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

Dennis D Hirsch
THE LAW AND POLICY OF ONLINE PRIVACY: REGULATION, SELF-REGULATION, OR CO-REGULATION?

DENNIS D. HIRSCH
GERALDINE W. HOWELL PROFESSOR OF LAW
CAPITAL UNIVERSITY LAW SCHOOL

FULBRIGHT SENIOR PROFESSOR
UNIVERSITY OF AMSTERDAM (2010)

dhirsch@law.capital.edu
(614) 236-6685
In 2010, I was awarded a Fulbright Senior Professorship to study innovative European laws that seek to protect personal information, and to evaluate whether they might provide a model for U.S. law and policy in the area of online privacy. This article is the first of two that will present the results of my research.

*                         *                         *

Introduction

The rise of the Internet poses profound new challenges for information privacy.¹ Private companies such as Google save and store our every search query and can often trace them back to us as individuals.² Web sites closely track how we use their sites and frequently share this information with others.³ Internet Service Providers (ISPs) have begun to examine the very packets of information that constitute our connection to 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. This has made the Internet Janus-faced. One the 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. This not only damages individual privacy. It also erodes people’s trust in the Internet and so threatens to undermine the continued growth of e-

¹ See 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 ___-___ and accompanying text (describing this practice).

³ See infra notes ___-___ and accompanying text (describing this practice).

⁴ See infra notes ___-___ and accompanying text (describing this practice).
commerce and the Internet economy.  

There is wide-spread agreement that these problems are real and that something should be done to address them. However, there is far less agreement as to what this action should be. Two main camps dominate the debate. The first calls for government regulation. 

It seeks legislation that would set, or authorize regulators to set, detailed and strict limits on the ways that companies can collect data online, the types and amounts of personal information they can collect, and on the ways they can use this data. Proponents of this approach maintain that strong government regulation is necessary to protect unsuspecting Internet users against the self-interested behavior of Internet-based companies. The second camp, which has thus far won the day, argues that the market and industry self-regulation will yield better results than government rules. It believes that Internet businesses already have a market incentive to protect user privacy so as not to lose customers. Insofar as rules are necessary to correct for market failures this group believes that industry, not government, should set them.

---

5 Pam Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1129 (“information privacy is a key to building trust among consumers and trust is essential for the promise of e-commerce to be realized.”)

6 DANIEL J. SOLOVE, MARC ROTTENBERG, PAUL M. SCHWARTZ, *INFORMATION PRIVACY LAW* 2 (2nd ed. 2006).

7 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.”)

8 See, e.g., Robert E. Litan, *Law and Policy in the Age of the Internet*, 50 DUKE L. REV. 1045, 1045 (when it comes to regulation of the Internet “policymakers’ first instinct should be to rely on markets and technology to address troublesome issues.”)

Each of these two main viewpoints is vulnerable to criticism. Critics of government regulation argue that regulators face high information costs in trying to learn enough about complex Internet businesses to produce well-designed rules for them. This will result in rules that are not well-suited to business realities and that impose excessive costs relative to their benefits. These critics further emphasize that rapid and continuous technological innovation causes the Internet economy to change faster than most other sectors. Slow government rulemaking processes will not be able to keep up with this rapid evolution. Government rules will soon become out of date and may lock in obsolete technologies or business models. The critics have set the terms of the debate and have had a strong impact. While Congress has considered several bills to regulate the online collection and use of personal information, it has not come close to passing them into law.

---

10 Id. at 188 (“critics maintain that government action creates burdensome, inflexible regulation and that self-regulation remains the best solution to privacy problems”); Bert-Jaap Koops, Miriam Lips, Sjaak Nouwt, Corien Prins & Maurice Schellekens, Should Self-Regulation be the Starting Point 25 (manuscript on file with author) (“Government regulation is often regarded as cumbersome, time-consuming, and costly.”)

11 Strauss & Rogerson, supra note ___ at 181 (discussing those who believe that the “fast-changing” nature of the Internet makes it ill-suited to government regulation); id. at 189 (“Critics of the legislative approach in the United States generally worry that the legislative/regulatory process is too slow and bureaucratic to effectively govern the Internet and that regulations will become burdensome and unnecessary.”)

12 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 people increasingly use to access the Internet. Such rules will seriously constrain innovation and/or become obsolete as technologies and business practices change.

Some critics further claim that government control does not fit with the de-centered nature of the Internet economy which typically transcends national boundaries. Koops, et al., supra note ___, at 13 (discussing those who hold this view). This can render ineffective a single government’s attempt to regulate this arena.

13 See CRS 2006 Internet Privacy Report 18 (describing Internet privacy bills 109th Congress and concluding that while some such bills were introduced in the House and Senate, none have passed); CRS 2004 Internet Privacy Report 4 (concluding that “many Internet privacy bills were considered, but did not clear, the 107th and 108th Congresses).
regulation appears to face both conceptual and political challenges.

