle. Government and society benefit from this approach by achieving better results (such as steeper pollution reductions) than might otherwise be politically achievable. Before turning to *privacy covenants*, it is worth taking a closer look at the Environmental Protection Agency's (EPA) use of *environmental covenants*, specifically Project XL and negotiated rulemaking, and briefly considering how (and why) they work.

1. Environmental Covenants

In general, environmental covenants are contractual agreements between regulators and regulated firms that are negotiated against a background of existing law or regulation. Their goal is to modify these default requirements to achieve greater flexibility and responsiveness to specific conditions and more rapid improvements than would otherwise occur under the existing regulatory regime.[155]

Project XL. - Project XL (standing for "eXcellence and Leadership") is a program developed under President Clinton's reinvention efforts for environmental regulation that encouraged businesses (and government entities) to experiment with new and innovative approaches to pollution controls. Specifically, the program authorized the EPA to negotiate site-specific covenants with regulated firms under which the agency would modify or relax existing regulatory requirements in exchange for enforceable commitments to achieve improved environmental results.[156] In an earlier article analyzing Project XL, Hirsch offers two representative examples of "experimental" XL projects: in one, Weyerhaeuser proposed using

[154] On the other hand, 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 when there are reliable monitoring technologies available to measure actual pollution releases and less well when such technologies are not that well developed; *see* Hirsch, *id.* at 37-40; *see* Fiorino, *id.* at 139.

[155] *See* Stewart, *supra* note 153 at 60-94 (discussing examples of environmental agreements at both the industry and firm level).

[156] *See generally* Regulatory Reinvention (XL) Pilot Projects: Solicitation of proposals and request for comment, *60 Fed. Reg. 27,282* (May 23, 1995)[hereinafter, Notice of Solicitation]. Although EPA envisioned three XL programs for individual facilities, for industry sectors, and government agencies, the following discussion looks primarily at the former.

pollution prevention measures to control hazardous air pollutants and to implement an Environmental Management System (EMS) but wanted EPA to agree to less frequent emission and discharge reports and to allow use of pollution prevention technology in lieu of end-of-pipe controls; in the other, Georgia Pacific proposed developing new gasification technology that would eliminate hazardous air pollutants generated by paper pulping processes, but sought an adjustment in applicable deadlines for achieving hazardous air pollutant reductions.[157]

Project XL works as follows: Interested firms submit initial project proposals to EPA that satisfy very general criteria such as superior performance, cost savings, stakeholder support, innovation, transferability (to other facilities and possibly for future use in rules of national scope), and feasibility. Once the EPA approves a proposal, the applicant works with federal and state regulators on a Final Project Agreement (FPA) defining the specific steps the company will take to improve performance, the regulatory relief that will be granted, how performance will be measured, and the expected environmental results. EPA allows stakeholders an opportunity to comment on a draft FPA before finalizing the agreement.[158] For participating businesses, Project XL offers major benefits, including regulatory flexibility, reduced compliance costs and greater regulatory certainty during the life of the agreement.[159] Although EPA hoped to begin fifty pilot projects within the two years of announcing Project XL,[160] it did not achieve this ambitious goal until a few years later. As of November 2000, forty-eight projects had signed FPAs and EPA had identified seventy "innovations" within these projects.[161]

Despite having met agency goals, Project XL enjoys a mixed reputation. Academic critics (who seem to outnumber supporters) point to three serious flaws in its design and implementation.[162] First, they question EPA's decision to refrain from establishing a "baseline" for determining superior performance, which has in turn led to overreaching by firms in requesting regulatory exemptions unrelated to the purported "improvements" as described in their XL project proposals.[163] Second, while the EPA identified "the support of parties that have a stake" in a project's environmental impacts as an "important factor" in approving a project, and defined stakeholders very broadly to include "communities near the project, local or state governments, businesses, environmental and other public interest groups," at the outset it offered very little guidance as to what meaningful stakeholder participation required. Was it a variety of

---

[157] *See* Dennis D. Hirsch, *Project XL and the Special Case: The EPA's Untold Success Story*, 26 COLUM. J. ENVTL. L. 219, 225–29 (2001) [hereinafter, Hirsch, *Success Story*]. Hirsch distinguishes these experimental XL projects from what he refers to as "special cases," which occur when there is a "bad fit" between applicable regulations and the circumstances at hand and a tailored rule would be fairer and better serves the regulatory purpose.

[158] *See* Notice of Solicitation, *supra* note 156, *60 Fed. Reg. at 27,282*.

[159] *See* Rena I. Steinzor, *Regulatory Reinvention and Project XL: Does the Emperor Have any Clothes?*, 26 ENVTL. L. REP. 10,527, 10,529-30 (Oct., 1996).

[160] *See* Notice of Solicitation, *supra* note 156, *60 Fed. Reg. at 27,287*.

[161] *See* U.S. EPA, Project XL 2000 Comprehensive Report, Executive Summary 2, *available at* http://www.epa.gov/projectxl/vol2toc.htm. For a current listing of projects, *see* U.S. EPA, Project XL Website, XL Projects, *available at* http://www.epa.gov/projectxl/projects.htm (last visited Feb. 2, 2010).

[162] *See* Hirsch, *Success Story*, *supra* note 157 at 221 (noting that "while some commentators have praised the program, most have criticized it on policy and legal grounds")(citations omitted).

[163] *See* Steinzor, *supra* note 159 at 10,529-30 (Oct., 1996); *see also* Hirsch, *Success Story*, *supra* note 157 at 249-251; Fiorino, *supra* note 153 at 141. EPA sought to address this problem by modifyin its original guidance on Project XL, *see* Regulatory Reinvention (XL) Pilot Projects: Notice of Modifications to Project XL, *60 Fed. Reg. 19, 872, 19,876* (April 23, 1997)[hereinafter, Notice of Modifications](requiring that sponsors articulate the link between the flexibility sought and the superior environmental performance; EPA also established a two-tier process for assessing such performance using both quantitative and qualitative benchmarks).

interested parties reaching a broad consensus that a proposed FPA protected the public interest or merely industry and government officials consulting with the local community? Moreover, national environmental groups complained that while they lacked the financial resources to participate in FPA negotiations, local community groups (whose participation EPA favored) lacked the necessary expertise to understand the highly technical issues discussed in many XL proposals.[164]

Finally, severe doubts arose as to whether EPA had enough legal authority to approve FPAs that embodied different legal requirements from those imposed by otherwise applicable statutes and regulations.[165] Hirsch identifies four mechanisms on which EPA relied to authorize these deviations from existing legal requirements, each of which has its weaknesses.[166] The first is enforcement discretion—EPA abstains from enforcing certain regulations against firms that honor the terms of their FPA. As many commentators have noted, this approach fails to shield firms from enforcement actions by other government agencies or from citizen suits under applicable environmental statutes.[167] The second is flexible interpretation—EPA interprets inconsistent rules so that they do not apply to XL participants, thereby protecting them from the threat of litigation. According to Hirsch, the main drawback of this mechanism is its limited scope.[168] The third is express waiver authority as provided by applicable environmental statutes, but as Hirsch points out, this "shares the strengths and weaknesses of flexible interpretation."[169] In view of these weaknesses, the EPA tends to rely mainly on the fourth mechanism, site-specific rulemaking.[170] This approach has obvious benefits but they come at a high cost, namely, the time and uncertainty implicit in any formal rulemaking process.

Project XL's shortcoming as applied to experimental projects might be remedied by legislation defining the environmental improvements required in every XL project, clarifying the process for stakeholder involvement, and granting EPA explicit authority to approve agreements that violate applicable regulatory or statutory requirements. However, as Hirsch points out, the prospects for such legislation seem very doubtful.[171] Yet Hirsch opposes abandoning the experimental dimension of Project XL, which he contends is needed "to allow EPA to test out new, and potentially, better regulatory approaches and environmental technologies."[172] With this goal in mind, he proposes three changes in the design of Project XL: First, rather than just encouraging industry proposals, EPA should take the lead in identifying the innovative approaches worth testing. Although EPA might encourage a diverse group of industry experts, environmentalists, academics and federal and state officials to propose ideas for improving

---

[164] *See* Steiznor, *supra* note 159 at 10,532-34; Hirsch, *Success Story*, *supra* note 157 at 251-53; Fiorino, *supra* note 153 at 141-2. EPA also sought to address this problem by clarifying what it meant by stakeholder involvement and providing up to $25,000 per project to assure that necessary technical assistance was available to support meaningful participation; *see* Notice of Modification, *id.*, *60 Fed. Reg. at 19,877-81*.

