The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?

Dennis D. Hirsch†

I. INTRODUCTION

The rise of the Internet poses profound new challenges for information privacy.[1] Companies such as Google save and store our every search query and can often trace them back to us as individuals.[2] Websites track how we use their sites and frequently share this information with others.[3] Internet service providers (ISPs) have begun to examine the packets of information by which we communicate with the Internet and to search them for data that will reveal our preferences and behaviors.[4] These companies do not engage in these activities because they dislike privacy. They do it because personal information, which can be used for marketing and many other purposes, has economic value. As a result, the Internet has become Janus-faced.[5] On one hand, it appears to offer great freedom and anonymity. On the other, it ferrets out and stores everything from our most banal behaviors to our deepest secrets.[6] This not only damages individual privacy; it also erodes people's trust in the online environment and threatens to undermine the continued growth of

† Geraldine W. Howell Professor, Capital University Law School. The author would like to thank: Daniel Fiorino, Ira Rubinstein, and Professors Susan Rose-Ackerman, Douwe Korff, Margriet Overkleeft-Verburg, Bernt Hugenholtz, Joris van Hoboken, Nico van Eijk, and Natali Helburger for offering insightful suggestions about, and support for, this project; Daniel Lenert for providing superb and diligent research assistance; and Capital University Law School for supporting this project with a summer research grant. The author alone is responsible for any errors or omissions.

1. S*ee generally* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (2001) (providing a clear and informative overview of this phenomenon).

2. *See infra* notes 34–53 and accompanying text (describing this practice).

3. *See infra* notes 34–53 and accompanying text (describing this practice).

4. *See infra* notes 57–62 and accompanying text (describing this practice).

5. Janus was a Roman god. The Romans typically depicted him with two faces looking in opposite directions. The term "Janus-faced" has accordingly come to mean two-faced. *See* MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 669 (11th ed. 2007) (defining "Janus" and "Janus-faced").

6. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1619–20 (1999) [hereinafter Schwartz, *Cyberspace*].

the Internet economy.[7] If the United States is to continue to be a society in which personal privacy and the Internet economy flourish together, then it is vital that we find an effective way to protect personal information on the Internet.[8]

Two main camps currently dominate the discussion as to how to protect personal privacy on the Internet. The first calls for government regulation.[9] It seeks legislation that would set strict limits on how companies collect data online, what types of personal information they can collect, and how they can use it.[10] Proponents of this approach maintain that strong government regulation is necessary to protect unsuspecting Internet users from the self-interested behavior of Internet-based companies.[11] The second camp, which has thus far won the day, resists government intrusion in the fragile and fast-moving Internet economy and argues that market and industry self-regulation will yield better results than government rules.[12] It maintains that Internet businesses already have a market incentive to protect user privacy to avoid losing customers.[13] Government regulation is unnecessary and could prove counterproductive.[14]

This Article has two main purposes. First, it shows that critics of both the government regulation and the market/self-regulation approach-

---

7. Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 28–30 (2006) (discussing a "tragedy of the commons" scenario that could cause many Internet users to lose trust in the medium and pull back from the online environment); Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1160 (2000) ("[I]nformation privacy is a key to building trust among consumers and trust is essential for the promise of e-commerce to be realized.").

8. *See* DANIEL J. SOLOVE, MARC ROTTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (2d ed. 2006).

9. Jared Strauss & Kenneth S. Rogerson, *Policies for Online Privacy in the United States and the European Union*, 19 TELEMATICS AND INFORMATICS 173, 188 (2002) ("Many privacy advocates and legislators have argued that the US Congress should pass legislation requiring businesses to follow fair information practices as has been done in the member states of the European Union.").

10. *See* MARCIA S. SMITH, CONG. RESEARCH SERV., RL 31408, INTERNET PRIVACY: OVERVIEW AND LEGISLATION IN THE 109TH CONGRESS, 1ST SESSION 4, 19 (2006) [hereinafter CRS 2006 INTERNET PRIVACY REPORT] (describing those who advocate for federal legislation and profiling pending online privacy bills).

11. *See id.* at 4 (discussing how advocates believe that legislation is needed to prevent "bad actors" from putting their own interests ahead of their social obligations).

12. *See, e.g.*, Robert E. Litan, *Law and Policy in the Age of the Internet*, 50 DUKE L. J. 1045, 1045 (2001) (arguing that when it comes to regulation of the Internet, "policymakers' first instinct should be to rely on markets and technology to address troublesome issues").

13. Strauss & Rogerson, *supra* note 9, at 179 (discussing those who hold this view); Orson G. Swindle, Comm'r, Fed. Trade Comm'n, Address to the Reston Chamber of Commerce: Regulation of Privacy on the Internet: Where Do You Want to Go Today? (April 8, 1999), *available at* http://www.ftc.gov/speeches/swindle/reston.shtm.

14. Strauss & Rogerson, *supra* note 9, at 181 (discussing those who believe that the online industries, not government regulators, should develop the rules).

es have raised important concerns about these proposed solutions. There are important reasons to question whether either of these approaches can effectively address the Internet privacy problem. Second, it argues that policy makers and scholars should explore an alternative approach known as "co-regulation." Co-regulation encompasses initiatives in which government and industry *share* responsibility for drafting and enforcing regulatory standards.[15] It is neither pure government regulation, nor pure industry self-regulation, but rather a hybrid of the two. Co-regulation is not a new phenomenon and can be found at various places in the regulatory landscape.[16] The question is: Can co-regulation provide a useful alternative strategy for protecting online privacy?

There are reasons to believe that it might. Proponents of co-regulation claim that it provides the flexibility of self-regulation[17] while adding the supervision and rigor of government rules.[18] They see co-regulation as the best of both worlds—an enforceable, rigorous approach that can protect individual privacy while also keeping up with, and meeting the needs of, the growing Internet economy.[19] But co-regulation, too, has its critics. These commentators assert that co-regulation lacks transparency and accountability as compared to traditional notice-and-comment rulemaking.[20] They warn that the backroom discussions in which government and industry negotiate regulatory compliance and "share" rulemaking and enforcement responsibilities will often result in

---

15. HANS-BREDOW-INSTITUT, FINAL REPORT: STUDY ON CO-REGULATION MEASURES IN THE MEDIA SECTOR 17 (2006) [hereinafter BREDOW-INSTITUT REPORT] (defining "co-regulation" as systems that "combin[e] state- and non-state regulation" and contrasting it with self-regulation, which operates "without any state involvement"). American legal and policy scholars often use the term interchangeably with "collaborative governance."

16. *See infra* notes 199–203 and accompanying text.

17. *See, e.g.*, NEIL GUNNINGHAM & DARREN SINCLAIR, LEADERS AND LAGGARDS: NEXT-GENERATION ENVIRONMENTAL REGULATION 104–05 (discussing these potential virtues of negotiated agreements); Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 21–33 (1997) (same). *See generally* JOSEPH REES, REFORMING THE WORKPLACE: A STUDY OF SELF-REGULATION IN OCCUPATIONAL SAFETY (1988).

18. GUNNINGHAM & SINCLAIR, *supra* note 17, at 107–09; Bert-Jaap Koops, Miriam Lips, Sjaak Nouwt, Corien Prins & Maurice Schellekens, *Should Self-Regulation be the Starting Point?*, *in* STARTING POINT FOR ITC REGULATION: DECONSTRUCTING PREVALENT POLICY ONE-LINERS 109, 149 (Bert-Jaap Koops, Corien Prins, Maurice Schellekens & Miriam Lips eds., 2006) (discussing how governments can play an important role in "raising awareness and in enhancing enforcement, so that self-regulatory rules are indeed followed in practice").

19. Strauss & Rogerson, *supra* note 9, at 190 (calling for a blend of legal and self-regulatory mechanisms that could "harness[] the adaptability of self-regulation and the government's enforcement capability"). *Cf.* Koops, et al., *supra* note 18, at 112 ("Co-regulation should combine binding legislative and regulatory action with actions taken by the actors most concerned, drawing on their practical expertise.").

20. Koops, et al., *supra* note 18, at 124 (discussing those who have concerns about self-regulation's lack of procedures for involving the public and the ensuing "lack of transparency").

deals that favor industry and sell short the public interest.[21] Some fear that industry will take advantage of co-regulatory processes to "capture" the agency and co-opt it to industry's point of view.[22] It is too early to tell whether the proponents or the critics have it right. Before making such an assessment, we need to study co-regulation and evaluate how it might function as a means of protecting personal information.[23]

An excellent opportunity to do this analysis recently arose. The European Union's 1995 Data Protection Directive allows E.U. member nations to experiment with a co-regulatory approach to the protection of personal data.[24] During the past decade, many of these nations have implemented such a program.[25] This experience can tell us a great deal about how collaborative governance might work in the realm of Internet privacy.

Under the European co-regulatory approach, each member nation passes a comprehensive data protection statute.[26] The nation then invites representatives from a given regulated sector to draft a "code of conduct" for the industry that embodies the statutory requirements.[27] If the regulatory authority agrees that the code of conduct meets the terms of the statute and approves it, then compliance with the code constitutes compliance with the statute.[28] From that point on, firms can follow a set of rules that their own peers have drafted (subject to government review and approval) and, in so doing, comply with the law. The European model is not self-regulation since the government retains an important role in reviewing, approving, and enforcing the proposed codes of conduct. But neither is it pure government regulation since the industry associations, not the regulators, draft the detailed rules and standards that will govern their members. Instead, it is a form of "co-regulation"[29] in

---

21. GUNNINGHAM & SINCLAIR, *supra* note 17, at 105–06 (citing these concerns).

22. *Id.* at 105 (citing these concerns).

23. One scholar who has begun to engage in this analysis is Ira Rubinstein. *See generally* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes* (N.Y. Univ. Sch. of Law. Pub. Law & Legal Theory Research Paper Series, Working Paper No. 10-16, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275.

24. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31, art. 27(1) (providing that member states should encourage economic sectors to draw up codes of conduct and thus participate in a co-regulatory approach to data protection).

25. *See infra* notes 245–72 and accompanying text (describing the various national laws that implement the code of conduct approach).

26. 1995 O.J. (L281) 31, art. 32(1) (requiring member nations to pass such a statute).

27. *Id.* art 27(1).

28. *Id.* art. 27(2). The relevant industry is also responsible for enforcing the codes of conduct. *See infra* notes 226–44 and accompanying text (describing this process).

29. *See generally* BREDOW-INSTITUT REPORT, *supra* note 15.

that government and industry share responsibility for drafting and enforcing regulatory standards.[30]

How have the European member states gone about implementing this approach? What do the statutes that embody it look like? Have the national programs been a success? Does the European experiment provide support for the proponents of co-regulation? Or does it validate the concerns of the critics? These important questions have received surprisingly little attention in U.S. scholarly literature, and almost none in U.S. law reviews. This Article begins to explore the topic. Focusing on the legal dimension of the E.U. initiative, it examines the provisions of the European Union's 1995 Data Protection Directive that allow member nations to engage in co-regulation.[31] It then provides the first comprehensive analysis in a U.S. law review of the national laws that have implemented this co-regulatory approach.[32] It compares these laws to one another, develops an original way of categorizing and understanding them, and draws lessons about the design of legislation to support co-regulation of online privacy.

The Article is structured as follows: Part II shows that the Internet generates serious new threats to individual privacy. Part III describes in more detail the arguments that critics have leveled against the government regulation and the market/self-regulation approaches and evaluates what experience has to tell us about these models. Part III also provides an introduction to co-regulation and surveys the theoretical literature regarding the strengths and weaknesses of this collaborative approach. Part IV turns to the European experiment with data protection codes of conduct. It analyzes the E.U. and national laws that authorize this initiative. The Article closes in Part V with suggestions for further research about this important area of privacy law and policy.

II. ONLINE THREATS TO INFORMATION PRIVACY

One of the most profound changes in American society in recent decades has been the emergence and exponential growth of the Internet and e-commerce.[33] This change has produced many benefits. But it has also led to an unprecedented increase in the collection, aggregation, and use of personal information, creating new and profound challenges to

30. *See id.* at 17 (defining "co-regulation" as systems that "combin[e] state- and non-state regulation" and contrasting it with self-regulation, which operates "without any state involvement").

31. *See infra* notes 226–44 and accompanying text.

32. *See infra* notes 245–72 and accompanying text.

33. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 1 (2000) [hereinafter FTC MAY 2000 REPORT]. The Internet has grown at an exponential rate. As of 2000, 90 million Americans used the Internet, and 60 million shopped online. *Id.*

information privacy.[34] This Part will describe how Internet businesses collect our personal information online and how they use this information.