Others have raised serious concerns about the market and self-regulation. They assert that while firms may have an incentive to protect customer information, they have a conflicting incentive to collect and use this valuable data. This will lead companies to obscure their data practices and make it difficult for users to opt out of them. Others have raised serious concerns about the market and self-regulation. They assert that while firms may have an incentive to protect customer information, they have a conflicting incentive to collect and use this valuable data. This will lead companies to obscure their data practices and make it difficult for users to opt out of them.14 Section II.B.1 of this article describes empirical studies that support these concerns. Critics also raise other theoretical objections to the market approach. They note that, due to high transaction costs, most users do not read or understand the privacy notices at the Web sites they visit. This results in information asymmetries that prevent users from making sound market choices and renders the market in personal information highly imperfect.15

Commentators have been somewhat more sanguine about industry self-regulation. They note that, in theory at least, industry’s information costs should lower than government’s, and its decision-making processes faster.16 This should make it better able to design intelligent rules and to update them quickly.17 Thus, some have claimed that “self-regulation can turn out to be more efficient and flexible than legislation.”18 Yet theory also predicts that self-regulatory bodies, which serve the very firms they are supposed to be

14 Strauss & Rogerson, supra note ___, at 180 (the “lack of complete and clear privacy policies presents a problem for the laissez-faire approach.”)

15 Id. at 179 (“Critics question whether the theory of laissez-faire can actually work, especially if consumers do not have perfect information.”)

16 Koops, et al., supra note ___ at 12 (“with self-regulation, the process of setting the rules draws on the specific expertise of the actors involved. . . Given the absence of time-consuming formal procedures, it allows for easy adaptation to changing circumstances.”)

17 Strauss & Rogerson, supra note ___ at 181 (self-regulation “allow[s] industry experts and privacy specialists to tailor requirements” to the realities of the sector); Koops, et al., supra note ___ at 25 (“self-regulation is more flexible and therefore better suited for regular updating . . . self-regulation may also impose lower compliance costs on businesses because they themselves can better tailor the rules to their situation.”)

18 Id. at 12.
regulating, will often create lenient rules and to fail to enforce them effectively. Industry will do just enough to preserve customer trust and stave off government regulation while leaving itself maximum flexibility to collect and use valuable information. As Section II.B.2 will describe, experience to date bears out this prediction. Industry self-regulatory efforts have been plagued by inadequate standards, insufficient participation, lax enforcement and spotty compliance. In sum, the overall picture is not a bright one. Theory and experience suggest that both government regulation, and the market and industry self-regulation, possess significant weaknesses when it comes to protecting privacy online.

What to do? In recent years, European nations have developed a third approach to privacy protection. Drawing on a Dutch regulatory experiment from the 1980's, they have provided a way for government and industry to work together to create and enforce a set of privacy rules. Under the European model, the government passes a comprehensive data protection statute that sets broad, flexible, standards regarding the collection and use of personal information. However, government officials do not then pass regulations fleshing out these standards, as those accustomed to the American regulatory model might expect. Instead, they invite the relevant industry sector, acting through its trade association, to draft an industry “code of conduct” that interprets the statute and spells out how it applies to that sector. A government agency reviews the code to assess whether it in fact meets the statutory requirements. If it does, the agency formally approves it. It then deems compliance with the

---

19 Strauss & Rogerson, supra note ___ at 181 (critics maintain that “self-regulation still does not guarantee the quality of privacy policies and lacks effective enforcement mechanisms.”); Koops, et al., supra note ___, at 23 (“the key disadvantage of self-regulatory schemes is their lack of adequate enforcement.”)

20 For a full description of the European approach, and citation to supporting authorities, see infra Part IV.
code to constitute compliance with the statute. 21 This allows firms to follow a set of rules that their own peers have drafted (subject to government review and approval) and, in so doing, to comply with the law.

The European model is not self-regulation since the government retains an important role in reviewing and approving 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 represents a third form of governance known as “co-regulation” 22 (or “collaborative governance” as it is sometimes called in American academic writing.) 23 As used in the scholarly literature on regulatory governance, “co-regulation” encompasses those initiatives in which government and industry share responsibility for setting regulatory goals and/or for drafting and enforcing regulatory standards. 24 Some policymakers and scholars endorse co-regulation. They claim that it incorporates the flexibility and industry knowledge of self-regulation 25 while adding the

21 See infra notes ___-___ and accompanying text (describing this process).


24 See id. at 17 (June 2006) (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.”)

25 See, e.g. GUNNINGHAM & SINCLAIR, supra note ___-___ at104-105 (discussing these potential virtues of negotiated agreements); JOSEPH REES, REFORMING THE WORKPLACE: A STUDY OF SELF-REGULATION IN OCCUPATIONAL SAFETY (1988) (same); Freeman,
supervision and rigor of government rules. They see co-regulation as the best of both worlds – an adaptive, workable approach that can protect individual privacy while also keeping up with, and meeting the needs of, the growing Internet economy.

Others disagree. Critics of co-regulation assert that it lacks transparency and accountability as compared to traditional notice-and-comment rulemaking. They warn that the back-room discussions in which government and industry negotiate the terms of a code of conduct can result in favorable deals that sell short the public interest. 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.

Is co-regulation a useful, alternative approach to protecting online privacy, or does it produce rules that are too lenient? How have the European member states gone about implementing this approach? Have the European programs been a success? Should we consider co-regulation as a model for U.S. law and policy in the area of Internet privacy? These important questions have received surprisingly little attention in U.S. scholarly literature, and almost none in U.S. law reviews.