[165] *See* Steiznor, *supra* note 159 at 10,535-36; Hirsch, *Success Story*, *supra* note 157 at 244-46; Fiorino, *supra* note 153 at 142.

[166] Hirsch, *Success Story*, *supra* note 157 at 244-46.

[167] *See* Steiznor, *supra* note 163 at 10,536.

[168] *See, e.g.*, Hirsch, *Success Story*, *supra* note 157 at 245 ("Many rules are sufficiently precise that EPA cannot easily reinterpret them to make them inapplicable to the XL project").

[169] *Id.* (noting that implied waivers of authority are nevertheless well-suited to special case XL projects).

[170] *Id* ("a new regulation that expressly authorizes the XL project as an alternative means of complying with the statute").

[171] *Id.* at 254 ("Three such bills have been introduced in recent years and none have been reported out of Committee")(citations omitted).

[172] *Id.* at 255.

environmental regulation, the agency would retain take the lead on which innovations should be tested. Second, EPA should pursue projects consistent with its list of proposed innovations and enter into a small number of agreements for carrying out discrete regulatory experiments at a limited number of facilities, with no intention of expanding these innovations on a national basis. Finally, these "Experimental XL" projects should be rigorously evaluated by the EPA in partnership with the same diverse group of stakeholders whose ideas contributed to EPA's initial list of innovations worth testing. Those projects that survive such rigorous scrutiny might later become the basis for rulemaking or even new legislation, thereby preserving those ideas that truly demonstrate superior environmental performance.[173] We will revisit Hirsch's proposal below in the discussion of privacy covenants.[174]

Negotiated Rulemaking. – Negotiated rulemaking (also referred to as regulatory negotiation or "reg neg") is a statutorily defined process by which agencies formally negotiate rules with regulated industry and other stakeholders as an alternative to conventional, notice-and-comment rulemaking.[175] The core insight underlying negotiated rulemaking is that conventional rulemaking discourages direct communication among the parties, often leading to misunderstanding and costly litigation over final rules. In contrast, negotiated rulemaking brings together agency personnel and representatives of the affected interested groups to negotiate the text of a proposed rule based on shared information more honestly presented and a willingness to compromise. If the negotiations succeed by achieving a consensus on a proposed rule, the resulting final rule should be of better quality, easier to implement, enjoy greater legitimacy, and lead to fewer legal challenges.[176]

The NRA establishes a statutory framework for negotiated rulemaking under which agencies have the discretion to bring together representatives of the affected parties in a negotiating committee (for example, industry, environmental and consumer groups, and state and local governments) for face-to-face discussions. If the committee reaches a consensus—which is defined as "unanimous concurrence among the interests represented" unless the committee agrees on a different definition such as general concurrence[177]—the agency can then issue the agreement as a proposed rule subject to normal administrative review processes. Proposed rules emerging from a negotiated rulemaking process are also subject to judicial review.[178] While the NRA augments APA rulemaking, it does not replace it. Indeed, most of the language of the Act is permissive and, as administrative law expert Jeffrey Lubbers notes, "the Act does not require

[173] For a discussion of how these three changes to Project XL overcome criticisms of the current program, *see id.* at 255-57.

[174] *See infra* III.B.2.

[175] Under the Administrative Procedure Act (APA) of 1946 (5 U.S.C. §551 *et seq.)*, conventional rulemaking generally requires publication of the proposed rule in the *Federal Register*, an opportunity for interested persons to comment on the proposed rule, and publication of a final rule at least 30 days prior to its effective date; *see* 5 U.S.C. § 553.

[176] *See* Negotiated Rulemaking Act of 1990 (the NRA), Pub. L. 101-648, 104 Stat.4969 (codified as amended at 5 U.S.C. §§ 561-570), Section 2(3)-(5), Congressional Findings; *see also* EPA, Negotiated Rulemaking Fact Sheet, *available at* www.epa.gov/adr/factsheetregneg.pdf; Philip J. Harter, *Negotiating Regulations: A Cure for Malaise*, 71 GEO. L.J. 1 (1982) (discussing negotiation as a means of breaking deadlocks produced by the conventional rulemaking process).

[177] 5 U.S.C. §562(2).

[178] *See* 5 U.S.C. §563(a)(7) and §570.

the agency to publish either a proposed or final rule merely because a negotiating committee proposed it."[179] If negotiations fail to reach consensus, the agency may proceed with its own rule.

Negotiated rulemaking under the NRA has five distinct phases: First, the head of an agency or a must determine whether the use of the negotiated rulemaking procedure is in the "public interest" based on seven statutorily identified criteria including need for the rule, whether there are a limited number of identifiable interests that will be substantially affected by the rule, the likelihood of achieving consensus without unreasonable delay, availability of agency resources, and agency commitment to using the committee's proposed rule as the basis for a new agency rule.[180] To assist in its determination, the agency may select a neutral "convener" to conduct a feasibility analysis and to identify persons who are qualified to represent affected interests.[181] Agencies are authorized to pay expenses of committee members otherwise lacking adequate financial resources to participate.[182]

Second, if the agency makes a favorable decision to move ahead with a negotiated rulemaking, it must publish a notice in the *Federal Register* describing the subject and scope of the proposed rule, a list of affected interests and potential members of the negotiating committee, and a solicitation for comments as well as instructions for how to apply or nominate another person for membership.[183] Third, after considering the public comments, the agency may establish a negotiated rulemaking committee of no more than twenty-five members including at least one person representing the agency.[184] Fourth, although the negotiating committee must be established in accordance with the Federal Advisory Committee Act (FACA),[185] the agency may (with the consensus of the committee) select a "facilitator" to chair meetings and assist committee members in conducting discussions and negotiations.[186] The activity of the negotiating committee includes assembling, analyzing and agreeing upon relevant data, consulting with constituents, identifying and analyzing options, attaining constituent ratification, and finalizing the proposed rule.[187] If the committee reaches a consensus, it must submit a report to the sponsoring agency containing the text of the proposed rule along with any other relevant information or recommendations; if it fails to reach consensus, the committee must submit a report specifying any areas of agreement.[188] Finally, the committee must terminate no later than promulgation of the final rule.[189]

---

[179] *See* Jeffrey S. Lubbers, *Achieving Policymaking Consensus: The (Unfortunate) Waning of Negotiated Rulemaking*, 49 S. Tex. L. Rev. 987, 989 (2008).

[180] *See* 5 U.S.C. §563(a).

[181] *See* 5 U.S.C. §563(b).

[182] *See* 5 U.S.C. §568(c).

[183] *See* 5 U.S.C. §564. The opportunity to comment or apply for membership must remain open for at least thirty days; *see* 5 U.S.C. §563(c).

[184] *See* 5 U.S.C. §565(a)-(b). If the agency decides not to establish such a committee, it must publish a notice of that fact and the reasons for its decision; *see* 5 U.S.C. §565(a)(2).

[185] Pub. L. No. 92-463, *86 Stat. 770 (1972)*(codified at 5 U.S.C. *app* 2)(regulating the formation and operation of federal advisory committees including members who are not full-time federal employees). FACA requires that an advisory committee obtain a charter, maintain a balanced membership, hold open public meetings at which the public may speak or file written statements, keep minutes or summaries, and maintain all committee documents for public inspection.

[186] *See* 5 U.S.C. §566(c)-(d). The facilitator chairs the meetings and assists in negotiations and is frequently the key appointment in ensuring a successful outcome; *see* Selmi, *infra* note 199 and accompanying text.