A. How Internet Businesses Collect Personal Information Online

1. Search Engines

Most users of the Internet begin by accessing a search engine[35] and entering a search query. The collection of the user's personal information begins here. Search engines collect and store every query that users make.[36] In most cases, they are able to link these queries both to the computer on which they were entered[37] and to the user's individual identity.[38] Search queries are often fairly innocuous, but they can also be highly personal. In 2006, AOL posted on its website a database of 20 million search queries entered by 657,000 users over a three-month period.[39] Among the searches were queries for "60 single men," "foods to avoid when breast feeding," "depression and medical leave," "fear that spouse contemplating cheating," and many thousands of queries related to sex and sexuality.[40] These queries were not atypical. Many users turn to the Internet for information related to their political beliefs, romantic aspirations, medical conditions, sexual preferences or fantasies, intellectual interests, anxieties, and life changes, to name but a few such personal areas. Collectively, these queries provide an intimate picture of the user's daily pursuits and inner life. They constitute a personal "catalog of intentions, curiosity, anxieties and quotidian questions."[41]

---

34. See *id.* at 33 ("While American businesses have always collected some data from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of unprecedented amounts of data that can be used for myriad subsequent purposes. It is the prevalence, ease and relatively low cost of such information collection and use that distinguishes the online environment from more traditional means of commerce and information collection and thereby raises significant consumer privacy concerns.").

35. For example, Google, AOL, or Yahoo!.

36. *In Search of Online Privacy*, INDEPENDENT (United Kingdom), April 9, 2008, at 26, *available at* http://www.independent.co.uk/opinion/leading-articles/leading-article-in-search-of-online-privacy-806284.html.

37. *Id.*; Kang, *supra* note 1, at 1224–25 (user reveals IP address to any server it contacts).

38. FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 4, 12 (2000) [hereinafter, FTC JUNE 2000 REPORT].

39. Michael Barbaro & Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html.

40. *Id.*

41. *Id.*

Search engines store these queries and retain them for months, or even years.[42] They are able to link them to the computer that sent them.[43] Where the user of that computer has registered for one or more services,[44] the search engines are then able to link the queries to the individual person.[45] This gives them the ability, should they choose to use it, to construct a detailed map of a given user's queries and, therefore, of her interests, political views, medical conditions, wishes, and fears.

Wary of privacy concerns, the major search engines claim that they do not link user queries with user identities. Many claim to carefully remove all references to the user's name and identity before they store that person's queries. For example AOL, when constructing the database of queries mentioned above, identified each searcher by an assigned number, rather than by name.[46] But even this practice is an inadequate shield. Journalists who examined the AOL database and reviewed the anonymous searches of one user (user No. 4417749) were able to piece together sufficient information to identify her by name.[47] Thus, search-engine collection and storage of user queries poses a threat to privacy both because the search engines themselves can link an individual to her queries and because third parties who are able to get their hands on the data—even data the search engines try to render anonymous—can often do so as well.

2. Websites

Having entered a query and received search-engine results, the typical user clicks on and enters one or more websites. The great majority of websites collect information about the users who visit them.[48] Some overtly request or require users to fill out registration, survey, or order forms that ask for personally identifying information (PII)[49] such as the

---

42. INDEPENDENT, *supra* note 36.

43. *Id.*; Kang, *supra* note 1, at 1224–25 (user reveals IP address to any server it contacts).

44. For example, free e-mail (e.g., G-mail) or free online storage space.

45. FTC JUNE 2000 REPORT, *supra* note 38, at 4.

46. Barbaro & Zeller, *supra* note 39.

47. *Id.* The individual user, Thelma Arnold, a 62-year-old resident of Lilburn, Georgia, searched for "60 single men," "landscapers in Lilburn, Ga," information on several people with the last name "Arnold," and "homes sold in shadow lake sub-division gwinnett county georgia." Based on these and other searches, the journalists were able to identify her. *Id.*

48. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS iii (1998) [hereinafter, FTC JUNE 1998 REPORT] ("[FTC research] shows that the vast majority of Web sites—upward of 85%—collect personal information from consumers."). *Accord* Schwartz, *Cyberspace*, *supra* note 6, at 1629–31 (describing how and why websites collect personal information).

49. Such information need not contain the user's name in order to qualify as personally identifiable. According to one study, it would be possible to identify 87% of the U.S. population based only on a 5-digit zip code, gender, and date of birth. FED. TRADE COMM'N, FTC STAFF REPORT:

user's name, postal address, e-mail address, driver's license number, or social security number. Other sites collect personal data more subtly through the use of "cookies"[50] and other technologies[51] that unobtrusively track user activities and associate them with a particular computer or device.[52] Through such technologies, website administrators are able to track and record which page a given user visits, how long the user spends there, and how the user engages with that page (e.g. what the user "clicks on").

While this "clickstream" data is anonymous in theory, it is often not so in practice. Many sites collect personally identifying information that they can link to a specific computer or device and also to cookie data associated with that computer.[53] Indeed, in 2000, the Federal Trade Commission (FTC) completed a survey and found that "most" of the sites surveyed were able to do this.[54] Moreover, user profiles have become so comprehensive [55] that it is often possible to infer a user's identity without PII.[56]

SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 24 & n.53 (2009) [hereinafter FTC 2009 STAFF REPORT] (citations omitted).

50. A cookie is a small text file that the website places on the user's hard drive when the user visits the site. *Id.* at 2, n.3. The cookie records data about the user's activity on the site—the pages the user has visited, the content she has viewed, how long she spent at the site, search queries that she entered while at the site, passwords she created, what she put in her "shopping cart," etc. *Id.* The next time the user visits the website, the cookie communicates this data to the site. This allows the site to recognize the individual consumer and tailor the Web experience to her (e.g., to remember what was in her "shopping cart"). *Id.* at 2. Over time, the site owner is able to build up a picture of the particular user and how she has utilized the site. *See id.* at 22; FTC JUNE 2000 REPORT, *supra* note 38, at 4. Though the user can disable cookies, few consumers seem to know about or take advantage of this opportunity and, even when they do, they may inadvertently undo this choice. *See* PAM DIXON, WORLD PRIVACY FORUM, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION 14–17 (2007) (describing these problems with consumer opt-out); *Privacy Policy*, GOOGLE.COM (Oct. 3, 2010), http://www.google.com/intl/en_us/privacypolicy.html.

51. *See* FTC 2009 STAFF REPORT, *supra* note 49 at 2 & n.3 (citing "web bugs," "web beacons," and "flash cookies").

52. *Id.* at 2.

53. *Id.* at 2 & n.4.

54. "Most of the sites surveyed, therefore, are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior information they collect to personally identifying information." FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 10 (2000) [hereinafter, FTC MAY 2000 REPORT]. *See also* FTC JUNE 1998 REPORT, *supra* note 48, at 25.

55. *See infra* notes 50–56 and accompanying text (describing how network advertisers combine cookie data from many different websites into a single, highly detailed user profile).

56. FTC 2009 STAFF REPORT, *supra* note 49, at 22–23 ("[W]hen combined, such information would constitute a highly detailed and sensitive profile that is potentially traceable to the consumer. The storage of such data also creates the risk that it could fall into the wrong hands or be used later in combination with even richer, more sensitive, data."); FTC JUNE 1998 REPORT, *supra* note 48, at 12 (According to commentators at an FTC workshop, "the comprehensive nature of the profiles and the technology used to create them make it reasonably easy to associate previously anonymous pro-

3. The Future: Internet Service Providers

If current trends are any indication, we may find our personal information collected without us even having to enter a query or visit a website. ISPs—Microsoft, AOL, and others—are beginning to experiment with "deep packet inspection."[57] This practice allows the ISP to automatically inspect the contents of data "packets" as they travel on the Internet in order to mine personal information from them.[58] These packets could contain relatively innocuous data like queries or websites; however, they could also easily contain e-mails or documents.[59] If widely adopted, deep packet inspection promises a whole new dimension to the problem of online privacy that will render it even more intense.

B. Who Uses Personal Information Collected Online?

Having introduced those who collect the most information online, we now turn to those who use this data. These include websites, network advertisers, data brokers, secondary users, and the government.

1. Websites

Websites use cookie data to improve users' experiences at the site. For example, a website will remember a username and password entered during a prior visit to the site, reconstitute the contents of a shopping cart on a return visit,[60] or provide personalized news and weather or stock quotes.[61] Many sites also use the information from past visits to predict which services or products are most likely to appeal to the user and to present the user with advertisements promoting those items.[62]

2. Network Advertisers

The principal users of online personal data, however, are "network advertisers."[63] Network advertisers are responsible for the banner advertisements that users see when they visit a website. Network advertisers enter into contractual relationships with many different websites: in ex-

---

files with particular individuals. This means that anyone who obtains access to ostensibly anonymous data—either by purchasing the data or hacking into it—might be able to mine the data and link it to identifiable individuals.").

57. *See generally* Samir Jain, *The Promise and Perils of Deep Packet Inspection*, 8 PRIVACY & SECURITY L. REP. 217.

58. *Id.*

59. *Id.*

60. FTC JUNE 2000 REPORT, *supra* note 38, at 8–9.

61. *Id.* at 9.

62. This is known as "first party" advertising since the same website is both collecting the data and conveying the ad. FTC 2009 STAFF REPORT, *supra* note 49, at iii, 26.

63. *See generally* FTC JUNE 2000 REPORT, *supra* note 38, at 2–3.

change for payment, the websites provide the network advertiser with user clickstream data and allow the advertiser to display advertisements on their site.[64] These arrangements allow a single network advertiser to collect user information from hundreds or thousands of different websites, and to see what a given user has done at each of these sites.[65]

The network advertiser combines this information with other information that it has purchased about the user. This includes search-query data, data that the user has provided through surveys and registration forms, and data collected by third-party sources regarding the user's off-line purchases and activities.[66] The result is a highly comprehensive and fine-grained "behavioral profile" of the user that can include hundreds of data fields—everything from the user's brand of toothpaste to medical conditions, preferred travel destinations, political commitments, intellectual interests, and sexual preferences or fantasies.[67] Moreover, it is often possible for the network advertiser to tie the profile to an identified user, either because the user at one point provided a name or other PII when filling out a survey or registration form or making a credit card purchase, or because the profile is sufficiently detailed to allow the advertiser (or another who has obtained the data) to infer the user's identity without PII.[68]

Network advertisers employ behavioral profiles to make inferences about the user's "tastes, needs and purchasing habits" and then select specific banner ads to show to that user.[69] They deliver these ads in conjunction with the networked websites. When a user visits such a site, the site automatically contacts the network advertiser and requests advertising content.[70] The advertiser searches its database of information on the specific user, chooses an ad or ads to present to him, and provides this to the site.[71] When the webpage arrives at the user's computer screen, it contains not only the requested content, but also the targeted ads. This happens so fast that the user does not notice it but accepts the ads as part of the requested webpage.[72] In 2000, the FTC estimated that network

---

64. KATHLEEN ANN RUANE, CONG. RESEARCH SERV., RL 34693, PRIVACY LAW AND ONLINE ADVERTISING: LEGAL ANALYSIS OF DATA GATHERING BY ONLINE ADVERTISERS SUCH AS DOUBLE CLICK AND NEBUAD 1–2 (2008).

65. FTC 2009 STAFF REPORT, *supra* note 49, at 3 & n.5.

66. FTC JUNE 2000 REPORT, *supra* note 38, at 5.

67. *See id.* at 5–6.

68. FTC MAY 2000 REPORT, *supra* note 54, at 9 & n.53; FTC 2009 STAFF REPORT, *supra* note 49, at 2 & n.4.

69. FTC JUNE 2000 REPORT, *supra* note 38, at 5.

70. FTC 2009 STAFF REPORT, *supra* note 49, at 3.

71. *Id.*

72. An example may help to illustrate the phenomenon. Assume that a user visits the website of the Washington Post, a network member, and reads an article about the Washington Nationals

advertisers had served tens of billions of banner ads to users.[73] That number has increased substantially over the past decade.[74]

This practice has its benefits. It makes it more likely that people will receive ads about goods and services they may actually be interested in,[75] saving them from having to wade through ads that hold no interest for them. It also makes businesses' advertising efforts far more efficient.[76] On the other hand, network advertisers have the ability to create "behavioral profiles" that chronicle our desires, anxieties, and beliefs and that are traceable directly to us.[77] This creates "a portrait that is quite comprehensive and, to many, inherently intrusive."[78] In this respect, network advertising significantly damages the privacy of Internet users.[79]

3. Data Brokers

Websites and network advertisers sometimes sell personal information that they have collected to data brokers.[80] Data brokers specialize in pulling together and analyzing personal information gleaned from many

---

baseball team. The Post's server places a third-party cookie on the user's browser that conveys the user's activity to the network advertiser. Next, the same user visits a travel website, also a network member, to search for flights from Washington, D.C. to New York. The travel company's server also places a third-party cookie and so conveys the user's activity to the advertiser. Finally, the user visits the website of the local television news station—also a network member—in order to check the next day's weather. The station's Web server sends a request to the network advertiser for a banner advertisement. Putting together the user's possible travel to New York City with his interest in baseball, the advertiser serves up a banner ad for tickets to New York Yankees baseball games at the new Yankee Stadium. This arrives as a seamless part of the news station's webpage displayed along with information about the next day's weather. *See id.* (minor changes made to the FTC's example).