Collaborative Governance, supra note ___, at 21-33 (same).

 twenty GUNNINGHAM & SINCLAIR, supra note ____-____ at 107-108; Koops, et al., supra note ___, at 32 (“governments can play an important role in “raising awareness and in enhancing enforcement, so that self-regulatory rules are indeed followed in practice.”)

 twentyseven Strauss & Rogerson, supra note ___ 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 ___, at 3 (“Co-regulation should combine binding legislative and regulatory action with actions taken by the actors most concerned, drawing on their practical experience.”)

twentyeight GUNNINGHAM & SINCLAIR, supra note ____-____ at 105-106 (citing these concerns).

twentynine Id. at 105 (citing these concerns).
In 2010, I received a Fulbright Senior Professorship to study these and related questions and so to begin to fill this gap. My research program consists of five main steps: (1) identify the online threats to information privacy; (2) evaluate whether government regulation, or the market and self-regulation, are sufficient to address these threats; (3) survey the theoretical literature on the strengths and weaknesses of co-regulation; (4) analyze and evaluate the E.U. law that requires member states to implement the “code of conduct” approach, and the statutes and regulations through which these member states have done so; and (5) travel to an E.U. member state (the Netherlands) to evaluate its implementation of the co-regulatory, code of conduct approach to privacy regulation. This article is the first in a two-part series that will present my findings. It covers steps one through four. A later article will cover step five and will report the findings of my six-month field study of Dutch data protection codes of conduct.

The current article is structured as follows. Part I will show that the Internet generates serious, new threats to individual privacy. Part II will describe in more detail the arguments that critics have leveled against the government regulation and the market/self-regulation approaches, and will evaluate what experience to date has to tell us about these models. Part III will provide an introduction to co-regulation and will survey the theoretical literature regarding the strengths and weaknesses of this collaborative approach. Part IV will turn to the European experiment with data protection codes of conduct. It will describe and analyze the 1995 Data Protection Directive’s requirement that E.U. member states include this strategy in their privacy laws. It will then provide the first comprehensive analysis in a U.S. law review of the national laws that have implemented this co-regulatory approach. It will compare these laws to one another and so develop an original way of categorizing and understanding them. It will close with suggestions for further research about this important
area of privacy law and policy.

I. 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. This has produced many benefits. But it has also led to an unprecedented increase in the collection, aggregation and use of personal information, and so to new and profound challenges to information privacy. 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 and entering a search


31See FTC May 2000 Report 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.”)

32For example, Google, AOL or Yahoo!
query. The collection of their personal information begins here as well. Search engines collect and store every query that users make. In most cases, they are able to link these queries to the computer on which they were entered and so, as we shall see, to the user’s individual identity.

Search queries are often fairly innocuous. But they can also be highly personal. In 2006, a team at AOL released to academic researchers a database of 20 million search queries entered by 657,000 users over a three-month period. 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. 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 “catalogue of intentions, curiosity, anxieties and quotidian questions.”

Search engines store these queries and retain them for months, or even years. They are able to link them to the computer that sent them. Where the user of that computer has registered for one or more services, the search engines are then able to link the queries to

---


34 Barbaro & Zeller, supra note ___.

35 Id.

36 For example, free e-mail (e.g. G-mail) or free online storage space.
the individual person. This gives them the ability, should they choose to use it, to construct a
detailed map of a given users’ queries and so 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. Some even go beyond this, claiming 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.37 But even where the search engines
abide by this practice, it is an inadequate shield. Journalists who examined the AOL database
and reviewed the anonymized searches of one user (user No. 4417749) were able to piece
together sufficient information to identify her by name.38 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 that the search engines have tried to render anonymous – can often do
so as well.

2. Web sites

Having entered a query and received search engine results, the typical user clicks on
and enters one or more Web sites. The great majority of Web sites collect information about

37 Barbaro & Zeller, supra note ___.

38 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 qwinnett county
georgia.” Id. Based on these and other searches the journalists were able to identify her. Id.
the users who visit them. Some overtly request or require users to fill out registration, survey or order forms that ask for personally identifying information (PII)\textsuperscript{39} such as the user’s name, postal address, e-mail address, driver’s license number, or social security number. Many collect personal data more subtly through the use of “cookies,”\textsuperscript{40} and other technologies\textsuperscript{41} that unobtrusively track user activities and associate them with a particular computer or device.\textsuperscript{42} Through such technologies, Web sites are able to track and record which pages 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. As was mentioned above, many sites collect personally identifying information that they can

---

\textsuperscript{39}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 eighty-seven percent of the U.S. population based only on a 5-digit zip code, gender, and date of birth. Federal Trade Commission, \textit{FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising} 24 & n. 53 (Feb. 2009) [hereinafter, \textit{FTC 2009 Staff Report}].

\textsuperscript{40}A cookie is a small text file that the Web site places on the user’s hard drive when the user visits the site. \textit{FTC 2009 Staff Report} 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 put in her “shopping cart,” etc. The next time the user visits, 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”). Over time, the site owner is able to build up a picture of the particular user and how she has utilized the site. See supra notes \textsuperscript{39}-\textsuperscript{40} and accompanying text; \textit{FTC 2009 Staff Report} at 22; Federal Trade Commission, \textit{Online Profiling: A Report to Congress} 4 (June 2000) [hereinafter, \textit{FTC June 2000 Report}].

\textsuperscript{41}See \textit{FTC 2009 Staff Report} at 2, n.4 (describing “web bugs,” “web beacons” and “flash cookies.”)