[187] *See* 5 U.S.C. §567; ADMINISTRATIVE CONFERENCE OF THE U.S., NEGOTIATED RULEMAKING SOURCEBOOK (David M. Pritzker & Deborah S. Dalton eds., 1995).

[188] *See* 5 U.S.C. §566(f).

[189] *See* 5 U.S.C. §567.

The promise of negotiated rulemaking is that by enlisting diverse stakeholders in the rulemaking process, responding to their concerns and reaching informed compromises, better quality rules will emerge at a lower cost and with greater legitimacy.[190] Critics counter that the process not only fails to deliver its purported benefits (and then only rarely) but that its very use undermines the foundations of administrative law by shifting the decision-making function from agencies tasked with protecting the public interest to a collection of interest groups with their own private agendas.[191] In 2000, administrative law scholars Jody Freeman and Laura Langbein published a comprehensive analysis and summary of an empirical study of negotiated rulemaking.[192] The study compared participant attitudes toward negotiated versus conventional rulemaking. Based on their analysis, they concluded that "reg neg generates more learning, better quality rules, and higher satisfaction than conventional rulemaking" as well as increasing legitimacy, which they defined as "the acceptability of the regulation to those involved in its development." [193]

But even if this very positive analysis is taken at face value, Lubbers shows that EPA use of negotiated rulemaking is in fact quite limited, falling in recent years from sixty-three negotiating committees formed between 1991 and 1999 to only twenty-two between 2000 and 2007. This is a significant decline, especially given that fifteen committees formed in the later period were mandated by statute.[194] Lubbers identifies several factors that may explain the waning of negotiated rulemaking including budgetary issues, the lack of enthusiasm for reg neg at the Office of Information and Regulatory Affairs (OIRA), and the applicability of FACA, which agencies and stakeholders may find unduly burdensome.[195] Yet Lubbers contends that this waning is unfortunate given the proven value of reg neg in providing creative solutions to regulatory problems.[196]

Despite this drop off in use, environmental law scholars have identified a few situations where the negotiated rulemaking should provide EPA with significant advantages. For example, Andrew Morris and his colleagues point to situations "where the substance of the regulation requires the credible transmission of information between the regulated entities and other interest groups, and where the agency's preference for a particular substantive outcome is weak."[197] Reg neg also requires "a relatively high degree of shared interest among the groups participating, the existence of gains from trade to allow parties to compromise, and a willingness by interest groups to reject the role of spoiler."[198] These views are largely consistent with the findings of Daniel Selmi, who conducted a detailed study of the negotiation of a regional air quality rule. Selmi explained why the parties were willing to compromise as follows: industry believed that

---

[190] *See* Harter, *supra* note 176.

[191] For a discussion of the main lines of criticism, *see* Lubbers, *supra* note179 at 1003-04.

[192] *See* Jody Freeman and Laura I. Langbein, *Regulatory Negotiation and the Legitimacy Benefit*, 9 N.Y.U. ENVIR. L. REV. 60 (2000)(presenting analysis and a summary of empirical evidence from Neil Kerwin and Laura Langbein's two-phase study of Environmental Protection Agency (EPA) negotiated rulemakings). I want to thank Peter Schuck for referring me to this article and alerting me to the relevance of the reg neg debate.

[193] *Id.* at 63.

[194] *See* Lubbers, *supra* note179 at 996. Although the NRA gives agencies discretion as to whether to rely on negotiated rulemaking, Congress has mandated it use in several statutes across a range of issues. For a list of Congressionally mandated reg negs, *see* Lubbers, *id.* at 1007-1015, Appendix.

[195] *Id.* at 996-1005.

[196] *Id.* at 1006 (giving the example of a recent reg neg involving a regional air quality rule).

[197] Andrew P. Morriss et al., *Choosing How to Regulate*, 29 HARV. ENVTL. L. REV. 179, 183 (2005).

[198] *Id.*

regulation was inevitable; the environmental groups recognized that even thought they preferred an outcome based on new and expensive technology, they lacked the political capital to achieve this result; while the agency was not locked into a rigid, initial position but remained open towards finding a solution that responded to information acquired during the negotiations. But the key factor in reaching a compromise was a very practical one, namely, that the facilitator had the necessary skills to assist the parties in identifying their priorities and helping them make tradeoffs in which they each achieved some of their goals.[199]

A final topic before concluding this discussion: Why does the covenanting approach succeed at all in achieving potentially better solutions to environmental problems than command-and-control regulations? Stewart offers an explanation based on the logic of Coasian bargaining principles:

> The premise is that legal rules will advance society's welfare if there are voluntarily agreed to by all relevant interests. If those with a stake in the regulatory requirements—the regulated, the regulator, and perhaps third party environmental or citizen interests—agree on an alternative to the standard requirements, the agreement may be presumed to be superior the standard.[200]

Freeman and Langbein explain the success of reg neg in terms of the very nature of the process, with its emphasis on "stakeholder representation, face-to-face negotiation, [and] consensus-based decision making."[201] Finally, Ayres and Braithwaite recommend negotiations through a tripartite process in which representatives of government, industry and public interest groups (PIGs) are equally matched and empowered.[202] What all these explanations have in common is a focus on information sharing, direct negotiations, self-interested mutual compromises, and voluntary agreement.

---

[199] *See* Daniel P. Selmi, *The Promise and Limits of Negotiated Rulemaking: Evaluating the Negotiation of a Regional Air Quality Rule*, 35 ENVTL. L. 415, 435-38 (2005). Scholars disagree over a much more general issue regarding the suitability of reg neg in any given situation. Selmi notes that some scholars "argue that controversial rules make good candidates for negotiation, while others contend the process is best utilized for narrow questions of implementation. A third group stresses that agencies should use negotiation to tackle situations where the policy implications are limited" (citations omitted); *see id.* at 468.

[200] Stewart, *supra* note 153 at 61. Stewart further explains:

> … each party to an environmental agreement will seek to maximize its share of the gains produced by the negotiated departure from standard requirements. A regulated firm or industry will seek to use the flexibility afforded by environmental agreements to reduce compliance costs and other burdens by using alternative or innovative means that would be precluded by the default requirements, gaining flexibility as to the timing of compliance investments, and reducing regulatory uncertainty. Regulated actors will seek security against future changes in the alternative requirements negotiated. For their part, the regulators and environmental and citizen group third parties will seek a higher level of environmental or other benefits than would have been obtained, as a practical matter, under the standard default requirements. Regulators may also seek to reserve the authority unilaterally to impose new requirements if new environmental problems arise or the agreement for other reasons later proves environmentally inadequate. … It will also be necessary to structure the negotiation and representation process so as to minimize the transaction and bargaining costs that could prevent successful negotiation.

Id. at 61-62.

[201] *See* Freeman and Langbein, *supra* note 192 at 71, 132-135.

[202] *See* Ayres and Braithwaite, *supra* note 67 at 55-56. In fairness to Ayres and Braithwaite, they present tripartism not as an explanation of why regulatory covenants might result in better rules but as a game-theoretic solution to the problem of regulatory capture; *see id.* at 54-100.