73. FTC JUNE 2000 REPORT, *supra* note 38, at 2–3.

74. Indeed, between 2002 and 2006 online advertising revenue nearly tripled, growing from $6 billion to $16.6 billion. FTC 2009 STAFF REPORT, *supra* note 49, at 8; Ryan Blitstein, *Microsoft, Google, Yahoo in Online Ad War*, SAN JOSE MERCURY NEWS, May 19, 2007.

75. FTC JUNE 2000 REPORT, *supra* note 38, at 9; FTC 2009 STAFF REPORT, *supra* note 49, at i.

76. FTC JUNE 2000 REPORT, *supra* note 38, at 9.

77. The future looks even bleaker. As mentioned above, the most recent trend does not even depend on website cookies. Instead, ISPs like Microsoft and AOL are beginning to collect clickstream data by analyzing the packets of information that a given user sends and receives on the Internet. *See* FTC 2009 STAFF REPORT, *supra* note 49, at 16 & n.40. This process, known as "deep packet inspection," encompasses *all* of a given user's Web activity, not just that which is conducted on the advertiser's network of sites. *Id.*; Samir Jain, *supra* note 57, at 217–20. It promises to yield behavioral profiles that are even more comprehensive and invasive. *See* FTC 2009 STAFF REPORT, *supra* note 49, at 16 & n.40; Samir Jain, *supra* note 57, at 217–20.

78. FTC JUNE 2000 REPORT, *supra* note 38, at 12.

79. In addition, it can be argued that the very targeted marketing for which the data is collected is itself harmful to individual privacy. By using our past behavior as a basis for selecting the ads we will see, online behavioral marketing tends to keep us on the same path that we are on. It presents us with fewer choices and influences and so may produce more "path dependence" in our growth and development.

80. *See* FTC JUNE 2000 REPORT, *supra* note 38, at 16 (citations omitted).

different sources, including public records, the media, credit-reporting agencies, and other sources.[81] Increasingly, data brokers have been combining this off-line data, traceable to specific individuals, with online data that they can match to those same individuals.[82] This aggregation of data makes the individual profiles—the picture that emerges when all of this data about a given person is put together—even more comprehensive and detailed. Moreover, the existence of detailed computer profiles creates the possibility that someone will hack into them, thereby increasing the threat of identity theft and fraud.[83]

4. Secondary Users

Websites and network advertisers use the information they collect in order to better serve and better market to Internet users. But do they also sell it to others, and if so, what do these other parties do with it? Do they use it to decide who they will hire, or provide with insurance or a loan? Little is known about these "secondary uses" of the personal information that Web-based companies collect on the Internet. Recently, the FTC surveyed websites regarding their collection and use of personal information. The survey asked about these "secondary" uses by entities other than the one that collects it.[84] The websites were quite forthcoming about their own collection and use of the data; however, they provided almost no information about secondary uses.[85] This silence is deafening. As the FTC itself has said, it is hard to believe that no one is making secondary use of this information.[86]

Preliminary information suggests that secondary uses are a cause for concern. Some businesses may be using the information to engage in "Weblining"—the practice of charging higher prices to some consumers based on their online profiles.[87] For example, life insurance companies may be using the information to decide how to price policies for specific individuals, or even whether to offer them a policy at all.[88] This practice is extremely invasive, especially where the information in question involves medical conditions. Similarly, lenders may be using personal in-

---

81. Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 301 (2003); *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1151 (2002).

82. *See* FTC JUNE 2000 REPORT, *supra* note 38, at 16 (citations omitted).

83. *Id.* at 12.

84. *Id.* at 13 (citations omitted).

85. *Id.*

86. Instead, the websites must be unwilling to disclose such uses because they fear that they would alarm the regulators and the public. Proponents of protecting privacy and personal information should be keen to learn more about this practice.

87. FTC JUNE 2000 REPORT, *supra* note 38, at 13 (citations omitted).

88. *Id.*

formation to decide whether to offer loans to specific individuals and how to price them.[89] Given the history of racially discriminatory "redlining" in this country, the prospect of Weblining in the real-estate market should be a cause for concern.

Employers may also be using the information to help them decide who to interview and hire.[90] This potential secondary use is particularly vexing. People may reveal information online regarding their shopping and spending habits, political interests, sexual orientation, marital status, or medical conditions. Employers may find this information to be very valuable when choosing future employees; however, few employers would ask for such personal information directly and most of us, if asked, would find such questions highly invasive for any job not requiring a high security clearance. Online data collection can allow employers to access this information without the applicant's knowledge. This access creates a serious invasion of personal privacy.

5. The Government

The most significant privacy issue, however, is the possibility of online companies sharing user information with the government. In some instances, government officials have requested that ISPs provide—or have even issued subpoenas for—the identity behind an e-mail or Internet Protocol address.[91] In other cases, government officials have subpoenaed information about users' Internet queries and Web travels.[92] Suspected criminals, or even citizens whose only sin is to oppose the views of those in power, could find their daily activities monitored to an extent beyond what even a wiretap on their phone would reveal—and all without the issuance of a warrant. This is an unwelcome prospect in a democracy.

III. GOVERNMENT REGULATION, MARKET REGULATION, AND SELF-REGULATION

The practices described above have convinced many that the online environment poses a meaningful threat to individual privacy. But there

89. *Id.* at 13 & n.45.

90. *See, e.g.*, Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 481, 487 (1995) (health information used inappropriately for employment decisions).

91. *See* Peter Shinkle, *65.227.106.78: This Internet Footprint Led to Suspected Killer*, ST. LOUIS POST-DISPATCH, June 16, 2002, at A1 (providing example of this).

92. *See* Arshad Mohammed, *Google Argues Against Subpoena: Turning Over Data Would Hurt Firm, Not Help U.S., Lawyers Say*, WASH. POST, Feb. 18, 2006, at D03 (discussing government subpoenas against various ISPs seeking search query data).

is far less consensus on how to deal with this problem. In the United States there are two main camps: those who favor detailed government regulation and those who prefer market and industry self-regulation.[93] Co-regulation offers a third alternative. In order to understand the role that co-regulation might play, it is important first to examine the two dominant views that frame the current debate.

A. Government Regulation

Proponents of government regulation argue that the desire for profits, coupled with the economic value of personal information, will inevitably lead private firms to collect a great deal of personal information online.[94] They assert that the legislature should take steps to protect Internet privacy as an important societal value; for instance, they call for legislation that would set specific limits on the online collection of personal information and on the distribution and use of that information.[95] Following the typical American regulatory model, this law would take shape through two stages. First, Congress would pass a sweeping and rigorous statute. Then, a regulatory agency such as the FTC would develop detailed regulations implementing this legal framework.

Federal legislators have introduced several such bills in the House and Senate, but neither chamber has come close to passing any of them.[96] Some of the bills provided for broad regulation of the Internet sector.[97] Others focused more narrowly on websites and network advertising.[98] On May 4, 2010, Representatives Boucher (D-Va.) and Stearns (R-Fla.) released a "Staff Discussion Draft" of a bill of the latter type.[99] The bill

---

93. *See supra* notes 9–14 and accompanying text. *Cf.* CRS 2006 INTERNET PRIVACY REPORT, *supra* note 10, at i ("The debate over website information policies concerns whether industry self regulation or legislation is the best approach to protecting consumer privacy.").

94. COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 134 (2003).

95. CRS 2006 INTERNET PRIVACY REPORT, *supra* note 10, at 4, 9.

96. *See* MARCIA S. SMITH, CONG. RESEARCH SERV., RL 31408, INTERNET PRIVACY: OVERVIEW AND PENDING LEGISLATION 4 (2004) [hereinafter CRS 2004 INTERNET PRIVACY REPORT] ("[M]any Internet privacy bills were considered, but did not clear, the 107th Congress"); CRS 2006 INTERNET PRIVACY REPORT, *supra* note 10, at 5, 18 (describing Internet privacy bills in the 109th Congress and concluding that while some such bills were introduced in the House and Senate, none have passed).

97. *See, e.g.* Online Privacy Protection Act of 2005, H.R. 84, 109th Cong. (2006) (covers all collection of personal information not already covered by the Children's Online Privacy Protection Act).

98. Act of May 3, 2010 (Discussion Draft 2010), *available at* http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf.

99. Press Release, Office of Rep. Boucher, Boucher, Stearns Release Discussion Draft of Privacy Legislation: Measure Confers Privacy Rights on Internet Users (May 4, 2010), *available at* http://www.boucher.house.gov/index.php?option=com_content&view=article&id=1957:boucher-

would require websites and network advertisers, among others, to provide users with "clear and conspicuous" notice of how they collect, use, store, and share users' personal information.[100] It would mandate that they provide users with meaningful choices about whether to allow these practices.[101] Moreover, it would require affirmative consent before collecting or using "sensitive information" (e.g., information relating to medical conditions, finances, race, sexual orientation, or precise location)[102] or sharing any personal information with unaffiliated third parties.[103] Finally, the bill would require websites and network advertisers to take reasonable and appropriate steps to ensure the accuracy and security of personal data that they collect and use.[104]

Like traditional government regulation, the bill would delegate to an agency (here the FTC) the authority to "issue such regulations as it determines to be necessary"[105] to carry out the bill's provisions and the power to issue penalties for violations.[106] It would further give state attorneys general the authority to bring civil enforcement actions on behalf of the citizens of their states.[107] Were Congress to enact it and the FTC to issue implementing regulations, the bill would likely constitute precisely the kind of detailed government regulation that proponents of this approach advocate.

Within days of the bill's introduction, industry and pro-market groups expressed opposition to the Boucher–Stearns bill. Some maintained that the bill would impose excessive costs on Internet-based businesses that are still trying to recover from the 2008 recession.[108] Others went further, complaining that "by mandating a hodge-podge of restrictive regulatory defaults, policymakers could unintentionally devastate the 'free' Internet as we know it, . . . raise prices, [and] quash digital innovation."[109] Still others claimed that the bill reflected a mistaken belief that "Congress and regulators . . . thought they knew how to deliver privacy

---

stearns-release-discussion-draft-of-privacy-legislation-may-4-2010&catid=33:2010-press-releases&Itemid=41.

100. Act of May 3, 2010 § 3(a)(2)(A)(i)(I).

101. *Id.* § 3(a)(1)(B), (a)(3).

102. *Id.* §§ 2(10) (defining "sensitive information"), 3(c) (requiring opt-in consent).

103. *Id.* § 3(b)(1).

104. *Id.* § 4(a), (b).

105. *Id.* § 8(a)(3).

106. *Id.* § 8(a)(1),(2).

107. *Id.* § 5(b).

108. Mathew Ingram, *Congress Proposes Sweeping Internet Privacy Bill*, GIGAOM (May 4, 2010), http://gigaom.com/2010/05/04/congress-proposes-sweeping-internet-privacy-bill.

109. News Release, The Progress and Freedom Foundation, PFF Statement on House Privacy Bill Discussion Draft: Szoka & Thierer Fear "Privacy Industrial Policy" Will Devastate Digital Economy (May 4, 2010), *available at* http://www.pff.org/news/news/2010/2010-05-04-Privacy_Bill.html.

better than markets. We know they don't, but they still think they do."[110] The Boucher–Stearns bill, like the legislative proposals that preceded it, will face an uphill battle in becoming law.[111]

The reactions to the Boucher–Stearns bill reflect many of the themes that opponents of government regulation have voiced for years. Critics emphasize the importance of the Internet to the future of the U.S. economy and express concern that legislation would impose burdensome costs on this sector.[112] They assert that government officials, who know little about the industries they regulate, will impose impractical requirements that will seriously undermine business competitiveness.[113] Critics also highlight the fast-changing nature of Internet technologies and business models, arguing that the government regulators who implement the legislation will not be able to keep pace with these changes[114] and that the rules they create will quickly become out of date and ill-suited to their intended purpose.[115] Judging by the legislature's failure to pass into law any of the various Internet privacy bills it has considered in recent years, these arguments have had a strong impact.[116]

---

110. Declan McCullagh, *House Privacy Bill Draws Fire from All Sides*, CNET NEWS, May 5, 2010, http://news.cnet.com/8301-13578_3-20004165-38.html (quoting Jim Harper, Director of Information Policy Studies at the Cato Institute).

111. Ingram, *supra* note 108 ("[Rep. Boucher has] been meeting with both industry groups such as the Interactive Advertising Bureau and privacy advocates trying to come up with a solution that satisfies both sides. But it doesn't appear that such a goal is even possible."). Even Rep. Stearns said publicly that he did not agree with everything in the bill—an unusual statement for the sponsor of a bill to make. McCullagh, *supra* note 110.