\textsuperscript{42}\textit{Id.} at 2.
link to a specific computer or device, and so to cookie data associated with that computer.\textsuperscript{43} Indeed, in a 2000 survey, the Federal Trade Commission (FTC) found that “most” of the sites surveyed were able to do this.\textsuperscript{44} Moreover, user profiles have become so comprehensive (see the discussion of network advertising, below)\textsuperscript{45} that it is often possible infer a user’s identity without PII.\textsuperscript{46}

3. The Future: Internet Service Providers

If current trends are any indication, we may find our personal information collected without even having to enter a query or visit a Web site. Internet service providers – Microsoft, AOL, and others – are beginning to experiment with “deep packet inspection.”\textsuperscript{47}

\textsuperscript{43}See supra notes ___-___ and accompanying text.

\textsuperscript{44}“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.” FTC May 2000 Report at 10; see also FTC 1998 Report at 25.

\textsuperscript{45}See infra notes ___-___ and accompanying text (describing how network advertisers combine cookie data from many different Web sites into a single, highly detailed user profile).

\textsuperscript{46}FTC 2009 Staff Report at 22-23 (“when 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 2000 Report 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 profiles 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.” FTC June 2000 Report at 12.

This practice allows the ISP automatically to inspect the contents of data “packets” as they travel on the Internet in order to mine personal information from them.\textsuperscript{48} These packets could contain queries or Web sites. But they could equally contain e-mails or documents.\textsuperscript{49} 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 the Web sites themselves, network advertisers, data brokers, secondary users, and the government.

1. Web sites

Web sites use cookie data to improve the user’s experience at the site. For example, they enable a Web site to remember a username and password entered during a prior visit to the site, reconstitute the contents of a shopping cart on a return visit,\textsuperscript{50} or provide personalized news and weather or stock quotes.\textsuperscript{51} Many sites also use the information on past visits to predict which of the site’s services or products is most likely to appeal to the user,

\textsuperscript{48} Id.

\textsuperscript{49} Id.

\textsuperscript{50} FTC June 2000 Report at 8-9.

\textsuperscript{51} Id. at 9; FTC 2009 Staff Report at 1.
and to present the user with advertisements promoting those items.\textsuperscript{52}

2. Network advertisers

Frequently, however, the banner advertisement that a user sees when she visits a Web site is provided, not by the Web site itself, but by a “network advertiser.”\textsuperscript{53} These entities are the principal users of online personal data and their operations merit a more in-depth description. Network advertisers enter into contractual relationships with many different Web sites. In exchange for a payment, the Web sites agree to provide the network advertiser with user clickstream data that they collect and to allow the advertiser to display advertisements on their site. These arrangements allow a single network advertiser to collect user information from hundreds or thousands of different Web sites, and to see what a given user has done at each of these sites.\textsuperscript{54}

The network advertiser combines this information with other information that it has purchased about the user, e.g. 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.\textsuperscript{55} 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 his preferred travel destinations, medical conditions, political

\textsuperscript{52} This is known as “first party” advertising since the same Web site is both collecting the data and conveying the ad. \textit{Id.} at iii, 26.

\textsuperscript{53} See generally FTC June 2000 Report at 3.

\textsuperscript{54} FTC 2009 Staff Report at 3 & n.5.

\textsuperscript{55} FTC June 2000 Report at 5.
commitments, intellectual interests and sexual preferences or fantasies. Moreover, as was explained above, it is often possible to tie the profile to an identified user, either because the user at one point provided her 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.

Network advertisers employ the behavioral profiles to make inferences about the user’s “tastes, needs and purchasing habits” and so to select specific banner ads to provide to that user. They deliver these ads in conjunction with the networked Web sites. When a user visits such a site, the site automatically contacts the network advertiser and requests advertising content. 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. When the web page 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. He just knows that he requested a web page and received both the content and ads. In 2000, the FTC estimated

---

56 Id at 5-6.

57 See supra notes ___-___ and accompanying text.; FTC May 2000 Report at 9, n. 53.


59 An example may help to illustrate the phenomenon. See FTC 2009 Staff Report at 3 (I have made only minor changes to the FTC’s example). Assume that a user visits the Web site of the Washington Post, a network member, and reads an article about the Washington Nationals 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 Web site, 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 Web site 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
that network advertisers had served tens of billions of banner ads to users.\textsuperscript{60} That number has increased substantially over the past decade.\textsuperscript{61}

This practice has its benefits. It raises the probability that people will receive ads about goods and services that may actually be interested in.\textsuperscript{62} This saves these individuals from having to wade through ads that hold no interest for them. It also makes businesses advertising efforts far more efficient.\textsuperscript{63} Yet network advertising has also led to the creation of “behavioral profiles” that chronicle our deepest desires, anxieties and beliefs, and that are traceable directly to us.\textsuperscript{64} This creates “a portrait that is quite comprehensive and, to many, inherently intrusive.”\textsuperscript{65} In this respect, network advertising significantly damages the privacy

\textsuperscript{60}FTC June 2000 Report at 3.

\textsuperscript{61}Indeed, between 2002 and 2006 online advertising revenue nearly tripled, growing from $6 billion to $16.6 billion. FTC 2009 Staff Report at 8; Ryan Blitstein, Microsoft, Google, Yahoo in Online Ad War, SAN JOSE MERCURY NEWS, May 19, 2007.