In sum, both Project XL and negotiated rulemaking have strengths and weaknesses. Key strengths include *innovation* (because covenants invite firms to tap into their own ingenuity to devise lower cost solutions); *flexibility* (in the form of tailored rules that either match the circumstances of an individual firm (as in Project XL) or the underlying conditions faced by a regulated industry based on superior expertise (as in negotiated rulemaking)); greater *commitment* (because companies write or at least negotiate their own rules rather than having them imposed externally); and more effective *compliance* (because internal discipline as practiced by firms that agree to rules of their own devising is likely to be more extensive and cheaper for everyone than government investigations and prosecutions). On the other hand, covenants have a number of obvious weaknesses including higher administrative burdens associated with negotiating the rules (although this might be mitigated by lower overall compliance and litigation costs); legal uncertainty in the case of Project XL; and a bias against small firms, which typically lack the resources necessary to negotiate facility-based standards or to participate in a negotiating committee.[203]

2. Privacy Covenants

Hirsch examines Dutch codes of conduct as his primary example of a privacy covenant reflecting second-generation regulatory strategies. Dutch data protection law allows industry sectors to draw up codes for processing of personal data, which are then submitted to the Dutch Data Protection Authority (DPA) for review and approval.[204] Specifically, organisations considered "sufficiently representative" of a sector and that are planning to draw up a code of conduct may ask the DPA for a declaration that "given the particular features of the sector or sectors of society in which these organisations are operating, the rules contained in the said code properly implement" Dutch law.[205] Art. 25(4) of the PDPA further provides that such declarations shall be "deemed to be the equivalent to" a binding administrative decision, making it similar in effect to FTC approval of COPPA safe harbor guidelines (in which case Dutch firms that comply with an industry code would be deemed to be in compliance with the Dutch PDPA). According to Hirsch, the DPA has 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.[206]

This Dutch approach is generally consistent with that of the EU Data Directive—Article 27(1) 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."[207] Ireland also has approved three codes of practices under its data protection law.[208] But the Dutch and other EU Member States are not alone in pursuing a covenanting approach. Australian privacy law also permits organisations to develop sectoral

---

[203] For a similar list of the strengths and weaknesses of enforced self-regulation, *see* Ayres and Braithwaite, *id.* at 110-16, 120-28.

[204] *See* the Dutch Personal Data Protection Act (PDPA), Chap. 3, art. 25, *available and translated at* http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml.

[205] *Id.*

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

[207] Council Directive 95/46/EC, Article 27(1).

[208] *See* Irish Data Protection Commissioner, Self Regulation and Codes of Practice, *available at* http://www.dataprotection.ie/viewdoc.asp?DocID=98.

privacy codes for the handling of personal information "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."[209]

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 National Privacy Principles or NPPs (the Australian version of FIPPs) 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 Privacy Commissioner or a third party as an independent adjudicator to whom complaints may be made.[210] In addition, the Privacy Commissioner must be satisfied "that members of the public have been given an adequate opportunity to comment on a draft of the code."[211] Although codes are voluntary, approved codes are legally binding on any company that consents to be bound.[212]

Unfortunately, like COPPA safe harbors, 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.[213] In view of the complex and costly nature of the code approval process and the lack of interest shown by Australian industry, the Australian Law Reform Commission (ALRC) suggested various reforms of privacy codes. These included specifying that approved codes operate in addition to the privacy principles, rather than replacing them, thereby promoting national consistency while reducing fragmentation and confusion. Under this approach, codes would provide specific and binding guidance on how the principles should be applied in particular sectors.[214] 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."[215] 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

---

[209] *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.

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

[211] *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 209 at 5-6.

[212] *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.

[213] 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).

[214] *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/.

[215] 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.

public consultation process.[216] 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."[217]

Clearly, there is nothing in the US like the Dutch codes of conduct or the Australian privacy codes for the obvious reason that the US lacks a comprehensive privacy law much less one that allows domestic firms to develop or seek approval of sectoral codes. But for Hirsch at least this is not an insuperable obstacle to the covenanting approach given that under threat of federal privacy regulation, industry has sufficient incentive to sit down with regulators and seek out deals. Writing in 2006, Hirsch pointed to the 1999 OPA Guidelines as a rather incomplete step towards a covenanting approach.[218] Arguably, the longstanding dealings between the NAI and the FTC more closely approximate what Hirsch had in mind,[219] but he stops short of offering any detailed description of how industry might negotiate a covenant in the absence of any appropriate legislative framework. A final example of negotiated agreement between regulators and the online industry are the consent decrees entered into between the FTC and individual firms charged with unfair or deceptive trade practices under Section 5 of the FTC Act.[220]

Ironically, the US government had virtually no involvement in what may be the best, US-based example of a privacy covenant based on Coasian bargaining principles, namely, a voluntary effort in which three leading Internet firms partnered with a diverse group of non-governmental actors to negotiate free speech and privacy principles for the Internet. 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.[221] A few months later, Rep. Chris Smith introduced a bill that would've rendered such practices illegal and forced US companies to confront a Hobson's choice: disregard Chinese licensing requirements imposed on foreign companies as a condition of providing Internet services in the Chinese market or obey Chinese censorship rules in violation of US law.[222] The companies then sat down with a cross-section of human rights

---

[216] *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 214 at § 48.22.

[217] *Supra* note 215, No. 48, Privacy Codes.

[218] *See* Hirsch *supra* note 153 at 55 (noting three reasons for this incompleteness: the OPA guidelines were developed unilaterally, rather than in negotiations between the FTC and industry, and privacy advocates were not at the table, thereby resulting in weak standards; the FTC threatened but failed to issue prescriptive regulations, exacerbating free rider problems; and, absent new legislation, the FTC gained no additional powers to enforce the OPA guidelines.).

[219] *See supra* Section II.A.

[220] For a recent example, *see* In *the Matter of CVS Caremark Corporation*, FTC File No. 072 3119 (June 23, 2009)(requiring CVS Caremark to establish, implement, and maintain a comprehensive information security program, to refrain from future misrepresentation of company security practices, and to obtain bi-annual audits from a qualified, independent, third-party professional).

[221] Tom M. Zeller, Jr., *Online Firms Facing Questions About Censoring Internet Searches in China*, N.Y. TIMES, Feb. 15, 2006. For a more detailed description of the incidents involving each company, *see* Human Rights Watch, Race to the Bottom: Corporate Complicity in Chinese Internet Censorship (2006), *available at* http://china.hrw.org/timeline/2006/race_to_the_bottom.

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

organizations, socially responsible investment firms, and academics to work on voluntary guidelines to protect freedom of expression and privacy on the Internet. [223] After eighteen months of negotiations and defections by several NGOs, the multi-stakeholder group reached agreement and launched the Global Network Initiative (GNI), jointly committing to a set of principles and implementation guidelines as well as an accountability system based on independent, third-party assessments.[224] More recently, a GNI member (Google) announced that it was no longer willing to continue censoring the results of its Chinese search engine and therefore might be forced to shut it down.[225]

Why did Yahoo!, Google and Microsoft agree to participate in a multi-stakeholder process in which a successful outcome required convening a group of actors with divergent interests, and often at loggerheads with each other, engaging in difficult and protracted negotiations, and staying at the table until a consensus was forged? As described above, the GNI negotiations were an entirely voluntary effort, with no legal mandate as to process or substance. Rather, 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. Although the US State Department welcomed the GNI initiative, it did not participate in any stakeholder meetings. Cynics might say that the three firms were merely responding to a public relations crisis related to their business operations in China, which forced them to pursue a covenanting approach not only to improve their public image, but to restore public faith in their company integrity and mollify Congressional demands for government intervention.[226] But even if GNI was initially spurred by negative publicity and a threat of government intervention, and has so far not attracted any new members, it represents a moderately successfully example of the covenanting approach at work. In the absence of a government-supervised rulemaking process, the stakeholders relied on Coasian bargaining principles by sharing credible information, developing trust based on discussion of common interests, and staying at the bargaining table until they reached a voluntary agreement.

In sum, there are a number of subtly different models for privacy covenants depending on six factors: do negotiations among the parties occur (1) voluntarily or under a credible threat of government intervention? (2) At the sectoral or firm level? (3) In consultation with advocacy groups or with under a consensus model requiring their approval? (4) Are they legally binding or

---

[223] Other stakeholders included the Center for Democracy and Technology, the Electronic Frontier Foundation, Human Rights First, Human Rights in China, Human Rights Watch, the Calvert Group, Domini Social Investments and F & C Asset Management. For a full list of participants, *see* Global Network Initiative, http://www.globalnetworkinitiative.org/participants/index.php.

[224] The guidelines state that companies should establish human rights risk assessment procedures and integrate the findings into business decision-making; require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression and privacy; provide users with clear, prominent and timely notice when access to specific content has been removed or blocked; encourage governments, international organizations and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy; and utilize independent assessments of company implementation of the GNI's principles. For the GNI's three core commitment documents, *see* http://www.globalnetworkinitiative.org/index.php. Other examples of multi-stakeholder processes designed to achieve basic human rights include 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.