112. *See* Koops, et al., *supra* note 18, at 109 (The source discusses those who "complain . . . about the lack of flexibility in legislation and are skeptical about the feasibility of efficient and adequate ICT regulation by means of legislation."). *See generally* Keith Perine, *The Persuader*, INDUSTRY STANDARD, (Nov. 13, 2000), *available at* http://findarticles.com/p/articles/mi_m0HWW/is_47_3/ai_66932989/?tag=content;col1 (discussing this criticism).

113. Strauss & Rogerson, *supra* note 9, at 188 ("[C]ritics maintain that government action creates burdensome, inflexible regulation and that self-regulation remains the best solution to privacy problems . . . .").

114. *See id.* at 181 (discussing those who believe that the "fast-changing" nature of the Internet makes it ill-suited to government regulation).

115. For example, a statute requiring firms to post large and eye-catching notices about their data collection practices, designed for delivery to computer screens, will not fit on the mobile phone screens through which more and more people now access the Internet. Such rules will seriously constrain innovation or become obsolete as technologies and business practices change.

116. *See* CRS 2006 INTERNET PRIVACY REPORT, *supra* note 10, at 18 (describing Internet privacy bills introduced in the 109th Congress and concluding that while some such bills were introduced in the House and Senate, none have passed); CRS 2004 INTERNET PRIVACY REPORT, *supra* note 96, at 4 (concluding that "many Internet privacy bills were considered by, but did not clear, the 107th Congress").

B. The Market and Self-Regulation

Critics of government regulation often argue that the market, either alone or in combination with industry self-regulation, will do a better job of protecting personal information.

1. Leave it to the Market

Those who favor a market solution argue that individual Internet businesses will enhance their competitive positions by responding to customer preferences for greater privacy, thereby leading to a more privacy-friendly Web.[117] According to this logic, if customers are not currently requiring websites and other Web-based firms to protect user privacy it means they value the services they are receiving more than the privacy they are losing. Proponents of the market solution contend that the market, left to its own devices, will arrive at the optimal level of privacy protection, whereas government regulation will distort this outcome.[118]

Those who object to a market solution focus on information asymmetries.[119] Web users are often unaware of the collection of their personal information online, as much of it occurs instantaneously and invisibly.[120] Even where they are aware of the collection of personal data, users often do not understand how network advertisers and data brokers will combine this information with other data about them; how employers, lenders, and others will use these profiles; and how data mining operations can infer additional, latent information from such data. This information gap prevents users from expressing their true preferences for privacy protection and so can prevent the market from responding appropriately. Because the market for online privacy is characterized by highly imperfect and asymmetrical information, firms can collect and use far more personal data than they could in a hypothetical perfect market.

Other critics focus on actual market experience. They reason that, if the laissez-faire theory were correct, the market would provide meaningful privacy protections; because the empirical data unfortunately suggests otherwise, a market system must be ineffective. The Fair Information Practice Principles (FIPPs), first developed by the Department of Health, Education, and Welfare in 1973,[121] are an internationally ac-

---

117. Strauss & Rogerson, *supra* note 9, at 19 (discussing those who hold this view); Swindle, *supra* note 13.

118. Strauss & Rogerson, *supra* note 9, at 19; Swindle, *supra* note 13.

119. Strauss & Rogerson, *supra* note 9, at 179 (discussing this criticism).

120. FTC JUNE 2000 REPORT, *supra* note 38, at 11; Schwartz, *Cyberspace*, *supra* note 6, at 1621–22.

121. U.S. DEP'T. OF HEALTH, EDUC. & WELFARE, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS 41–42 (1973).

cepted standard for what constitutes adequate privacy protection.[122] They require those who collect and use personal information to provide the following:

> (1) Notice—data collectors must disclose their information practices before collecting personal information from consumers; (2) Choice—consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided; (3) Access—consumers should be able to view and contest the accuracy and completeness of data collected about them; and (4) Security—data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.[123]

Not surprisingly, these criteria correspond to some of the essential preconditions that must be met before users can make informed market choices.[124]

In 2000, the FTC surveyed the busiest U.S. commercial websites in order "to assess industry's progress in protecting consumer privacy online."[125] The results showed the percentage of websites that collected personally identifying information and the percentage that provided privacy disclosures to their users.[126] For those sites that provided a disclosure (often in the form of a privacy policy), the FTC assessed how the site's privacy policy compared with the FIPPs. The FTC found that, while the great majority of the busiest websites collected personal information,[127] nearly forty percent posted no privacy policy.[128] Of those that did post a policy, the majority did not meet the minimum standards set

---

122. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get),* 2001 STAN. TECH. L. REV. 1, 44 (2001) (explaining how the Fair Information Practices influenced the Organization of Economic Cooperation and Development's privacy guidelines).

123. FTC MAY 2000 REPORT, *supra* note 33, at 4.

124. Strauss & Rogerson, *supra* note 9, at 181 ("[E]nforcing fair information practices is the best way to harness market forces, because these practices ensure that consumers have the full information needed to make informed choices.").

125. FTC MAY 2000 REPORT, *supra* note 33, at 7.

126. *Id.* at 9–11.

127. The Commission found that 97% of the sites collect an e-mail address or some other type of personal identifying information. *Id.* at 9. A widely cited Georgetown University study confirms these results, finding that, in 1999, only 10% of sites provided disclosures that touch on all four fair information practice principles. *See generally* MARY CULNAN, GEORGETOWN INTERNET PRIVACY POLICY SURVEY: REPORT TO THE FEDERAL TRADE COMMISSION (1999). Moreover, there is a 99% chance that a user surfing the busiest websites will, over the course of a one-month period, visit a site that collects personally identifying information. FTC MAY 2000 REPORT, *supra* note 33, at 9.

128. FTC MAY 2000 REPORT, *supra* note 33, at 10.

out in the FIPPs.[129] Probing further, the FTC evaluated the content of the privacy policies and found that many used contradictory language,[130] buried exceptions deep in the fine print,[131] provided ambiguous or misleading statements about how the site handled user "choice,"[132] and reserved the right to change policies without notice.[133] No one has updated the FTC's 2000 report. More recent assessments suggest, however, that while more websites now post privacy policies, these documents remain inaccessible and hard to understand.[134] Given the high profits associated with the collection, use, and sale of personal information, in addition to the transaction costs and information asymmetries that distort the market, these findings are not surprising.[135]

2. Self-Regulation

Some who favor the market approach recognize that market imperfections are possible and accept that some type of collective regulation may be necessary. They assert, however, that industry self-regulation, rather than direct government regulation, is the best way to achieve this.[136] Self-regulation, for the purposes of this discussion, is a regulato-

---

129. Only one in five implemented all four information practices to some degree. *Id.* at 35. Only 41% met the notice and choice standards. *Id.*

130. *Id.* at 24.

131. *Id.* at 25. It is difficult for users to read through these lengthy documents, especially if they are visiting multiple websites in rapid succession, and few take the time to do so. *See* CTR. FOR DEMOCRACY AND TECH., RESPONSE TO THE 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT FOR ONLINE BEHAVIORAL ADVERTISING 4 (2008). *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & POL'Y FOR INFO. SOC'Y 543 (2008).

132. FTC MAY 2000 REPORT, *supra* note 33, at 26.

133. *Id.*

134. ALESSANDRO ACQUISTI, JANICE TSAI, SERGE EGELMAN & LORRIE CRANOR, THE EFFECT OF ONLINE PRIVACY INFORMATION ON PURCHASING BEHAVIOR: AN EXPERIMENTAL STUDY 1 (2007) (noting that recent literature concludes that many privacy policies are inaccessible and hard to understand).

135. Could it be that Web users really do not value protection of their personal information, and that is why the websites are not providing it? Studies of user preferences suggest not. In a *Business Week* survey, 89% of users expressed discomfort with the idea that their personal identity could be linked to their Web-browsing and shopping patterns. FTC JUNE 2000 REPORT, *supra* note 38, at 14–15 (internal citations omitted). 63% expressed discomfort even if their profiles were not linked to their name or identity. *Id.* at 15. *See also* FTC 2009 STAFF REPORT, *supra* note 49, at 24 & n.52. According to other reputable surveys, 92% of respondents were uncomfortable with the idea that websites would share their information with others, and 93% expressed discomfort with the notion that websites would sell this information. FTC JUNE 2000 REPORT, *supra* note 38, at 16.

136. *See* CRS 2006 INTERNET PRIVACY REPORT, *supra* note 10, at 3–4 (describing advocates of self-regulation); Strauss & Rogerson, *supra* note 9, at 181 ("[T]he federal government, industry members, and private associations have touted self-regulation as the answer to privacy concerns.").

ry system in which business representatives define and enforce standards for their sector with little or no government involvement.[137]

Proponents of self-regulation argue that this method will institute protective standards while avoiding the pitfalls of government legislation.[138] They point out that industry members know their operations and business plans better than anyone else and therefore are uniquely positioned to identify the most effective and efficient means of protecting public values such as privacy.[139] Self-regulation will reduce the costs and burdens associated with online privacy regulation while focusing regulation on those areas where it will count the most. In a similar vein, proponents contend that industry members are better able to predict future technologies and business developments and design standards that can accommodate changes.[140] Thus, self-regulation will remain more relevant and workable than government-imposed standards. Finally, proponents contend that industry members will be more likely to accept rules designed and imposed by their peers. Industry will comply more readily with such rules and will spend less time and energy resisting them.

This rosy picture may be overly optimistic.[141] Critics of self-regulation have advanced several arguments against this approach. First, they argue that firms will put their own profits ahead of the public interest. As a result, self-regulatory standards will inevitably prove too lenient.[142] Second, critics question whether industry representatives, who do not hold governmental power to fine or otherwise penalize scofflaws, will possess sufficient power or incentive to enforce industry standards against their peers.[143] Third, critics assert that self-regulatory processes are lacking in transparency compared to traditional rulemaking, meaning the public interest will not be adequately represented.[144] Finally, these critics worry that without sanctions for those who do not participate,

---

137. *See* GUNNINGHAM & SINCLAIR, *supra* note 17, at 97 (discussing "unilateral commitments" in which "both the targets and determinations of how they are to be met and monitored [are] at the discretion of the enterprises or associations themselves"); REES, *supra* note 17, at 9 (describing how in self-regulation "rulemaking and enforcement are both carried out privately"); Koops, et al., *supra* note 18, at 109 ("[S]elf-regulation implies that private actors themselves implement the applicable norms and rules and, ideally, monitor compliance and enforce the rules in the case of non-compliance.").

138. Strauss & Rogerson, *supra* note 9, at 181.

139. *See generally* Koops, et al., *supra* note 18.

140. *Id.*

141. *See generally* CHRIS JAY HOOFNAGLE, ELEC. PRIVACY INFO. CTR., PRIVACY SELF-REGULATION: A DECADE OF DISAPPOINTMENT (2005).

142. BENNETT & RAAB, *supra* note 94, at 134.

143. Strauss & Rogerson, *supra* note 9, at 183. *See generally* Koops, et al., *supra* note 18.

144. *See generally* Koops, et al., *supra* note 18.

many firms will stand by while their competitors institute costly, self-regulatory standards, then free ride on the sector's improved reputation for protecting privacy.[145] Unsurprisingly, many of these critics call for government legislation instead of self-regulation.[146]

Self-regulation of Internet privacy is not just a matter of theory. It has been in practice since the 1990s. For the better part of the past two decades, the federal government has embraced self-regulation as the means to protect Internet privacy.[147] In 1997, the Clinton Administration declared that "[f]or electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation wherever appropriate . . . ."[148] The FTC, the agency with the greatest role in privacy regulation, has also favored self-regulation. For example, in the late 1990s, the Commission stated that "self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology"[149] and that "the Commission's goal has been to encourage and facilitate effective self-regulation . . . ."[150] Following a brief period during which the FTC appeared to lose faith in industry efforts and began to call for legislation,[151] the Commission returned to its endorsement of self-regulation.[152] Industry members responded by launching two initiatives to govern privacy on the Internet, demonstrating how self-regulation of online privacy has worked in practice. The results were not encouraging.

a. The Online Privacy Alliance

In 1998, the FTC demanded industry self-regulation of online privacy and threatened that, if it was not forthcoming, the government

145. *See* GUNNINGHAM & SINCLAIR, *supra* note 17, at 107.

146. *See* CRS 2006 INTERNET PRIVACY REPORT, *supra* note 10, at 4 (describing those who "believe self regulation is insufficient" and instead call for legislation).

147. *See* CRS 2004 INTERNET PRIVACY REPORT, *supra* note 96, at 1 ("[M]any in Congress and in the Clinton Administration preferred industry self regulation.").