\textsuperscript{62}FTC June 2000 Report at 9; FTC 2009 Staff Report at i, 31.

\textsuperscript{63}FTC June 2000 Report at 9.

\textsuperscript{64}The future looks even bleaker. As was mentioned above, the most recent trend does not even depend on Web site cookies. Instead, internet service providers (ISPs) such as Microsoft or AOL are beginning to collect clickstream data by analyzing the packets of information that a given user sends and receives on the Internet. 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. It promises to yield behavioral profiles that are even more comprehensive and invasive. See FTC 2009 Staff Report at 16 n. 40. BNA Privacy and Security Law Vol. 8 at 217-220. Hearing before Telecommunications Subcommittee (July 17, 2008), What your Broadband Provider Knows About your Web Use: Deep Packet Inspection and Communication laws and Policies, \textit{http://energycommerce.house.gov/cmte_mtgts/110-ti-hrg.071708.DeepPacket.shtml}.

\textsuperscript{65}FTC June 2000 Report at 12.
of Web users.\textsuperscript{66}

3. Data brokers

In addition to using it themselves, Web sites and network advertisers sometimes sell personal information that they have collected to data brokers.\textsuperscript{67} These companies specialize in pulling together and analyzing personal information gleaned from many different sources, including public records, the media, credit reporting agencies and other sources.\textsuperscript{68} Increasingly, they have been combining this “offline” data, traceable to specific individuals, with online data that they can match to those same individuals.\textsuperscript{69} This 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. This increases the risk to privacy by an order of magnitude. 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.\textsuperscript{70}

\begin{itemize}
\item \textsuperscript{66} In addition, some argue 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.
\item \textsuperscript{67} FTC June 2000 Report at 5.
\item \textsuperscript{69} FTC June 2000 Report at 5.
\item \textsuperscript{70} \textit{Id.} at 12.
\end{itemize}
4. Secondary users

We know that Web sites and network advertisers use the information they collect in order to better serve, and better market to, Web users. But what about the data brokers and others to whom they sell this information? How do they use it?

Recently, the FTC surveyed Web sites regarding their collection and use of personal information. The survey also asked about these “secondary” uses, i.e. use by entities other than the one that collects it. The Web sites were quite forthcoming about their own collection and use of the data. However, they provided almost no information about secondary uses. 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. Instead, the Web sites must be unwilling to disclose such uses because they fear that they would alarm the regulators and the public. Anyone who cares about protecting privacy and personal information should be keen to learn more about this practice.

Preliminary information suggests that secondary uses are a cause for concern. Some businesses are using the information to engage in “Weblining”–the practice of charging higher prices to some consumers based on their online profiles. In one particular manifestation of this practice, life insurance companies are using the information to decide how to price policies for specific individuals, or even whether to offer them a policy at all. This is especially invasive where the information in question involves medical conditions. Similarly, banks are using it to decide whether to offer loans, including home mortgages, and
how to price them. 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 are also using the information to help them decide who to interview and hire. This is a particularly vexing secondary use. A person 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 in terms of choosing future employees. However, few would ask for it 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 knowing about it. Many would find this to be serious, and consequential, invasion of personal privacy.

5. The Government

The most significant privacy issue, however, may be the possibility that online companies could share the information with the government. There is precedent for this. In a number of well-publicized instances government officials have requested that ISPs provide, and in some cases have issued subpoenas for, the identity that lies behind an e-mail or Internet Protocol address. Under the same theory, government officials could subpoena information about a given user’s Internet queries and Web travels. Suspected criminals, terrorists, or simply citizens who actively oppose the views of those in power, could find their daily activities and personal qualities monitored to an extent that goes beyond what even a wiretap placed on their phone would reveal – and all without the issuance of a warrant. This

---

7Id. at 13.
is an unwelcome prospect in a democracy.

II. The 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 is far less agreement on how to go about dealing with this problem. As was mentioned above, the main voices in the current debate can be distilled into two main camps: those who favor detailed government regulation, and those who prefer the market and industry self-regulation. 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 prevent private firms from taking adequate steps to protect online privacy. They assert that the legislature should take a strong hand in protecting this important societal value. They call for legislation that would set specific


\[^{73}\text{Strauss & Rogerson, supra note \---, at 188 ("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.").}

22
limits on the online collection of personal information and on the distribution and use of that information. Following the typical American regulatory model, these proponents envision this law taking shape in two stages. First, Congress would pass a sweeping and rigorous statute. Then a regulatory agency such as the Federal Trade Commission would develop detailed regulations implementing this legal framework.