[225] S*ee* Kim Zetter, *Google to Stop Censoring Search Results in China After Hack Attack*, WIRED, Jan. 12, 2010, *available at* http://www.wired.com/threatlevel/2010/01/google-censorship-china/.

[226] *See* Neil Gunningham, *Environment, Self-Regulation, and the Chemical Industry: Assessing Responsible Care*, 17 LAW & POL'Y 57, 63 (1995) (citing these three factors as the reason that large multinationals in the chemical industry established a voluntary initiative known as Responsible Care in the wake of the Bhopal disaster).

merely precatory? (5) May they derogate from applicable legal standards by being both more or less stringent? And (6) may they be initiated only by the private sector or may they be requested by the government or even imposed on a recalcitrant sector or firm?

C. From Self-Regulation to Regulatory Innovation

The previous section examined second-generation environmental regulatory strategies including Project XL and negotiated rulemaking and then analyzed existing privacy covenants such as Dutch and Australian privacy codes sanctioned by law. These statutory codes were then contrasted with a voluntary code—the GNI—which relied on a multi-stakeholder process designed to achieve human rights protections. With the exception of the GNI, all of these initiatives are co-regulatory; they combine self-initiated rules devised by industry with some degree of government oversight. More specifically, they fall within the category of mandated self-regulation, which Rees earlier defined as "a governmental strategy for strengthening private regulatory systems." This next section draws lessons from the earlier discussion by sketching in three recommended approaches to regulatory innovation in privacy, all of which leave behind purely voluntary self-regulation in favor of mandated self-regulation.

The first is modeled on Hirsch's proposal of a Project XL for experimental projects and would enable FTC to test out new, and potentially better, regulatory approaches and PETs. Arguably, the Commission has regulatory authority under the FTC Act to issue a notice defining the goals, criteria and requirements of a "Project XL for Privacy" program and inviting interested parties to submit proposals for experimental projects.[227] The FTC would then select the best proposals and enter into binding covenants with the sponsors, who would run the projects as experiments subject to agency evaluation and review. The next section describes several innovative ideas of varying scope and ambitiousness that might be suitably recast as XL projects. These range from tools and techniques that supplement FIPPs to cutting edge proposals that depart substantially from the familiar control-based system of data protection at the heart of FIPPs.

The second regulatory innovation is simply for FTC to utilize negotiated rulemaking in appropriate situations. Because negotiated rulemaking presupposes that an agency has rulemaking authority, this approach is limited to those areas where Congress has enacted privacy laws authorizing the Commission to engage in rulemaking under the APA.[228] It seems likely that if Congress enacts privacy legislation, it will grant the FTC such authority to promulgate such regulations as may be necessary to carry out the purposes of the new law. Thus, the FTC may initiate a negotiated rulemaking for certain aspects of these rules. This section will specifically examine what a negotiated rulemaking involving OBA might look like and why it might achieve better results than a rule based on notice-and-comment.

The third and final approach also requires that Congress enact comprehensive substantive privacy legislation. It assumes that any such law will include a safe harbor provisions modeled on § 6503 of COPPA, and sketches out how this safe harbor would work if the incentives for participating and the process for drafting and approving industry guidelines were substantially modified in keeping with second-generation regulatory strategies.

---

[227] Project XL enjoyed White House support under Clinton's regulatory reinvention initiative. If there are doubts regarding FTC's authority to launch such a program, the Commission could seek Executive Branch support from the Office of Information and Regulatory Affairs or ask Congress for a new grant of legislative authority.

[228] For a discussion of FTC's rulemaking authority generally, *see infra* notes 244-246 and accompanying text.

1. Project XL for Privacy

As discussed in Part II, the ability of consumers to control the collection, use and transfer of their personal data is a fundamental aspect of any privacy regime centered on FIPPs. The control metaphor assumes that consumers can understand the written privacy policies they encounter online, thereby enabling meaningful consent experiences. But informed consent is rarer than hens' teeth because most online privacy notices are too long and complex, and too laced with legal jargon, for consumers to understand them. In response, both the private sector and NGOs like the World Wide Web Consortium (W3C) have developed various approaches for improving the notice-and-choice experience. These include point solutions such as use of multilayered notices,[229] standardized-table formats for privacy policies[230] icons representing behavioral advertising practices[231] experiments with "dashboards" that offer users greater control and transparency over their account data,[232] and improved anonymization techniques that seek to address data retention issues.[233] All of these tools and techniques may be characterized as PETs.[234] In 1997, W3C developed P3P, a computer protocol for helping web sites express their privacy practices in a standardized, machine-readable format that could be automatically retrieved and interpreted by tools built into browsers or separate applications. These tools allowed end users to set their own privacy preferences and thereby readily determine whether a Web site's practices were consistent with their own, with the goal of making users better equipped to make informed choices.[235]

These initiatives all tend to follow a similar pattern: sponsors launch the new PET with overly enthusiastic claims about its benefits, while at least a few privacy advocates denounce the PET as a subterfuge devised by industry mainly for the purpose of blocking new privacy legislation. For its part, the FTC may offer qualified support of the new PET in testimony, staff

---

[229] *See* The Center for Information Policy Leadership, Multilayered Notices, http://www.hunton.com/Resources/Sites/general.aspx?id=325 (last visited Feb. 12, 2010) .

[230] *See* P. Kelley, et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, Technical Report CMU-CyLab-09-014, Carnegie Mellon University (2009) *available at* http://www.cylab.cmu.edu/research/techreports/2009/tr-cylab09014.html.

[231] *See* The Future of Privacy Forum.org, Future of Privacy Forum Releases Behavioral Notices Study, http://www.futureofprivacy.org/2010/01/27/future-of-privacy-forum-releases-behavioral-notices-study/ (last visited Feb. 12, 2010)(describing study of behavioral advertising disclosures using icons as an alternative to providing transparency and choice via traditional online privacy notices).

[232] *See* Miguel Helft, *Google to Offer Ads Based on Interests, With Privacy Rights*, N.Y. TIMES, Mar. 11, 2009 at B3. (describing service that summarizes the data that Google collects in various users' accounts).

[233] *See* Miguel Heft, *Yahoo Limits Retention of Personal Data*, N.Y. TIMES, Nov. 5, 2009 (describing differences in data retention periods among leading search engine provides and quoting a Microsoft spokesman as stating that "the method of anonymization is more important than the anonymization timeframe").

[234] For an early overview of PETs, *see* Herbert Burket, *Privacy-Enhancing Technologies: Typology, Critique, Vision* in TECHOLOGY AND PRIVACY: THE NEW LANDSCAPE 125 (Philip E. Agre & Marc Rotenberg, eds.) (1998)(defining PETs as "[seeking] to eliminate the use of personal data altogether or to give direct control over revelation of personal information to the person concerned"). More recent work take a more comprehensive approach that has come to be known as Privacy by Design; *see, e.g.*, CDT, The Role of Privacy by Design in Protecting Consumer Privacy, Comments at the FTC Exploring Privacy: A Roundtable Series (Dec. 21, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00067.htm [hereinafter, CDT, The Role of Privacy by Design].