148. Memorandum on Electronic Commerce, 2 Pub. Papers 898 (July 1, 1997).

149. FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (1999).

150. FTC JUNE 1998 REPORT, *supra* note 48, at i.

151. FTC MAY 2000 REPORT, *supra* note 33, at 36.

152. For example, in 2009, it responded to growing controversy over online behavioral marketing by issuing a set of "Self-Regulatory Principles" to guide industry efforts in this area and by "call[ing] upon [the online behavioral advertising] industry to redouble its efforts in developing self-regulatory programs." FTC 2009 STAFF REPORT, *supra* note 49, at 47. This report omitted any mention of the need for federal legislation.

would move towards direct regulation.[153] The Online Privacy Alliance (OPA), a group formed in the mid-1990s and consisting of leading Internet firms,[154] responded by issuing Guidelines for Online Privacy Policies.[155] The Guidelines required all OPA members to implement a privacy policy that would provide users with basic notice about online collection and use of personal data, allow users to "opt-out" of those uses and to correct inaccurate data, and institute measures to assure data security and reliability.[156]

The Guidelines failed. They did not prohibit the collection of sensitive data or protect against harmful uses of data by any means other than an "opt-out" policy.[157] Pointing to the inadequacy of such a provision, privacy expert Bob Gellman complained, "[I]t can't be a case that if a customer doesn't object, you can do anything."[158] The OPA also failed to identify a process for enforcing the Guidelines against members that did not follow them.[159] Finally, and most significantly, the OPA proved unable to recruit and retain a critical mass of key industry players. Only 100 or so companies ultimately joined the group, with significant firms such as Amazon.com and Lycos choosing not to participate at all.[160] With such limited participation, the OPA could hardly claim that it was creating an Internet environment in which privacy was protected. After a couple of years, the OPA itself admitted that its self-regulatory approach had "come up short" and began to support online privacy legislation.[161] The OPA has since ceased to exist.

b. The Network Advertising Initiative

The second self-regulatory initiative, the Network Advertising Initiative (NAI), followed soon thereafter. The NAI, an organization of

153. Brian McWilliams, *Alliance Aims to Beat FTC to the Online-Privacy Punch*, CNN.COM (July 23, 1998), http://articles.cnn.com/1998-07-23/tech/9807_23_webprivacy.idg_1_privacy-seal-privacy-policies-online-privacy-alliance?_s=PM:TECH.

154. AOL, IBM, Hewlett-Packard, and others founded OPA in the mid-1990s to "lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce." *Frequently Asked Questions*, ONLINE PRIVACY ALLIANCE, http://www.privacyalliance.org/facts/ (last visited Oct. 21, 2010).

155. *Guidelines for Online Privacy Policies*, ONLINE PRIVACY ALLIANCE, http://www.privacyalliance.org/resources/ppguidelines.shtml (last visited Oct. 21, 2010).

156. *Id.*

157. *Id.*

158. Ashley Craddock, *Pretty Poor Privacy*, WIRED, June 06, 1998, *available at* http://www.wired.com/politics/law/news/1998/06/13256.

159. *Id.*

160. *See generally* Perine, *supra* note 112.

161. *Id.*

Internet firms, required members to uphold certain privacy principles.[162] But rather than seek to include a broad array of companies as the OPA had done, the NAI focused exclusively on the network advertising industry.[163]

The NAI owes its beginnings both to the failure of the OPA and to the controversy that erupted when a proposed merger created an unprecedented threat to online privacy. DoubleClick Inc., the nation's leading network advertising firm, announced plans to merge with Abacus Direct Corporation, the owner of a database of magazine and catalog purchasing records covering over 80 million households.[164] This plan to join online and off-line data, and link the data to specific, named individuals,[165] provoked protest[166] as well as investigations by the FTC and the Michigan attorney general's office.[167] Shortly thereafter, the Network Advertising Initiative came into existence and announced a set of "Self-Regulatory Principles for Online Preference Marketing By Network Advertisers."[168]

As might be expected, the 2000 NAI principles focused on the merger of non-personally identifiable information (Non-PII), such as the clickstream data that network advertisers like Doubleclick collect, and personally identifiable information (PII), such as the off-line purchasing data that Abacus Direct had collected. The principles drew a line between clickstream data collected prior to the publication of the principles and data collected after publication. They required network advertising firms to get specific consent ("opt-in" consent) before combining pre-publication clickstream data with PII[169] but mandated only that the firms

---

162. *See A Track Record of Success*, NETWORK ADVER. INITIATIVE, http://www.networkadvertising.org/about/history.asp (last visited Oct. 23, 2010) (describing NAI Principles); *see also Participating Networks*, NETWORK ADVER. INITIATIVE, http://www.networkadvertising.org/participating (last visited Oct. 23, 2010) (listing member firms who agree to abide by the NAI principles).

163. *See supra* notes 63–79 for a description of online behavioral advertising, also called "network advertising."

164. Press Release, DoubleClick Inc. & Abacus Direct Corp., DoubleClick, Inc. and Abacus Direct Corporation to Merge in a $1 Billion Stock Transaction (June 14, 1999), *available at* http://www.secinfo.com/dvjdn.69p.b.htm; Greg Miller, *DoubleClick Cancels Plan to Link Net Users' Names, Habits*, L.A. TIMES, March 3, 2000, at C1, *available at* http://articles.latimes.com/2000/mar/03/business/fi-4897.

165. Hiawatha Bray, *DoubleClick Backs Off on Net Data, Bows to Protests on Use of Personal Information*, BOS. GLOBE, Mar. 3, 2000, at C1, *available at* http://articles.latimes.com/2000/mar/03/business/fi-4897; Chris O'Brien, *DoubleClick Looks to Regain Surfers' Trust*, SAN JOSE MERCURY NEWS, Feb. 27, 2000, at 1D.

166. Miller, *supra* note 164.

167. *Id.*

168. NETWORK ADVER. INITIATIVE, SELF-REGULATORY PRINCIPLES FOR ONLINE PREFERENCE MARKETING BY NETWORK ADVERTISERS 1 (2000) [hereinafter NAI 2000 PRINCIPLES], *available at* http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf.

169. *Id.*

provide users with notice and an opportunity to opt out of the combination of their post-publication clickstream data with PII.[170] Effectively, the principles allowed the merger of post-publication clickstream data and PII unless the user took the unlikely steps of accessing a website's privacy policy, reading and understanding it, and affirmatively opting out of such merger. Moreover, the principles placed no limits on secondary use of the information so long as the individual had notice and an opportunity to opt out. This placed a large burden on the individual users to protect their own privacy.

The principles also required NAI members to post privacy policies giving users notice that the site would be collecting personal information and, with respect to PII at least, explaining how the information would be used or distributed to third parties.[171] On its face, this requirement satisfied the Fair Information Practices requirements of "notice" and "choice."[172] As the FTC's survey demonstrated, however, users often fail to read the full privacy policy,[173] and even when they do, they frequently do not understand it.[174] The reality of user behavior made the NAI requirements ineffective for meeting Fair Information Practices requirements.

As the critics of self-regulation might have predicted,[175] the NAI faced its biggest challenges in the realms of compliance and enforcement. The 2000 principles indicated that a third party (later deemed to be TRUSTe, the privacy seal organization)[176] would enforce the principles through random audits and investigation of consumer complaints.[177] The NAI further promised to sanction non-compliant mem-

---

170. *Id.* (phrasing this as a requirement that the members follow the Online Privacy Alliance's guidelines on privacy policies for PII). This opt-out feature, as well as those referred to below, may be located in the company's privacy policy, *id.* at 4, and may be accomplished through the use of an "opt-out cookie," *id.* at 7.

171. *Id.* at 1 (phrasing the special rules for PII as a requirement that the members follow the Online Privacy Alliance's guidelines on privacy policies for PII, which the NAI Principles incorporate by reference). The principles also require members to refrain from using "sensitive" PII. *Id.* at 3 (defining "sensitive" PII as personally identifiable information about "medical or financial data, sexual behavior or sexual orientation, [and] social security numbers . . . .").

172. *See supra* notes 121–23 and accompanying text.

173. *See* CTR. FOR DEMOCRACY AND TECH., *supra* note 131, at 4; McDonald & Cranor, *supra* note 131.

174. FTC MAY 2000 REPORT, *supra* note 33, at 24–26. For example, many policies begin by stating generally that the site will not disclose user information, but then, deeper in the policy, include numerous exceptions to this rule. *Id.* at 25. This may lead users to believe that the site is tightly restricting access to their information, when in fact it is sharing the information with numerous other parties such as "business partners, sponsors and other third parties." *Id.*

175. *See supra* notes 9–14 and accompanying text.

176. *See* Dixon, *supra* note 50, at 32–33 (noting NAI selecting TRUSTe as third-party enforcement organization). *See generally* TRUSTE, http://www.truste.com (last visited Oct. 24, 2010).

177. NAI 2000 PRINCIPLES, *supra* note 168, at 12.

bers by revoking their NAI membership or notifying the FTC and the public, or both.[178] As time passed, however, it became increasingly clear that the NAI would not follow through on these commitments. By 2003, membership in the organization had fallen from twelve companies[179] to two.[180] Enforcement followed a similar trajectory. When TRUSTe initially took on the enforcer role, it reported user complaints in its online "Watchdog Reports," specifying the number, nature, and resolution of complaints.[181] Between 2003 and 2005, however, it ceased providing the number and description of complaints filed, reporting only the number of complaints that had been *resolved*.[182] During this time, TRUSTe itself became an associate member of the NAI for one year.[183] This directly conflicted with the NAI's earlier statements that the enforcement entity would be completely "independent."[184] Finally, in 2006, TRUSTe simply stopped reporting NAI complaints as a separate, identifiable category.[185] Moreover, there is no evidence that TRUSTe *ever* conducted random audits of members as the principles required it to do.[186] According to one commentator, TRUSTe's enforcement was "neither independent nor transparent" and failed to serve as an effective measure of the NAI principles' value.[187]

---

178. *Id.* The document does not specify which sanctions will follow which violations. *Network Advertising Initiative: Principles not Privacy*, ELEC. PRIVACY INFO. CENTER (July 2000), *available at* http://epic.org/privacy/internet/NAI_analysis.html. In addition, the principles neither provide individuals with a mechanism to follow up their complaints nor specify a remedy for their injuries. *Id.*

179. These initial members represented over 90% of industry revenue and ads served. FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS PART 2: RECOMMENDATIONS 10 (2000) [hereinafter FTC JULY 2000 REPORT].

180. Dixon, *supra* note 50, at 28–29. Compounding this problem, the NAI in 2002 created a new "associate membership" status through which entities could join the organization without having to comply fully with the principles. *Id.* at 29–30. Associate members soon outnumbered full members. *Id.* at 30.

181. *Id.* at 35. The Watchdog website is still available. *See* TRUSTE, https://www.truste.org/consumers/compliance.php#c1 (last visited Oct. 24, 2010) (describing Watchdog processes).

182. Dixon, *supra* note 50, at 34.

183. *Id.* at 35.

184. *Id.* at 30.

185. It is hard to believe that there were no NAI-related complaints during this period, when there had been some for every month except one during earlier periods.

186. Dixon, *supra* note 50, at 34.

187. *Id.* at 39. The FTC, too, appears to have been less than pleased. Initially, the FTC expressed some optimism about the NAI principles, commending the member companies "for the innovative aspects of their proposal and for their willingness to adopt and follow these self-regulatory principle[s]." FTC JULY 2000 REPORT, *supra* note 179, at 9. Even at that point, however, the Commission was not ready to put its trust entirely in self-regulation. It continued to maintain that "backstop legislation addressing online profiling is still required" and to recommend that Congress pass such legislation. *Id.* at 10. Over time the Commission's faith in the principles appears to have faded considerably. On December 20, 2007, in a sign that the NAI Principles needed im-

Acknowledging the flaws in its original effort, the NAI published revised principles in 2008.[188] While the new principles contain several improvements,[189] they appear to have taken a step backward with respect to the most troublesome area: enforcement. Instead of designating a third-party enforcement entity, the 2008 principles provide for the NAI itself to police the compliance of its paying members.[190] This is a clear conflict of interest that may well bring about a repeat of the enforcement failings of the initial effort.

The past decade of self-regulation has been discouraging. The OPA and the first NAI effort each suffered from inadequate participation, weak enforcement, and standards that were not sufficiently protective. This experience supports the critics' claims that self-regulatory standards will be too lenient, that industry members will be hesitant and ineffectual in trying to enforce these standards against one another, and that substantial numbers of firms will fail to participate and will instead free ride on the efforts of others.[191]

3. Co-Regulation: A Viable Alternative?

Self-regulation is not working to fill the market's blind spot with respect to online privacy.[192] There are also serious questions about whether detailed government regulation is appropriate for this fast-moving, complex part of the economy or even feasible in light of major political obstacles.[193] While the country searches for an appropriate means of regulation, Internet firms are collecting and storing more and

---

provement, the Commission released a set of "Guidelines" for how to design acceptable self-regulatory principles. *See* FTC 2009 STAFF REPORT, *supra* note 49, at 1, 45–46 (describing proposal).

188. Taking the hint, the NAI in 2008 released a revised set of principles. NETWORK ADVER. INITIATIVE, 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT 3 (2008) [hereinafter NAI 2008 PRINCIPLES], *available at* http://www.networkadvertising.org/networks/principles_comments.asp.