Legislators have introduced several such bills in the House and/or Senate although neither chamber has come close to passing any of them. Some of the bills provide for broad regulation of the Internet sector. Others focus more on Web sites and network advertising. On May 4, 2010, Representatives Boucher (D-Va.) and Stearns (R-Fla.) released a “Staff Discussion Draft” of the latter, narrower kind of bill. It provides an example of what government regulation of this type might look like were it ever enacted into law. The bill would require Web sites and network advertisers, among others, to provide users with “clear and conspicuous” notice of how they collect, use, store and share their personal information. It would mandate that they provide users with meaningful choice (opt-out) about whether to

---

74 See Congressional Research Service, CRS Report for Congress, Internet Privacy: Overview and Pending Legislation 4 (Dec. 22, 2004) (concluding that “many Internet privacy bills were considered, but did not clear, the 107th and 108th Congresses) [hereinafter, CRS 2004 Internet Privacy Report]; Congressional Research Service, CRS Report for Congress, Internet Privacy: Overview and Legislation in the 109th Congress, 1st Session 5, 18 (Jan. 26, 2006) (describing Internet privacy bills 109th Congress and concluding that while some such bills were introduced in the House and Senate, none have passed) [hereinafter, CRS 2006 Internet Privacy Report].

allow these practices.\textsuperscript{76} Moreover, it would require them to obtain affirmative consent (opt-in) before collecting or using “sensitive information” (i.e. medical, financial, race, sexual orientation, precise location)\textsuperscript{77} or sharing any personal information with unaffiliated third parties.\textsuperscript{78} Finally, it would require Web sites and network advertisers to take reasonable and appropriate steps to ensure the accuracy and security of personal data that they collect and use.\textsuperscript{79} Importantly for the present purposes, the bill would delegate to the Federal Trade Commission the authority to “issue such regulations as it determines to be necessary to carry out this Act”\textsuperscript{80} and would give it the power to issue penalties to enforce the Act’s requirements.\textsuperscript{81} It would further give state Attorneys General the authority to bring civil actions on behalf of the citizens of their state to enforce the Act.\textsuperscript{82} The bill does not provide for industry codes of conduct or any other form of co-regulation. Were Congress to enact it and the FTC to issue implementing regulations, it would likely constitute the kind of detailed government regulation that proponents of this approach have called for.

Within days, industry and pro-market groups expressed opposition to the Boucher-Stearns bill. Some maintained that the bill would impose excessive costs on Internet-based


\textsuperscript{77}Id. § 2(10) (defining “sensitive information”); § 3(c) (requiring opt-in consent).

\textsuperscript{78}Id. § 3(b).

\textsuperscript{79}Id. § 4(a), (b).

\textsuperscript{80}Id. § 8(a)(3).

\textsuperscript{81}Id. § 8(a)(1),(2).

\textsuperscript{82}Id. § 8(b).
businesses that are still trying to recover from the 2008 recession.\textsuperscript{83} Others went farther, complaining that “by mandating a hodge-podge of restrictive regulatory defaults, policymakers could unintentionally devastate the free Internet as we know it . . . raise prices, quash innovation.”\textsuperscript{84} Still others claimed that the bill perpetuated a failed belief that “Congress and regulators . . . know how to deliver privacy better than markets. We know they don’t. But they still think they do.”\textsuperscript{85} The general assessment is that the Boucher-Stearns bill, like the legislative proposals that preceded it, will face an uphill battle in becoming law.\textsuperscript{86}

The reactions to the Boucher-Stearns bill sound many of the themes that critics 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.\textsuperscript{87} They assert that government officials, who know little


\textsuperscript{86} Ingram, \textit{supra} note ___ (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, \textit{supra} note ___.

\textsuperscript{87} \textit{See Keith Perrine, The Persuader, INDUSTRY STANDARD}, Nov. 13, 2000 (discussing this criticism); Koops, et al., \textit{supra} note ___, at 1 (discussing those who “complain . . . about the lack of flexibility in legislatino and are skeptical about the feasibility of efficient and adequate ICT regulation by means of legislation.”)
about the industries they are regulating, will impose impractical and costly requirements that will seriously undermine business competitiveness. The critics highlight the fast-changing nature of Internet technologies and business models. They argue that the government regulators who will inevitably implement the legislation will not be able to keep pace with these changes and that the rules they create will quickly become out of date and ill-suited to their intended purpose. These arguments have had a strong impact. As was already mentioned, the House and Senate have considered various Internet privacy bills in recent years but have not passed them into law.

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.

---

88 Strauss & Rogerson, supra note ___, at 188 (“critics maintain that government action creates burdensome, inflexible regulation and that self-regulation remains the best solution to privacy problems.”

89 See Id. at 181 (discussing those who believe that the “fast-changing” nature of the Internet makes it ill-suited to government regulation).

90 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 and/or become obsolete as technologies and business practices change.

91 See CRS 2006 Internet Privacy Report 18 (describing Internet privacy bills 109th Congress and concluding that while some such bills were introduced in the House and Senate, none have passed); CRS 2004 Internet Privacy Report 4 (concluding that “many Internet privacy bills were considered, but did not clear, the 107th and 108th Congresses).
1. Leave it to the Market

Those who favor a market solution argue that individual firms will enhance their competitive position by responding to customer preferences for greater privacy. It follows that market forces will themselves lead to a more privacy-friendly Web. Insofar as customers are not requiring Web sites and other Web-based firms to do this, it is because they value the services they are receiving more than the privacy they are losing. As far as these commentators are concerned the market, left to its own devices, will arrive at the optimal level of privacy protection. Regulation will only interfere with, and distort, this outcome.

Those who object to this view focus on information asymmetries. Web users often are not aware of the collection of their personal information online, much of which occurs instantaneously and invisibly. Even where they are aware of it, they 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. These information gaps prevent users from expressing their true preferences for privacy protection and so can prevent


93Strauss & Rogerson, supra note ___, at 179 (discussing this criticism).
the market from responding to this desire. In short, the market for online privacy is characterized by highly imperfect and asymmetrical information. This leads firms to collect and use far more personal data than they would in a hypothetical perfect market.