[235] S*ee* World Wide Web Consortium, The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Draft (Nov. 13, 2006) *available at* http://www.w3.org/TR/P3P11/.

reports, speeches or industry consultations, but refrains from taking a stance on any disputed regulatory issues. P3P is a paradigmatic case. Although W3C presented P3P as part of a larger, more comprehensive set of technical and legal solutions and never contended that it solved all privacy concerns on the Web,[236] Microsoft, AOL and Netscape behaved as if it largely obviated the need for an omnibus privacy law.[237] Meanwhile, EPIC and others condemned P3P harshly on numerous grounds.[238] Finally, while FTC supported P3P to the extent of testifying that a new privacy law might interfere with P3P's broad adoption by imposing incompatible notice requirements, the Commission never sought to resolve any of the legal issues concerning P3P that may have slowed its deployment.[239]

Project XL offers an alternative approach to this stalemate. As noted previously, experimental XL projects require a firm, trade association or standards organization to submit to FTC a proposal describing their new initiative in detail, including how it does a better job of protecting consumer privacy, whether it has the support of various stakeholders, and what regulatory relief if any might be required. Thus, innovative ideas developed within a Project XL framework not only could achieve greater regulatory certainty for their sponsors and early adopters but might also win the support of advocacy groups if they were consulted at the outset and given an opportunity to review a PET's design and implementation before it was set in stone. Ideally, all of the stakeholders would discuss whether the new approach achieves a high enough standard of privacy protection to justify regulatory relief such as FTC establishing clear guidelines for ensuring that P3P policies harmonize with written privacy statements while treating them as enforceable promises.[240] Certainly, a high profile project like P3P would have benefited from a more collaborative process in which all affected parties and the regulators worked together to embrace P3P's strong points rather than squabbling over its weak points.

In addition to experimenting with PETs that help implement FIPPs, the XL process also might be appropriate for exploring new approaches to privacy protection that refocus or even

---

[236] S*ee* P3P and Privacy on the Web, FAQ 22, *available at* http://www.w3.org/P3P/p3pfaq.html#solve (last visited Feb. 15, 2010).

[237] S*ee, e.g.*, Glenn R. Simpson, *The Battle Over Web Privacy: As Congress Mulls New Laws, Microsoft Pushes a System That's Tied to Its Browser*, WALL ST. J., March 21, 2001 at B1.

[238] *See, e.g.*, Electronic Privacy Information Center & Junkbusters Corp., Pretty Poor Privacy: An Assessment of P3P and Internet Privacy (June 2000), *available at* http://www.epic.org/reports/prettypoorprivacy.html.

[239] *See S. 2201, Online Personal Privacy Act, Hearings Before the Comm. on Commerce, Science and Transportation*, 107th Cong., 2nd Sess., Apr. 21, 2002 (Statement of Tim Muris, Chairman FTC) 11, *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_senate_hearings&docid=f:91368.pdf. The worrisome legal issues included the extent to which P3P policies were legally binding and/or fully discharged legal obligations under applicable notice-and-choice requirements and what Web sites should do about limitations of the P3P vocabulary, which made it difficult to express company privacy policies in P3P code. Indeed, one e-commerce expert characterized Microsoft's implementation of P3P in its Internet Explorer (IE) 6 browser as legally "hazardous" to web administrators and advised them to publish "dummy" P3P codes that would circumvent IE 6 cookie-filtering, while at the same time declaring in their P3P polices that such P3P codes "are meaningless and carry no effect." *See* Benjamin Wright, Disavow P3P Liability: Deploy Cookies with Legal Piece of Mind under Internet Explorer 6, *reprinted in* LAW OF ELECTRONIC COMMERCE P-15 (Jane Kaufmann Winn and Benjamin Wright, eds.) (4th ed. 2009). (Note: The author was lead privacy counsel at Microsoft when it built P3P capabilities into IE 6 and testified before Congress regarding the advantages of P3P for protecting consumer privacy; *see Need for Internet Privacy Legislation, Hearings Before the Comm. on Commerce, Science and Transportation*, 107th Cong., 1st Sess., July 11, 2001 (Statement of Ira Rubinstein, Assoc. Gen. Counsel, Microsoft Corp.), 84-95, *available at* http://ftp.resource.org/gpo.gov/hearings/107s/88997.pdf.)

[240] S*ee* William McGiveran, Note *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812 (2001)(recommending that lawmakers combine P3P code with market forces and a legal rationale based on enforcement of promises).

supplant FIPPs. For example, Fred Cate has suggested a new approach that emphasizes tangible harms. Cate argues that despite their lofty goals, FIPPs fail in practice by "maximizing consumer choice" rather than "protecting privacy while permitting data flows."[241] He has outlined 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.[242]

Building on Cate's analysis, the Business Forum for Consumer Privacy (BFCP) has proposed a new "use-and-obligations" model for implementing FIPPs.[243] This new model rejects the idea that consumers should have the primary responsibility for controlling the flow of personal information about them and policing its appropriate use, a task for which they are ill-suited given the complexity and lack of transparency of information flows in today's networked world. Rather, the use-and-obligations model "shifts responsibility for disciplined data use to the data collector and all holders (e.g., third party vendors) of data," imposing requirements on these data holders based upon how they use the data. The BFCP proposal identifies five categories of use: fulfillment, internal business processes, marketing, fraud prevention and authentication, and national security and legal. It then applies eight categories of obligations (based on FIPPs) together with a prevention of harm principle, to various business scenarios to illustrate how organization would "assess the risks to individuals raised by data collection and use, and take steps to mitigate these risks." Although the BFCP proposal is in its early stages, and requires additional work on establishing a framework for accountability, an XL project might be an excellent way to test it out and determine whether it achieves enhanced privacy protection, on the one hand, and what if any regulatory relief is appropriate under the existing, control-based approach to FIPPs, on the other.

Of course, not every privacy-enhancing initiative needs or deserves an XL project. In the environmental arena, the benefits of Project XL are reasonably clear: regulatory flexibility, reduced compliance costs and greater certainty regarding the regulatory implications of using new technologies or more integrated approaches. But privacy law is not nearly as hard and fast as environmental regulation nor is FTC enforcement as extensive or costly as EPA's civil, clean up and criminal enforcement programs. As a result, only a handful of highly regulated privacy leaders are likely to pursue a privacy-related XL project given the burdens of doing so and the high standards that the stakeholders and the FTC would require to obtain any guarantee of regulatory relief.[244] Nor would an FTC version of Project XL necessarily overcome the flaws in the original program such as the need for baseline requirements, better guidance regarding

---

[241] *See* Fred H. Cate, *The Failure of Fair Information Practice Principles* in CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 369 (Jane K, Winn, ed., 2006).

[242] Similarly, a group of MIT researchers 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; *see* Daniel J. Weitzner et al, *Information Accountability*, 51 COMM. OF THE ACM 82, 86 (2008)(arguing that "privacy is protected not by limiting the collection of data, but by placing strict rules on how the data may be used").

[243] BFCP submitted its proposal as a public comment to the FTC's recent Exploring Privacy: A Roundtable Series; *see* BFCP, A Use and Obligations Approach to Protecting Privacy: A Discussion Document, (Dec. 7, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.htm.

[244] This point was suggested to me by Lisa Sotto.

stakeholder participation, and (absent a statute) a lack of clear legal authority. But FTC could mitigate these problems by learning from the EPA experience and following Hirsch's advice: select a few meritorious projects with clear goals; devise an appropriate stakeholder process; and postpone any broader policy decisions until the experimental projects have been thoroughly scrutinized.

2. Negotiated Rulemaking and Online Behavioral Advertising

Should the FTC engage in negotiated rulemaking when issuing rules governing the online collection of personal information? Before considering the potential advantages of this approach, a brief discussion of the FTC's rulemaking authority is needed, given that it stems from two quite different sources. Under Section 18 of the FTC Act, the Commission has *limited* authority to prescribe rules defining "unfair or deceptive acts or practices in or affecting commerce."[245]

Before commencing a rulemaking under this section, however, the Commission must jump over high hurdles set by Congress in 1980 in response to perceived abuses of the agency's rulemaking authority. These requirements include advance rulemaking notice to Congress and the public, public hearings at which interested parties have limited rights of cross-examination, and a statement of basis and purpose addressing both the prevalence of the acts or practices specified by the rule and its economic effect.[246]

When Congress grants the FTC rulemaking authority to address a more narrowly focused problem under a specific statute, on the other hand, the Commission may use the notice-and-comment rulemaking procedures followed by most federal agencies. For example, the Commission has followed APA procedures in issuing rules regulating children's privacy,[247]

---

[245] *See* 15 U.S.C. §57a(a)(2).