189. The NAI allowed members of the public to comment on the 2008 principles and provided an expanded definition of "sensitive information." *See* CTR. FOR DEMOCRACY AND TECH., *supra* note 131, at 2–3. The organization also promised (again) to publish its enforcement data. *See The NAI Compliance Program Overview*, NETWORK ADVER. INITIATIVE, http://www.networkadvertising.org/managing/enforcement.asp (Dec. 30, 2009) ("Beginning in 2009, the NAI will produce an annual summary of the nature and number of consumer complaints received, the nature and number of complaints that were escalated to membership and the nature and number of matters referred to the Board, specifying the name of companies, if any, that were sanctioned for failure to remedy compliance defects.").

190. CTR. FOR DEMOCRACY AND TECH., *supra* note 131, at 4.

191. *See supra* notes 9–14 and accompanying text.

192. *See supra* notes 125–27 and accompanying text.

193. *See supra* notes 94–116 and accompanying text.

more personal information with every passing day. Another solution is imperative.

Co-regulation is a third approach that has the potential to combine the strengths of the first two.[194] Not enough information is yet available about how this method would fare with respect to the protection of information privacy. An examination of proponents' claims about co-regulation's virtues and critics' concerns about its potential weaknesses, along with a survey of international industry codes of conduct, will begin to fill in this gap. This section examines the most prominent real-world experience with a co-regulatory approach to data protection: the European experiment. By analyzing the individual national laws regarding industry codes of conduct, this discussion provides insight into how the Europeans have implemented the co-regulation initiative and potential guidance for the United States in implementing its own strategy.

a. What is Co-Regulation?

The key distinction between co-regulation, government regulation, and self-regulation concerns who sets and enforces regulatory goals and standards.[195] In self-regulation, the regulated industry itself sets the goals, develops the rules, and enforces the standards. In government regulation, public officials handle these tasks. In co-regulation, government and private parties share responsibility.[196] They may do this by splitting the tasks up. For example, government might set the overall goals but then allow industry to set and enforce the standards. Or, more commonly, government and the private sector might perform one or more of the tasks together. For example, government and an industry trade association might negotiate the proper regulatory goals, collaborate on the drafting of standards, and work cooperatively to enforce the standards against specific firms that violate them. Scholars refer to this type of co-regulation as "collaborative governance"[197] or "contractual regulation."[198]

---

194. *See supra* notes 14–23 and accompanying text.

195. *See* REES, *supra* note 17, at 9 (explaining that regulation consists of setting rules and enforcing them and that types of regulation may be defined in terms of who performs these functions).

196. *See* BREDOW-INSTITUT REPORT, *supra* note 15, at 17 (defining "co-regulation" as systems that "combin[e] state and non-state regulatory activities" and contrasting it with self-regulation which operate "without any state involvement").

197. *See generally* Freeman, *Collaborative Governance*, *supra* note 17.

198. *See* Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 CAP. U. L. REV. 21, 63, 80 (2001) (using the terms "micro contracts" and "macro contracts").

Many administrative agencies have used co-regulation.[199] For example, negotiated rulemaking ("reg-neg"), which many agencies have employed, brings agency representatives and stakeholders together to negotiate consensus-based rules.[200] This is a form of co-regulation. Similarly, the Environmental Protection Agency's Brownfields and Habitat Conservation programs involve negotiated, site-specific compliance arrangements that fit the circumstances of particular firms or parcels of property.[201] Various other agencies draw on industry guidelines in developing safety or product standards and, if they measure up to agency review, incorporate them into law.[202] For example, the California Occupational Health and Safety Administration implemented an innovative program in which it worked with representatives of both management and labor to develop and enforce safety standards tailored to specific construction sites.[203] Such government–industry collaboration, whether in the setting of goals, the formulation of standards and rules, or the enforcement of rules, is the defining feature of co-regulation.

b. Claims and Concerns

While co-regulatory initiatives can be quite diverse, the claims that proponents make about them are often consistent. As with self-regulation, some of the claims stem from the notion that industry members have unique knowledge of their own processes and business strategies.[204] Proponents believe that collaborative processes will encourage these firms to be more forthcoming with this information than they would be if government alone were setting the agenda.[205] They argue that this openness will yield goals that are more realistic and rules and standards that are more cost-effective,[206] workable,[207] and adaptive to

199. *See* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 547 (2000) [hereinafter Freeman, *Private Role*].

200. *See id.* at 654–55; Philip J. Harter, *Collaboration: The Future of Governance*, 2009 J. DISP. RESOL. 411, 423 (2009).

201. *See* Freeman, *Private Role*, *supra* note 199, at 657–64; Stewart, *supra* note 198, at 68–80.

202. Freeman, *Private Role*, *supra* note 199, at 638–40. For example, Section 551 of the Telecommunications Act of 1996 gives the FCC authority to promulgate ratings for violent, sexual, or other material that parents may find objectionable for their children to watch. Pub. L. No. 104-104, 110 Stat. 56 (1996) § 551(b)(1)(w)(1) (codified at 47 U.S.C. § 303 (2006)). But it first offers the broadcasting and movie industries a chance to develop "voluntary standards." *Id.* § 551(e)(1)(A). If the FCC finds these standards to be acceptable, it is to use them instead of developing its own. *Id.*

203. *See* Freeman, *Private Role*, *supra* note 199, at 651–53.

204. GUNNINGHAM & SINCLAIR, *supra* note 17, at 97 (discussing the "assumption that industry knows best how to abate its own environmental problems").

205. LYLE SCRUGGS, SUSTAINING ABUNDANCE: ENVIRONMENTAL PERFORMANCE IN INDUSTRIAL DEMOCRACIES 145–46 (2003); Freeman, *Collaborative Governance*, *supra* note 17, at 22–24.

206. *See* GUNNINGHAM & SINCLAIR, *supra* note 17, at 104.

changing business realities[208] than the rules that government would create on its own.[209] Regulated businesses will also have a stronger sense of ownership over the rules that govern them and will comply more readily.[210] This ownership will reduce the delays and administrative costs associated with industry challenges to government regulation.[211] It will also make co-regulation more politically practicable than direct government requirements.[212]

For proponents, co-regulation promises important advantages that self-regulation does not. First, government officials will push business to prioritize public goals over their own interests, resulting in regulations that are less one-sided than under a self-regulatory scheme. Second, bringing government and business together in a collaborative enterprise should lead to improved government-industry relations, turning adversaries into joint problem solvers and setting the groundwork for increased information sharing and cooperation in the future.[213] This collaboration will lead to more creative solutions to social problems than either party could devise alone.[214] Parties that have engaged in a collaborative process will also feel accountable to each other, adding a layer of shared responsibility that would not exist under a pure governmental approach.[215] Because of these advantages, proponents of co-regulation argue, collaborative governance will ultimately yield better social performance than direct government regulation.[216] If these claims are correct, then co-regulation may be able to address some of the shortcomings of market regulation, self-regulation, and government regulation, making it worth considering as a potential mechanism for protecting privacy on the Internet.

---

207. *See* Freeman, *Collaborative Governance*, *supra* note 17, at 26.

208. *See id.*; Stewart, *supra* note 198, at 82–83.

209. SCRUGGS, *supra* note 205, at 152 (Cooperative approaches can create "a regime where flexible, cost-effective implementation of high standards can occur.").

210. Freeman, *Collaborative Governance*, *supra* note 17, at 22–24; *see* SCRUGGS, *supra* note 205, at 146.

211. *See* GUNNINGHAM & SINCLAIR, *supra* note 17, at 104.

212. *Id.* at 109–10.

213. Freeman, *Collaborative Governance*, *supra* note 17, at 22–24; *see* SCRUGGS, *supra* note 205, at 143.

214. Freeman, *Collaborative Governance*, *supra* note 17, at 22–24.

215. *Id.* at 22.

216. *See* REES, *supra* note 17, at 2, 224, 233 (comparing accident rates at construction sites that regulate safety through a collaborative process and those that use a more top-down model, and finding that the former have a lower rate of accidents); SCRUGGS, *supra* note 205, at 153 (conducting empirical study of environmental performance in developed nations and finding that those countries that employ consensual, neo-corporatist regulatory methods show "systematically" better environmental performance than those that follow an interest group model).

Yet it is also worth considering the arguments against co-regulation. Critics of co-regulatory methods argue that industry will not reveal insider knowledge to regulators but will instead use its informational upper hand to obtain weaker standards.[217] Moreover, the reduction in the public's opportunity to participate in co-regulatory initiatives will lead to less creativity, not more.[218] Because collaborative discussions often take place outside of the public eye, this system could also facilitate agency "capture," whereby government begins to pursue industry's agenda rather than the public's agenda.[219] Furthermore, business representatives may not enforce the rules vigorously,[220] and in the absence of such enforcement, some firms may free ride on the efforts of others.[221] Established firms could also have an unfair advantage in that they could use collaborative negotiations to establish standards that discriminate against new entrants.[222] Finally, industry representatives who participate in the co-regulatory process will be conflicted because they have a strong incentive—and even a legal obligation to their shareholders—to put bottom-line concerns ahead of the public interest.[223] Critics of co-regulation express profound skepticism that this process, which gives industry a greater voice in government regulation, will yield improved social outcomes.[224]

While the arguments of the proponents suggest that it is worth exploring co-regulatory solutions to the Internet privacy problem, the critics make it plain that it would be unwise to head down this path without careful consideration of the possible negative consequences and of ways to avoid them. These competing views make it important to study how co-regulation actually works in the area of privacy protection.

IV. EUROPEAN CODES OF CONDUCT: THE LEGAL FRAMEWORK

The E.U. member nations' data protection codes of conduct are a ready-made laboratory for study of the co-regulation of privacy. As explained above, pursuant to the 1995 Data Protection Directive, each of the E.U. member nations passed a comprehensive data protection statute

217. GUNNINGHAM & SINCLAIR, *supra* note 17, at 105.

218. SCRUGGS, *supra* note 205, at 135, 139 (discussing critics' argument that the public has fewer opportunities to participate in co-regulation than in traditional rulemaking).

219. GUNNINGHAM & SINCLAIR, *supra* note 17, at 105 (describing this argument); SCRUGGS, *supra* note 205, at 128 (same); REES, *supra* note 17, at 12, 236 (same). These critics note that the repeated, private meetings that characterize the collaborative approach provide an ideal setting for such a distortion of the regulatory process. *See* GUNNINGHAM & SINCLAIR, *supra* note 17, at 105.

220. *See generally* Koops, et al., *supra* note 18.

221. GUNNINGHAM & SINCLAIR, *supra* note 17, at 103.

222. *See* SCRUGGS, *supra* note 205, at 136 (describing this argument).

223. *See id.*

224. BENNETT & RAAB, *supra* note 94, at 134.

into law.[225] Article 27 of the Directive requires member nations to build into their statutes a provision allowing industry sectors to draft a "code of conduct" that spells out how the broad requirements of the statute will apply to their particular industry.[226] This code of conduct then becomes the basis for a co-regulatory approach. Industry sectors submit the code of conduct to the national Data Protection Authority (the Authority).[227] The Authority evaluates it, negotiates its terms with the relevant sector, and ultimately determines whether the code meets the requirements of the statute.[228] If the Authority approves the code, then the code becomes the official guide to determining what industry members must do to comply with the statute.[229] Codes of conduct thus allow government and industry to work together to develop specific standards governing how industry must protect personal data. This European experiment represents co-regulation applied to the field of data protection and offers a testing ground on which to evaluate how this approach works in the privacy field.

Surprisingly, few American scholars or policymakers have paid attention to this initiative.[230] For now, the data protection statutes themselves are the most comprehensive resource. These statutes set out the legal framework within which government and industry negotiate the codes of conduct. An analysis of these statutes can begin to answer at least some of the questions about these co-regulatory instruments.

A. The 1995 Data Protection Directive

The European Commission's 1995 Data Protection Directive requires E.U. member nations to adopt legislation governing the collection, use, and disclosure of personal information.[231] According to the Directive, each member nation must establish by statute a national data protection authority;[232] identify the conditions under which it is and is not appropriate to collect personal information;[233] require that firms notify the data protection authority prior to commencing data processing operations;[234] prohibit (with certain exceptions) the collection and use of sensi-

225. *See supra* notes 245–72 and accompanying text.

226. Directive 95/46/EC, *supra* note 24, art. 27(1).

227. *Id.* art. 27(2).

228. *Id.*

229. *See id.*

230. In a forthcoming article, one insightful American scholar has begun to pay attention to the European codes of conduct and their relevance for U.S. privacy policy. *See generally* Ira Rubinstein, *supra* note 23.

231. Directive 95/46/EC, *supra* note 24, art. 32(1).

232. *Id.* art. 28(1).

233. *Id.* arts. 6–7.

234. *Id.* art. 18(1).

tive personal information such as race, religion, or sexual orientation;[235] and require that firms notify individuals and get their informed consent before collecting and processing their personal data.[236] These requirements apply to Internet firms as well as other companies. U.S. law provides no counterpart to these ambitious, comprehensive protections.