Other critics focus on actual market experience. They reason that, if the laissez-faire theory were correct, we should expect to see the market providing meaningful privacy protections. The empirical data, however, suggests otherwise. To measure this observers rely on the Fair Information Practice Principles (FIPPs). First developed by the Department of Health, Education and Welfare in 1973, the FIPPs have become an internationally-accepted standard for what constitutes adequate privacy protection. They require those who collect and use personal information to provide:

“(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 context 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.”

Not surprisingly, these criteria correspond to some of the essential pre-conditions that must be met for users to make informed market choices. They are therefore a good benchmark to

---


96 FTC May 2000 Report.

97 Strauss & Rogerson, supra note ___, at 181 (“enforcing fair information practices is the best way to harness market forces, because these practices ensure that consumers have the
evaluate the functioning of the market in online privacy.

In 2000, the Federal Trade Commission surveyed the busiest U.S. commercial Web sites in order “to assess industry’s progress in protecting consumer privacy online.”\textsuperscript{98} It identified the percentage of Web sites that collected personally identifying information and the percentage that provided privacy disclosures to their users. For those sites that did provide such a disclosure (privacy policy), the FTC assessed how the site’s privacy policy compared with the Fair Information Practice Principles. The FTC found that while the great majority of the busiest Web sites collect personal information\textsuperscript{99} nearly forty percent posted no privacy policy. Of those that did, the policy did not meet the minimum Fair Information Practices standards in the majority of cases.\textsuperscript{100} Probing further, the FTC evaluated the content of the privacy policies and found that many used contradictory language,\textsuperscript{101} buried exceptions deep in the fine print of a firm’s privacy policy,\textsuperscript{102} provided ambiguous or

\textsuperscript{98}FTC, June 2000 Report, at 7.

\textsuperscript{99}The Commission found that ninety-seven percent of the sites collect an e-mail address or some other type of personal identifying information. FTC May 2000 Report, at 9. A widely-cited Georgetown University study confirms these results, finding that, in 1999, only ten percent of sites provided disclosures that touch on all four fair information practice principles. Mary Culnan, \textit{Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission} (June 1999). Moreover, there is a ninety-nine percent chance that a user surfing the busiest Web sites will, over the course of a one-month period, visit a site that collects personally identifying information. FTC May 2000 Report, at 9.

\textsuperscript{100}Only one in five implemented all four information practices to some degree. FTC Only forty-one percent met the notice and choice standards. \textit{Id.} at 35.

\textsuperscript{101}\textit{Id.} at 24

\textsuperscript{102}\textit{Id.} at 25. It is difficult for users to read through these lengthy documents, especially if they are visiting multiple Web sites in rapid succession, and few take the time to do so. Center for Democracy and Technology, \textit{supra} note \_, at 4; Alecia M. McDonald and Lorrie Faith Cranor, \textit{The Cost of Reading Privacy Policies} (Sept. 2008).
misleading statements about the way in which the site handled user “choice,” and reserved the right to change policies without notice. The FTC survey suggests that many Web sites, even those that post privacy policies, do not comply with the Fair Information Practices or, if they do, “comply” in confusing or inaccessible ways. No one has updated the FTC’s 2000 report. However, more recent assessments suggest that while more Web sites now post privacy policies, these documents remain inaccessible and hard to understand. Given the high profits associated with the collection, use and sale of personal information, and the transaction costs and information asymmetries that distort the market, these findings are not surprising.

104 Id. at 26.
105 Alessandro Acquisti, Janice Tsai, Serge Egelman, & Lorrie Cranor, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Carnegie Mellon University (2007) (recent literature concludes that many privacy policies are inaccessible and hard to understand).
106 Could it be that Web users really do not value protection of their personal information, and that is why the Web sites are not providing it? Studies of user preferences suggest not. In a Business Week survey, eighty-nine percent 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 at 15. Sixty-three percent expressed discomfort even if their profiles were not linked to their name or identity. Id.; see also FTC 2009 Staff Report at 24 & n. 52. According to other, reputable surveys, ninety-two percent of respondents were uncomfortable with the idea that Web sites would share their information with others, and ninety-three percent expressed discomfort with the notion that Web sites would sell this information. FTC June 2000 Report at 16. Second, the FTC’s survey results are now over ten years old, a long time in the life of the Web. Are they still relevant?
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. However, they assert that this should be achieved through industry self-regulation rather than through direct government regulation.¹⁰⁷ For these purposes, we define self-regulation as a regulatory system in which business representatives define and enforce standards for their sector with little or no government involvement.¹⁰⁸

Proponents argue that self-regulation will institute protective standards while avoiding the pitfalls of government legislation. They point out that industry members know their operations and business plans better than anyone else and so are uniquely positioned to identify the most effective and efficient means of protecting public values such as privacy.¹⁰⁹ This 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, they contend that industry members will be better able to predict future technologies and business developments and so will be more able to design standards that can accommodate these

¹⁰⁷ See CRS 2006 Internet Privacy Report (describing advocates of self-regulation); Strauss & Rogerson, supra note ___, at 181 (“the federal government, industry members, and private associations have touted self-regulation as the answer to privacy concerns.”)