[246] *See* 15 U.S.C. §57a(b)(1) and (2). *See generally* JULIAN O. VON KALINOWSKI ET AL., ANTITRUST AND TRADE REGULATION §5.14. The FTC's limited rulemaking authority under Section 18 merits some further explanation, although readers mainly interested in negotiated rulemaking may safely skip this footnote. Due to the burdensome and time consuming procedures imposed by Section 18, the FTC often prefers to rely on strategic enforcement actions to achieve its regulatory goals. This seems consistent with published statements of how the Commission views its option for regulating privacy practices. For example, in a July 14, 2000 letter to the EC explaining the agency's jurisdiction over such practices, former Chairman Pitofsky indicated that while Section 5 clearly provides a legal basis for enforcement actions against firms that misrepresent their privacy practices (deceptive practices) or that fail to secure their customers' personal information (unfair practices), "it currently may not be within the FTC's power to broadly require that entities collecting information on the Internet adhere to a privacy policy or to any particular privacy policy." *See* Issuance of Safe Harbor Principles, *supra* note 104, *65 Fed. Reg. at 45,883-685.* More recent statements by Liebowitz and Vladeck suggest that the Commission is reconsidering this policy as a result of dissatisfaction with a consumer privacy strategy based primarily on enforcement and self-regulation. *See supra* notes 45-46 and accompanying text. If Congress does not enact new substantive privacy law, it will be interesting to see if the Commission rethinks the appropriateness of using Section 18 to promulgate a rule requiring adherence to FIPPs. Alternatively, Congress is currently considering a new financial regulatory reform bill that includes a provision lifting the restrictions on Section 18 rulemaking procedures. *See* the Wall Street Reform and Consumer Protection Act of 2009, H.R. 4173, 111th Cong., 2nd sess., Sec. 4901 (2009). If enacted, this law would amend §57a(b) to allow the FTC to promulgate rules defining unfair or deceptive practices using conventional rulemaking procedures under the APA, without having to observe any additional procedural safeguards.

[247] *See* COPPA, 15 U.S.C. § 6503(b)(1).

financial privacy,[248] and the standards for commercial email marketing.[249] Although the Commission did not rely on the negotiating rulemaking process for any of these rules, nothing prevents it from doing so in the future if it were to modify an existing rule under COPPA, GLB or CAN-SPAM. This is also the case if Congress were to enact new, substantive privacy legislation and this statute specifically authorized APA rulemaking as necessary to implement any newly-defined privacy principles.

With these preliminaries out of the way, this section now argues that if Congress passes a bill along the lines suggested by Rep. Boucher, the FTC *should* rely on negotiated rulemaking to address the privacy concerns raised by OBA. Boucher described his plans to include in his bill a safe harbor program for firms engaged in OBA. To qualify, firms would need to allow consumers to opt-out of network advertising or to view and modify, or opt out of entirely, the profile maintained about them for advertising purposes. His bill would also direct FTC to promulgate a rule implementing this provision. As discussed previously, negotiated rulemaking is most beneficial when the underlying rule requires information sharing between the regulators, the regulated industry and other affected parties, and the parties believe they have something to gain from working together and achieving a compromise.[250] Arguably, these conditions would be met if the FTC formed a negotiated rulemaking committee to tackle a safe harbor rule addressing OBA.

A negotiated rulemaking for OBA may strike the reader as quixotic. After all, industry's bottom line is to maintain the free flow of information including personal data needed for ad targeting, which in turn increases advertising revenues; hence, it strongly favors an opt-out regime backed by accountability measures such as compliance reviews conducted by trade associations. Advocates, on the other hand, seek more meaningful protection from intrusive profiling, hence they demand legislative solutions based on opt-in choice, a broader definition of PII, very short data retention periods, and external audits. These differences are deep-seated and perhaps ideological, and not easily ignored.[251] Yet there is reason to believe that all of the affected parties—the regulated industry, the advocates representing the public interest, and the regulators—might be highly motivated to engage in face-to-face negotiations and would benefit from the information sharing that inevitably occurs in this setting.

As to motivation: First, industry should recognize that if Congress enacts a new privacy law, it is very likely to regulate OBA, while if Congress fails to act, Leibowitz and Vladeck are very likely to reject further self-regulation as inadequate and instead pursue a far more aggressive enforcement strategy or even a new rulemaking directed at OBA practices. Second, advocates should realize that they face an uphill battle in persuading Congress that new privacy legislation would have no negative economic impacts on the online advertising revenues that currently subsidize free online content and services or that a drop in these revenues won't result

[248] *See* Gramm-Leach-Bliley (GLB) Act of 1999, §§ 501, 504, 15 U.S.C. §§ 6801, 6804 (2000).

[249] *See* the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, § 13, 15 U.S.C. § 7711.

[250] *See supra* text accompanying notes 200-202.

[251] This roughly describes the current state of play. After the FTC staff issued its report on self-regulatory guidelines in the online advertising industry, *see supra* note 44, a consortium of advertising trade groups issued a new set of privacy principles in the hopes of fending off regulation by closely tracking the FTC's recommendations; *see* Stephanie Clifford, *Industry Tightens Its Standards for Tracking Web Surfers*, N.Y. TIMES, July 1, 2009. 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.

in higher costs for consumers. Third, the FTC is not yet locked-in to any one approach. To the contrary, when Leibowitz was recently asked what people should expect from the FTC's roundtable series on privacy and where the agency was headed, he answered: "I can honestly say: we don't know. Our minds are open." [252]

Finally, as to information sharing: the negotiated rulemaking process by its very nature encourages more credible transmission of information among the parties. To begin with, the network advertising industry undoubtedly possesses greater expertise and insight into the complex technology and evolving business models underlying OBA than either privacy advocates or FTC staff. In the past, this information has been shared or elicited mostly through one-sided communications—unilateral codes of conduct; complaints filed with the FTC; or charges and countercharges at public forums. In a negotiated rulemaking process, however, the logic of Coasian bargaining prevails. In other words, each party seeks to "maximize its share of the gains produced by departure from standard requirements" and this requires that parties "educate each other, pool knowledge, and cooperate in problem solving."[253] In short, when both sides engage in explicit bargaining over priorities and tradeoffs, they are far more likely to achieve a satisfactory compromise than by relying on the indirect communications that characterize conventional notice-and-comment rulemaking.

3. Statutory Safe Harbors Revisited

The previous section examined the potential use of negotiated rulemaking in the event that Congress enacted a new law that included a safe harbor for firms that collect and use data for OBA purposes, provided they follow certain specified practices. This section offers a much broader look at how Congress might integrate the covenanting approach into any new privacy legislation by including a revamped safe harbor provision. Assume for the sake of argument that Congress enacts privacy legislation requiring websites that collect information from Internet users to follow default requirements based on FIPPs, unless they participate in an approved safe harbor modeled on §6503 of COPPA. A modest approach to redesigning this safe harbor might be to add several new elements based on the Dutch and Australian privacy codes discussed above. For example, Congress might grant the FTC broad discretion to approve self-regulatory guidelines for different industry sectors so long as (1) the organization seeking approval is sufficiently representative of the sector; (2) industry members consult with other interested parties, including privacy and consumer advocacy groups, and/or engage in direct negotiations with them; (3) industry clearly justifies any derogation from FIPPs; (4) the Commission reviews industry guidelines under a notice and comment process before final approval; and (5) approved guidelines bind only those companies that chose to participate.

Of course, this brief description raises more questions than it answers: Which trade associations should FTC work with, especially if there are competing organizations with

[252] *See* Jon Leibowitz, Chairman, FTC, Introductory Remarks at the FTC's Exploring Privacy-A Roundtable Series (Dec. 7, 2009), http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf ; *see also* Vladeck Interview, *supra* note 46 (when asked what he meant by clearer notice and consent, Vladeck stated: "I don't want to suggest that we've prejudged anything. I think the key is transparency across the board …. I don't know whether we'd gravitate toward a universal opt-in").

[253] *See* Freeman and Langbein, *supra* note 192at 69. For a very similar point, *see* Morriss, *supra* note 197 at 201 (observing that "…agencies may need the negotiation process to allow one set of interests to make credible commitments or disclosures to another set of interests that enable the regulation to be recognized as a Pareto improvement").