After a member nation adopts a statute, Article 27 of the Directive instructs member nations to work with the industry to incorporate codes of conduct into their laws. It reads as follows:

> (1) The 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.
>
> (2) Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.
>
> Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.
>
> (3) Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.[237]

This language describes how E.U. member nations are to incorporate the codes of conduct into their privacy laws. First, Article 27 explains the purpose of a code of conduct. The codes are "intended to contribute to the proper implementation of the national provisions . . . taking account of the specific features of the various sectors."[238] In other words, the codes for each sector are to elaborate how generic data protection

235. *Id.* art. 8(1)–(3).
236. *Id.* arts. 10, 14.
237. *Id.* art. 27.
238. *Id.* art. 27(1).

laws should apply to the specific features of that particular sector. They should set out a tailored set of rules that adjust the national standards to fit the realities of each sector.[239]

Second, Article 27 instructs member nations and the European Commission to "encourage" sectors to draft codes of conduct.[240] This instruction is ambiguous. What does it mean to "encourage" a sector to draw up a code? Should a member state leave the task largely up to the sector, perhaps with some incentives to act? Or should it actively push, or even require, sectors to draft codes of conduct? Article 27 does not clearly instruct member nations on this point. The resulting national laws reflect this ambiguity.[241]

Third, Article 27 affirms that sectors can submit their draft code of conduct to the national Data Protection Authority, and that the Authority should offer its opinion as to whether the code is consistent with the underlying national data protection law.[242] This provision, too, creates ambiguity. What is the legal import of the Authority's opinion? Is it legally binding on the Authority? Or does it merely provide guidance as to how the Authority currently views the code, with the caveat that the Authority may change its mind? To what extent, if any, is the opinion binding on the courts? Are the courts required to treat compliance with the code as compliance with the law? Need they, at a minimum, defer to the Authority's expert assessment that the code accurately expresses the law? These areas of ambiguity, too, find their way into the member nations' data protection laws; some treat the codes as legally binding, while others clearly do not.

Fourth, Article 27 provides that "[i]f it sees fit, the authority shall seek the views of data subjects or their representatives" when determining whether the code is consistent with the underlying data protection law.[243] The mixed signal of "shall, if it sees fit" encourages the Authority to meet with data subjects and their representatives but ultimately makes this function discretionary. E.U. member nations have interpreted the provision differently. Some require the national Authority to meet with the industry, while others make it discretionary or avoid the topic altogether. This variety in interpretation adds to the inconsistency of national laws regarding codes of conduct.

---

239. DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE: REPORT ON THE FINDINGS OF THE STUDY 185 (2002) (codes of conduct can "clarify the application of data protection law in a particular sector . . . and [Article 27] confirms that this is seen as a possibly effective instrument in this regard.").

240. Directive 95/46/EC, *supra* note 24, art. 27(1).

241. *See infra* note 244 and accompanying text.

242. Directive 95/46/EC, *supra* note 24, art. 27(2).

243. *Id.*

Finally, Article 27 clarifies that there are actually two types of codes: national and community.[244] National codes of conduct apply to a specific industry sector in a particular E.U. member nation. The representatives of that national sector generally develop such a code and submit it to the national Data Protection Authority for review. Community codes of conduct apply to an industry sector as it exists throughout the entire European community. Representatives of that sector from throughout the European Union draft the code and submit it to the Article 29 Working Party for review. The two types of codes, therefore, differ both in their scope and in the process by which they are reviewed.

B. National Laws Governing Data Protection Codes of Conduct: Common Elements

While the national laws that implement Article 27 diverge from each other in important ways, they also share some important elements. First, all the national laws contain substantive data protection requirements that apply by default to sectors that do not draft their own codes. Thus, the sectoral codes of conduct all operate against a background of substantive data protection law. Second, consistent with the Article 27 language, most statutes say that the purpose of a code of conduct is to adapt the national law so that it fits the realities of the sector. For example, the Dutch data protection law states that organizations should draft codes of conduct that implement the law in light of "the particular features of the sector or sectors of society in which these organizations are operating . . . ."[245] Other national laws are similar.[246] At least one nation goes further and defines the codes' purpose more ambitiously. In 1999, the Portuguese Authority passed a formal resolution in which it said that sectoral codes of conduct should "*add to* the provisions of the legislation in force by embodying legal rules specific to their particular industrial or commercial sector" and that they should be "designed to contribute to the *stricter enforcement* of the provisions of the data protection law in each activity sector."[247] This language suggests that Portugal will look for

244. *Id.* art. 27(1), (3).

245. Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(1), Stb. 2000, p. 302 (Neth.)

246. *See, e.g.*, Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel [Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data] art. 2(a) (Lux.) (sectors draw up codes of conduct "in order to apply this Law correctly").

247. PORTUGUESE DATA PROT. AUTH., ANNUAL ACTIVITY REPORT 1999: RESUMÉ PAPER (in English) 22 (1999) (emphasis added), *quoted in* DOUWE KORFF, FED'N OF EUROPEAN DIRECT MKTG., THE PORTUGUESE DATA PROTECTION LAW: A BRIEFING ON LAW N° 67/98 OF 26 OCTOBER 1998 (LAW ON THE PROTECTION OF PERSONAL DATA) § 8 (2005) [hereinafter KORFF, PORTUGUESE DATA PROTECTION].

codes to be more rigorous than the data protection statutes that they interpret and apply.

Third, virtually all national laws provide that, where a sector submits a code of conduct, the Authority must review it and issue an opinion on whether it is consistent with the national data protection law. For example, the Swedish data protection law states that "The Data Protection Board Shall . . . issue an opinion on [proposed codes of conduct, which] . . . shall relate to the compatibility of the branch agreement with the Personal Data Act."[248] Similarly, the Belgian law states that "the Commission shall verify whether the drafts that are submitted to it are in accordance with this law and with the decrees that have been taken in implementation thereof." [249] Other national laws contain similar language.[250] These provisions make it clear that the national Authority has a nondiscretionary obligation to review a code and to determine whether it conforms to the national data protection law.

E.U. member nations' statutes differ when it comes to the legal import of the Authority's decision. Some do not explicitly assign any legal status to the Authority's opinion. Instead, they treat it much like agency "guidance" in the United States—an authoritative but nonbinding state-

---

248. 12 § PERSONUPPGIFTSFÖRORDNING [Personal Data Ordinance] (Svensk författningssamli ng [SFS] 1998:1191) (Swed.), *available at* http://www.sweden.gov.se/content/1/c6/02/56/33/ed5aaf5 3.pdf.

249. La Loi Relative à la Protection des Données à Caractère Personnel [Law of Privacy Protection in Relation to the Processing of Personal Data] of Dec. 8, 1992, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], June 26, 2003, art. 44 (Belg.).

250. Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], May 22, 2001, BUNDESGESETZBLATT I [BGBL I] at 904, § 38a(2) (Ger.) ("The supervisory authority shall examine the compatibility of the submitted draft[] [codes of conduct] with the applicable law on data protection."); Decreto Legislativo 30 giugno 2003, n. 196 § 12(1), in G.U. July 29, 2003, n. 174 (It.), *available at* http://www.privacy.it/privacycode-en.html (authority shall verify codes' "compliance with laws and regulations"); Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel [Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data] art. 32(3)(g) (Lux.) (authority "to receive and where applicable . . . approve codes of conduct"); Att Dwar il-Protezzjoni u l-Privatezza tad-Data [Data Protection Act] art. 40(g), 2001 Cap. 440. 1 (Malta) (authority should "ascertain that the provisions of such codes are in accordance with the provisions of this Act"); Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(1), Stb. 2000, p. 302 (Neth.) (authority should "declare that . . . the rules contained in the said code properly implement this Act or other legal provisions on the processing of personal data"); Protection of Personal Data Law art. 32(3) (B.O.E. 1999, 298) (Spain) (authority to evaluate whether or not the "code [complies] with the legal and regulatory provisions on the subject"); DOUWE KORFF, FED'N OF EUROPEAN DIRECT MKTG., THE FRENCH DATA PROTECTION LAW § 7 (2005) (authority must provide opinions on drafts of "professional codes"); DOUWE KORFF, FED'N OF EUROPEAN DIRECT MKTG., THE IRISH DATA PROTECTION LAW: A BRIEFING ON THE DATA PROTECTION ACTS OF 1988 AND 2003 § 8 (2005) [hereinafter KORFF, IRISH DATA PROTECTION] (commission must evaluate whether code meets the requirements of the act).

ment of the Authority's view on what the law requires.[251] For example, the Danish statute states that approved codes of conduct are only "intended to contribute to the proper implementation of the rules laid down in this Act."[252] Other statutes implicitly suggest that the opinion is binding on the Authority itself. For instance, the Spanish data protection law states that once the Authority has approved a code of conduct it must "deposit[] and enter[] [the code] in the General Data Protection Register . . . ."[253] The entry of the code in the Register "indicates that the Data Protection Authority agrees that the provisions of the code *do* comply with the Law and any relevant other rules; and that compliance . . . with the code will thus ensure compliance with the Law."[254] A few statutes go even further and provide a mechanism by which a code of conduct can be given the force of law, thereby becoming binding not only on the Authority, but on the courts as well. For example, the Italian law states that the Authority must publish an approved code of conduct in the Official Journal of the Italian Republic whereupon the Minister of Justice may, by decree, have the code included in a special annex to the data protection law itself.[255] Where this occurs, the code "becomes part of the legal obligations of controllers in the relevant sector . . . ."[256] While

---

251. JERRY L. ANDERSON & DENNIS D. HIRSCH, ENVIRONMENTAL LAW PRACTICE: PROBLEMS AND EXERCISES FOR SKILLS DEVELOPMENT 43 (3rd ed. 2010) (defining agency guidance).

252. Act on Processing of Personal Data, May 31, 2000, LOVTIDENDE, June 2, 2000, at 2663, ch. 19 § 74 (Den.).

253. Protection of Personal Data Law art. 32(3) (B.O.E. 1999, 298) (Spain).

254. DOUWE KORFF, FED'N OF EUROPEAN DIRECT MKTG., THE SPANISH DATA PROTECTION LAW: A BRIEFING ON LOPD LAW ON THE PROTECTION OF PERSONAL DATA (ORGANIC LAW 15/1999 OF 13 DECEMBER 1999), § 8 (2005). The Spanish law goes on to say that, where the authority does not believe the code of conduct to be an accurate expression of the law, it may refuse to enter it in the General Data Protection Register and must then "require the applicants to make the necessary changes." Protection of Personal Data Law art. 32(3) (B.O.E. 1999, 298) (Spain). For other laws of this type, see Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel [Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data] art. 32(3)(g) (Lux.) (statute says that authority should "approve" codes of conduct submitted to it); Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(1), (4) Stb. 2000, p. 302 (Neth.) (authority's positive opinion "shall be deemed to be equivalent to a decision within the meaning of the General Administrative Regulations Act"); Lei da Protecção de Dados Pessoais [Law to Protect Personal Data], Oct. 26, 1998, DIÁRIO DA REPÚBLICA at 5536, ch. V, art. 32(3) (Port.) (The statute provides that the authority may "declare whether the drafts are in accordance with the laws and regulations," and the authority has decided to make these declarations in the form of Resolutions which "constitute binding administrative decisions."). Commentators say that the use of the term "approve" goes beyond the simple offering of an "opinion" and means that the authority will treat compliance with the code as equivalent to compliance with the law. KORFF, PORTUGUESE DATA PROTECTION, *supra* note 247, § 8.

255. Decreto Legislativo 30 giugno 2003, n. 196 § 12, in G.U. July 29, 2003 (It.), *available at* http://www.privacy.it/privacycode-en.html.

256. DOUWE KORFF, FED'N OF EUROPEAN DIRECT MKTG., THE ITALIAN DATA PROTECTION LAWS § 8 (2005). At least one other nation provides a similar mechanism. KORFF, IRISH DATA PROTECTION, *supra* note 250, § 8 (Irish law allows Minister of Justice to submit an approved code to

these laws vary as to the legal import of the Authority's opinion, they concur in the basic idea that the Authority should review codes of conduct for compliance with the law and issue an opinion. Article 27 requires as much.

C. Classifying the National Laws

The key feature that divides the various statutes is the degree to which they give an industry sector room to decide whether it wants to adopt a code of conduct or, under the language of Article 27, the degree of force with which the statutes "encourage" the sector to adopt such a code. Other elements tend to cluster around this central feature. Accordingly, this feature can be used to organize and group the laws into three categories: (1) industry choice, (2) balance of power, and (3) government choice.