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? The negotiated rulemaking process answers these questions definitively, so perhaps Congress should encourage its use as the principal (but not exclusive) method of approving proposed safe harbor programs under a new privacy law.

For a new safe harbor program to have much likelihood of success, Congress would also need to ensure that industry did not view privacy codes 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, Congress could define specific standards as a default, but then allow the FTC to negotiate tailored requirements with firms or industry trade groups that substitute for compliance with the default standards. Those firms that did not sign up for a code of conduct still would have to comply with the default requirements, thereby overcoming the free-rider problem. But 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, Congress should use both sticks and carrots.[254] 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 demonstrate high performance avoid these sticks and/or enjoy these carrots. What sticks and carrots might be devised to enhance a new privacy safe harbor, given that the COPPA safe harbor 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. In sharp contrast, compliance with approved self-regulatory guidelines would not only serve as a safe harbor in any enforcement action but exempt program participants from civil law suits and monetary penalties.[255] Additional carrots might include official government recognition

[254] *See* Fiorino, *supra* note 153 at 124.

[255] 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

of superior performance by top tier performers in safe harbor programs (while non-participating firms would be ineligible for such recognition) as well as certain purchase preferences. (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.[256]

What, then, are the privacy practices that industry must follow to be eligible for safe harbor treatment? Before addressing this key issue, a brief summary of the argument so far is in order. 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, one of the purposes of second generation strategies like those described in the previous section is to distinguish good performers from bad performers and treat them accordingly. This means reserving safe harbor benefits (both availability of carrots and avoidance of sticks) for top tier

---

(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. Not all safe harbors shield participants from liability, however. Some safe harbor programs 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 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.

[256] 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*).

firms as determined by suitable performance measures.[257] Obviously, this requires reliable performance measures, such as—in the environmental field—exceeding targeted goals for reducing pollution or emissions.[258] Arguably, privacy performance is harder to measure than air or water quality. At the very least, the science of measuring privacy performance is in the early stages of development. Yet is it still possible to sketch out some preliminary views on what steps firms should take to achieve higher levels of privacy protection for consumers. This is a very large and complex topic and well beyond the scope of this paper. The next few paragraphs briefly consider a holistic approach to privacy protection, which has three subcomponents: data governance, privacy methodologies and best practices.[259] After briefly describing each component, this section concludes with a few observations on how government should—and shouldn't—develop performance measures based on this holistic approach.

Data governance is "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."[260] 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;[261] (2) publicizing within the company who has authority and accountability for governance decisions; (3) deployment of enough 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.

Second, a privacy team with data governance responsibilities also needs to ensure that a firm follows suitable methodologies to ensure the implementation of privacy protection measures into all information-related processes that collect or use personal data. (This team may consist in

---

[257] *See* Fiorino, *supra* note 153 at 200-01 (describing how agencies might incorporate performance tiers into regulations by defining criteria for differentiating among firms and deciding how top performers should be treated differently).

[258] *See supra* note 154.

[259] For a preliminary description of the holistic approach to privacy protection, the best source is a Discussion Document prepared for 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. Others have discussed similar ideas under the rubric of Privacy by Design; *see also* CDT, The Role of Privacy by Design, *supra* note 234 at 4 n. 6 (referencing privacy by design initiatives of IBM, Sun, HP and Microsoft). The relation of privacy to information technology is currently under examination within the internationals standards community by Joint Technical Committee 1 (JTC 1) of the International Standards Organization (ISO). In particular, Subcommittee 27 (SC 27), IT Security Techniques, is working on several projects including ISO/IEC/ WD 29100, *Privacy Framework;* ISO/IEC/ WD 29101, *Privacy Reference Architecture;* and ISO/IEC/ NP 29190, *Proposal on a Privacy Capability Maturity Model.* For the ideas discussed in the following paragraphs, I reviewed these materials and relied as well 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).

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

[261] *See* Bennett and Raab, *supra* note 259 at 267 (noting that CPOs help ensure that data governance issues are debated at the top level of the organization); Swire, *supra* note 152.

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, 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;[262] (8) use of leading edge development processes; (9) use of privacy impact assessments (PIAs) for new products or initiatives;[263] (10) use of methods for addressing privacy issues with third-parties such as suppliers, outsourcing partners and agency workers;[264] and (11) use of a privacy incident handling process.

Finally, most organizations that implement data governance systems and appropriate privacy methodologies rely on additional 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;[265] (14) use of specific privacy-protective techniques such as layered notice, data anonymization, P3P and other PETs;[266] (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 not at all clear whether these nineteen factors constitute the necessary and sufficient criteria for improving privacy performance or how exactly they might be translated into performance measures for purposes of safe harbor eligibility. Two points are clear, however. First, government should rely principally on the private sector, academia and international standards bodies for further development of the holistic approach described above. Second, government should not attempt to define performance measures. Rather, it should support existing efforts to develop such measures by funding academic research, encouraging US trade associations and firms to participate in international standards efforts, and—as these standards mature—promoting market demand through purchasing criteria, giving preferred regulatory

---

[262] The FTC already endorses this approach; s*ee* 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).

[263] *See* Bennett & Raab, *supra* note 259 at 204-10.

[264] The FTC already endorses this approach as well; *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").

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

[266] *See supra* notes 235-240 and accompanying texts.

treatment to firms that meet these emerging requirements, or expressly adopting privately generated standards in public regulation.[267]

IV. CONCLUSION AND RECOMMENDATIONS

Whatever its shortcoming, and despite its many critics, self-regulation is a recurrent theme in the US approach to online privacy and perhaps a permanent part 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 applied solutions.

Next, this Article presented three case studies of mandated self-regulation. This included overviews of the NAI Principles and the SHA, as well as a more empirical analysis of the CARU safe harbor program. An assessment of these case studies against five criteria (completeness, free rider problems, oversight and enforcement, transparency, and formation of norms) 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 is chiefly 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."[268] 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, this Article concludes with a set of specific recommendations based on the ideas discussed in Part III.C.

If Congress enacts comprehensive privacy legislation based on FIPPs, the first recommendation is that the new law include a safe harbor program, which should echo the COPPA safe harbor to the extent of encouraging groups to submit self-regulatory guidelines and, if approved by the FTC, treat compliance with these guidelines as deemed compliance with statutory requirements. The FTC should be granted APA rulemaking powers to implement necessary rules including a safe harbor rule. Congress should also consider whether to mandate a

[267] Once again environmental law provides insights into these policy instruments. *See, e.g.*, Hirsch, *supra* note 153 at 60-63 (discussing Environmental Management Systems (EMSs) as a model for using organizational practices and procedures to improve privacy); Fiorino, *supra* note 153 at 144-49 (describing the EPA's National Environmental Performance Track, an initiative that gives special treatment to firms meeting four criteria: sustained compliance with environmental law; use of an EMS; public outreach; and committing to continuous improvement in environmental performance); Errol E. Meidinger, *Environmental Certification Programs and U.S. Environmental Law: Closer Than You May Think*, 31 ENVTL. L. REP. 10,162 (2001) (describing environmental certification programs and how they are incorporated into legal systems).

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

negotiated rulemaking for an OBA safe harbor or for safe harbor programs more generally. In any case, FTC should give serious thought to using the negotiated rulemaking process in developing a safe harbor program or approving specific guidelines. In addition, the safe harbor program should be overhauled to reflect second-generation strategies. Specifically, the statute should articulate default requirements but allow FTC more discretion in determining whether proposed industry guidelines achieve desired outcomes, without firms having to match detailed regulatory requirements on a point by point basis.

Second, 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.C. The FTC would need to approve both components. Third, the enforcement provision should include new incentives such as tiered liability and lighter regulatory burdens for firms that qualify for safe harbor treatment. Finally, because performance measures for privacy remain an underdeveloped area with scant literature describing these measures or their usefulness in predicting superior performance, the FTC should support non-governmental efforts for developing appropriate measures of privacy performance.