1. Industry Choice

The first category encompasses those laws that give the industry sector complete discretion in deciding whether or not to draft a code of conduct. For example, the Austrian data protection law provides that "representations of interest established by law, other professional associations and comparable bodies *may* draw up codes of conduct for the private sector."[257] Other laws in this group are similar.[258] The laws that fall into this category interpret liberally Article 27's instruction that the national laws should "encourage the drawing up of codes of conduct . . . ."[259] They permit sectors to set out a code of conduct but do not

---

the Parliament for further approval.) "If both houses of Parliament endorse the code (by means of resolutions to that effect), the code in question gains the force of law: the code is treated like a *statutory instrument*, and its provisions are treated (or rather, will have become) as if they were *binding legal provisions*." *Id. Cf.* Data Protection Act, 1998, c. 29, § 52(3) (U.K.) ("The Commissioner shall lay before each House of Parliament any code of practice prepared" at the behest of the Secretary of State.).

257. BUNDESGESETZ ÜBER DEN SCHUTZ PERSONENBEZOGENER DATEN [FEDERAL ACT CONCERNING THE PROTECTION OF PERSONAL DATA] BUNDESGESETZBLATT I [BGBL I] No. 165/1999, § 6(4) (Austria) (emphasis added).

258. *See* La Loi Relative à la Protection des Données à Caractère Personnel [Law of Privacy Protection in Relation to the Processing of Personal Data] of Dec. 8, 1992, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], June 26, 2003, art. 44 (Belg.); Act on Processing of Personal Data, May 31, 2000, LOVTIDENDE, June 2, 2000, at 2663, ch. 19 § 74 (Den.); Personuppgiftslag [Personal Data Act] 523/1999, as amended, § 42 (data controllers "may draft sectoral codes of conduct") (Fin.); Bundesdatenschutzgesetz (BDSG) [Federal Data Protection Act], May 22, 2001, BUNDESGESETZBLATT I [BGBL I] at 904, § 38a (Ger.) (associations "may submit draft rules of conduct"); Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(1), Stb. 2000, p. 302 (Neth.) (organization planning to draft a code of conduct may request the authority to review it).

259. Directive 95/46/EC, *supra* note 24, art. 27.

push them to do so.[260] Even so, laws of this type do not abdicate government's role in favor of pure self-regulation. Sectors that decide not to draft a code of conduct will still be subject to the general data protection law and its many requirements. Moreover, where a sector in one of these nations does choose to draft a code of conduct, the Authority reviews and gives its "opinion" on it.

Laws that fit this category tend to have other features in common. First, they are more likely to require (as opposed to allow) the Authority to consult with data subjects when formulating its consistency opinion.[261] Second, a law in this category may give courts the ability to review the Authority's consistency opinion.[262] This feature allows a trade association, firm, or citizen group to legally challenge the Authority's opinion on whether the code meets the terms of the statute. In these two ways, this group of statutes limits the Authority's discretion at the same time as it expands the industry's role (and, to some extent, that of the public). The statutes in this group temper the Authority's power while emphasizing the interests of both the data controllers (the industry sector) and the data subjects.

2. Balance of Power

Statutes in the second group put more emphasis on the national government's Article 27 duty to "encourage" sectors to draft codes.

---

260. Presumably, if the authority gives a negative opinion, this will make it incumbent on the sector to go back and revise the code to make it compliant with the law. *See, e.g.*, Protection of Personal Data Law art. 32(3) (B.O.E. 1999, 298) (Spain) (Where the authority reviews a code and finds that it does not meet legal standards the authority "must require the applicants to make the necessary changes.") Thus, it is not true that any code of conduct will do. A sector's code must meet the government's standards in order to be officially recognized. In short, the sector gets to decide whether it wants to have a code of conduct. In that regard, the sector gets to take the initiative. But once it decides to do so, the national law and the authority's consistency opinion guide the effort.

261. For example, the Swedish data protection law states that the authority "shall, before it issues its opinion, if appropriate ensure that the organizations that represent the person registered [i.e. the data subjects] have been given an opportunity to express their views on the proposals for a branch agreement." 12 § PERSONUPPGIFTSFÖRORDNING [Personal Data Ordinance] (Svensk författningssamling [SFS] 1998:1191) (Swed.). *See also* La Loi Relative à la Protection des Données à Caractère Personnel [Law of Privacy Protection in Relation to the Processing of Personal Data] of Dec. 8, 1992, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], June 26, 2003, art. 44 (Belg.). (the Commission "shall . . . investigate, as far as possible, the standpoints of the persons concerned or of their representatives.").

262. Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(4), Stb. 2000, p. 302 (Neth.) (stating that the authority's opinion should be "deemed equivalent to a decision within the meaning of the General Administrative Regulations Act"). In practical terms, this means that it is subject to judicial review, just as any other such decision is. DOUWE KORFF, THE FED'N OF EUROPEAN DIRECT MKTG., THE DUTCH DATA PROTECTION LAW: A BRIEFING ON THE LAW OF 6 JULY 2000 CONTAINING RULES RELATING TO THE PROTECTION OF PERSONAL DATA (PERSONAL DATA PROTECTION LAW) § 7 (2005).

These statutes require the Authority to "call on"[263] or "encourage"[264] sectors to draft a code of conduct, although they do not spell out the lengths to which the Authority is to go. Laws in this category are more likely to require the sector to consult or "cooperate" with the Authority when drafting a code of conduct.[265] They are also more likely to provide a mechanism by which the code can be elevated to the status of law and so become binding, not just on the Authority, but on the courts as well. Under this approach, the industry and the government share power more equally. The Authority will strongly encourage an industry code of conduct and advocate for more rigorous standards;[266] at the same time, the Authority's involvement gives more regulatory weight to the code of conduct that the industry helped draft. Once the Authority has approved the code, the industry can fully rely on it. The statutes in this group, therefore, motivate both the government and the industry to invest in the formulation of a code of conduct and enhance the importance of the document that results.

3. Government Choice

The statutes in the third category push sectors to develop codes. Some of the statutes in this category stipulate that if a sector does not draft a code, the Authority should draft a code itself and impose it on the sector. For example, the Irish law states that if the Commissioner believes that a code of conduct would be useful and the sector fails to submit one, the Commissioner may himself draft the code after consulting

---

263. *See, e.g.*, Peri Epexergadias Dedomenōn Prodōpikon Charaktēra (Prostasia ton Atomon) Nomo ton 2001, 138(I), § 23(b) (Cypress) (The authority shall "call on and assist professional organizations and other unions of natural or legal persons . . . in drawing up codes of conduct . . . ."); Nomos (1997: 2472) Prodtadia ton Atómon apó tēn Epexergadia Dedomévōv Prodōpikoń Garaktēra [Protection of Individuals with Regard to the Processing of Personal Data] EPSĒMERIDA TĒS KYVERNĒDEŌS [ΦΕΚ] 1997, A:50, art. 19(1)(b) (Greece) (as amended by Laws 2819/2000 and 2915/2001) (The authority "shall call on and assist trade unions and other associations of legal and natural persons keeping personal data files in the preparation of codes of conduct . . . .").

264. *See, e.g.*, Decreto Legislativo 30 giugno 2003, n. 196 § 12(1), in G.U. July 29, 2003, n.174, (It.) ("The Garante shall encourage . . . the drawing up of codes of conduct and professional practice for specific sectors . . . ."); Att Dwar il-Protezzjoni u l-Privatezza tad-Data [Data Protection Act] art. 40(g), 2001 Cap. 440. 1 (Malta) (The Commissioner shall "encourage the drawing up of suitable codes of conduct by the various sectors . . . ."); Lei da Protecção de Dados Pessoais [Law to Protect Personal Data], Oct. 26, 1998, DIÁRIO DA REPÚBLICA at 5536, ch. V, art. 32 (Port.) (The authority "shall encourage the drawing up of codes of conduct.").

265. For example, the Italian statute states that the authority must "contribute" to the formulation of the code. D. Lgs. 196/2003 § 12(1) (It.) ("The Garante shall encourage . . . the drawing up of codes of conduct and professional practice for specific sectors . . . .").

266. Indeed, in a resolution interpreting one of the laws in this category, the Portuguese authority stated that the purpose of a sectoral code of conduct is not just to ensure compliance with the law, but to "add" to existing legal requirements and make enforcement "stricter." KORFF, PORTUGUESE DATA PROTECTION, *supra* note 247, § 8.

with relevant trade associations and interested parties.[267] The United Kingdom provides for a similar process in its data protection law.[268] This approach goes beyond mere encouragement and threatens a prescribed code of conduct to force sectors to develop their own rules.[269] Still, a sector retains the option of not producing a code and allowing the Authority to do it.

At least one nation removes all discretion, actually requiring sectors to develop codes. The Romanian law states that "professional associations *have the obligation* to elaborate and submit for approval, to the supervisory authority, codes of conduct . . . ."[270] It further provides that the Authority is to "approv[e]" the code, not just issue an "opinion" on it.[271] This obligation increases the legal force of the Authority's assessment and appears to make it, at a minimum, binding on the Authority itself. Interestingly, the Romanian law departs from the usual statement that the codes' purpose is to tailor the law to the realities of a given sector. Instead, it states that the purpose is to "protect the rights of persons" whose data is being processed.[272] Altogether, it is a more forceful provision that seems to have the rights of data subjects, rather than the convenience of industry, at its core. The Romanian statute emphasizes the power of the Authority to require the industry sector to draft a code and to approve the code. It is possible that Romania's historical grounding in Communist dictatorship increases its desire to protect personal privacy and causes people to look to a strong data protection authority in order to achieve this end. In any event, the codes take on even greater regulatory significance under this system.

It is not yet certain which legal framework will prove most effective. The first gives the industry more discretion and downplays the legal significance of any code that it chooses to develop. The second puts more pressure on both the industry and agency to negotiate a code and enhances the importance of the document that results. The third requires

---

267. KORFF, IRISH DATA PROTECTION, *supra* note 250, § 8 (explaining this feature of the Irish data protection law).

268. Data Protection Act, 1998, c. 29, § 51(3) (U.K.) (authorizing Commissioner "after such consultation with trade associations, data subjects or persons representing data subjects as appears to him to be appropriate" to "prepare and disseminate . . . codes of practice for guidance as to good practice").

269. One commentator has referred to it as the "stick behind the door" strategy. DOUWE KORFF, FED'N OF EUROPEAN DIRECT MKTG., THE UNITED KINGDOM DATA PROTECTION LAW: A BRIEFING ON THE DATA PROTECTION ACT OF 1998 AND ON THE TELECOMMUNICATIONS (DATA AND PRIVACY) REGULATION 1999 § 8 (2005).

270. Lege nr. 677 din 21 Noiembrie 2001 Pentru Protecţia Persoanelor cu Privire la Prelucrarea Datelor cu Caracter Personal şi Libera Circulaţie a Acestor Date, M.Of. 790/2001, art. 28(1) (Rom.).

271. *Id.*

272. *Id.*

the industry to draft a code and then gives the document even stronger legal force. Determining which legal framework results in the most nuanced, creative, and effective codes will require in-depth comparative study of the different legal approaches and the codes that emerge from them. It will necessitate analysis of policy documents by which national data protection authorities implement their approaches to codes of conduct. Even more importantly, it will require in-depth study of the codes themselves, the processes by which the industry sectors and the data protection authorities negotiate them, and the success of these codes in protecting personal information. Future research on these areas is imperative if the European Union's privacy regulation is to provide guidance for U.S. consideration of co-regulatory strategies.

V. CONCLUSION

As Internet businesses ramp up their collection and use of personal information, the regulation of online privacy in the United States remains stuck in neutral. Industry self-regulation, the dominant approach, is not working. While some call for legislation to address the issue, it is unclear whether online privacy is an area that lends itself to a legislative solution. In the meantime, with each passing day, websites, network advertisers, ISPs, and others collect and store more and more personal information. For all its benefits, the Internet is eroding personal privacy. If this dynamic does not change, it could destroy user trust and threaten the future of the Internet economy itself.

This article has considered co-regulation—a regulatory method in which government and industry work together to define and enforce standards—as a possible alternative. If those who endorse it are correct, co-regulation could yield more cost-effective, flexible standards that provide meaningful privacy protection. This approach might prove politically acceptable to all sides and could provide a means of transcending the current policy stalemate. Yet, the critics of co-regulation raise important red flags about this alternative approach. They warn that industry–government negotiations, taking place outside of the public eye, will yield one-sided deals that fail to protect individual privacy. They insist that industry will use its informational advantage to water down standards and will inevitably put its own interests before that of the public. They worry that co-regulatory arrangements will do no more than provide business with secure sanctuary in which to negotiate favorable arrangements.

This Article describes this ongoing debate, but it does not attempt to resolve it. Further research must be done on co-regulatory initiatives in the privacy field before it is possible to reach a conclusion. This research

should focus on the E.U. experience with data protection codes of conduct—a co-regulatory experiment that is going on right now and that will no doubt hold important lessons. This Article has already described and analyzed the statutory provisions through which the various E.U. nations have implemented the co-regulatory initiative; however, this analysis of the legal framework is but a first step in understanding the European codes of conduct and their implications for the U.S. regulation of online privacy. It will require further work, building on this Article, to determine whether co-regulation is an effective way to protect online privacy.