¹⁰⁸ See Koops, et al., supra note ___, at 1 (“self-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”); REES, supra note ___, at 9 (in self-regulation “rulemaking and enforcement are both carried out privately.”); GUNNINGHAM & SINCLAIR, supra note ___, 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.”)

¹⁰⁹ Koops, et al., supra note ___, at 25.
inevitable changes. Thus, self-regulation will remain more relevant and workable than government-imposed standards. Finally, they contend that industry members will be more likely to accept rules designed and imposed by their peers. They will comply more readily with such rules and will spend less time and energy resisting them.

While this sounds like a rosy picture indeed, some believe that it is more the world as seen through rose-tinted glasses. These critics of self-regulation maintain that firms will always put their own profits ahead of the public interest and that self-regulatory standards will inevitably prove to be too lenient. They also question whether industry representatives, who do not hold governmental power to fine or otherwise penalize scofflaws, will have sufficient power or incentive to enforce industry standards against their peers.

Third, critics assert that self-regulatory processes are lacking in transparency when compared to traditional rulemaking. Finally, these critics worry that, in the absence of sanctions for those who do not participate, many firms will stand aside, let their competitors institute costly, self-regulatory standards, and free-ride on the sector’s improved reputation for protecting privacy. As was mentioned above, many of these critics call for government legislation instead of self-regulation.

The federal government has largely embraced self-regulation as the means to protect

\(^{110}\) Id.

\(^{111}\) See Electronic Privacy Information Center, Privacy Self-Regulation: A Decade of Disappointment (Marcy 4, 2005).

\(^{112}\) Koops, et al., supra note __, at 23; Strauss & Rogerson, supra note __, at 183.

\(^{113}\) Koops, et al., supra note __, at 24.

\(^{114}\) Gunningham & Sinclair, supra note __, at 107.

\(^{115}\) See CRS 2006 Internet Privacy Report 4 (describing those who “believe self-regulation is insufficient” and instead call for legislation).
Internet privacy. As early as 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 whenever appropriate.” The Federal Trade Commission, the agency with the greatest responsibility for and voice in privacy regulation, has also favored self-regulation. For example, in the late 1990’s, 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” and that “[t]he Commissions’s goal has been to encourage and facilitate effective self-regulation.” Following a brief period during which the FTC appeared to lose faith in industry efforts and began to call for legislation, the Commission returned to its endorsement of self-regulation. Industry has responded by launching two initiatives to govern privacy on the Internet. They allow us see how self-regulation has worked in practice in the field of online privacy. The results are not encouraging.

116 See CRS 2004 Internet Privacy Report 1 (“many in Congress and in the Clinton Administration preferred industry self-regulation”).

117 Bill Clinton, Presidential Directive on E-Commerce (July 1, 1997).


119 FTC, June 1998 Report, at i.

120 FTC, May 2000 Report at 36.

121 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 at 47. This report omitted any mention of the need for federal legislation.
a. The Online Privacy Alliance

In 1998, the FTC called strongly for industry self-regulation of online privacy and threatened that, if it were not forthcoming, the government would move towards direct regulation. The Online Privacy Alliance (OPA), a group that leading Internet firms had formed in the mid-1990s, responded by issuing a set of Guidelines for Online Privacy Policies. 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, to allow users “opt-out” choice with respect to those uses, and to institute measures that would assure data security and reliability and allow users to correct inaccurate data.

The Guidelines were not a success. They failed to prohibit the collection of sensitive data or to protect against harmful uses of data by anything other than an “opt-out” policy. Privacy expert Robert Gellman complained that “it can’t be the case that if a customer doesn’t object, you can do anything.” The OPA also failed to identify a process for enforcing the guidelines against members that failed to follow it. Finally, and most

---

122 Brian McWilliams, *Alliance Aims to Beat FTC to the Online-Privacy Punch*, CNN.com (July 23, 1998).

123 America Online, 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.” Online Privacy Alliance, Frequently Asked Questions, [http://www.privacyalliance.org/facts](http://www.privacyalliance.org/facts).


125 *Id.*


127 *Id.*
significantly, the organization proved unable to recruit and retain a critical mass of key industry players. Only a hundred or so companies ultimately joined the group, with significant firms such as Amazon.com and Lycos choosing not to participate at all. With narrow coverage of this sort, the OPA could hardly represent 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. The OPA has since ceased to exist.

b. The Network Advertising Initiative

The second self-regulatory initiative, the Network Advertising Initiative, followed soon thereafter. Like the OPA, the NAI set up an organization and required members to uphold certain privacy principles. However, rather than seek to include a broad array of Web-based firms as the OPA had done, the NAI focused exclusively on the network advertising industry.

The NAI appears to owe its beginnings both to the failure of the OPA and to the controversy that erupted when 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 catalogue purchasing records covering over 80 million households. This


\[129\] Id.

\[130\] See supra notes ____-____ for a description of online behavioral advertising, also called “network advertising.”

\[131\] Doubleclick, Inc. and Abacus Direct Corporation to Merge in $1 Billion Stock
plan to merge online and offline data, and to link it to specific, named individuals,\textsuperscript{132} provoked protest\textsuperscript{133} as well as investigations by the FTC and the Michigan Attorney General’s Office.\textsuperscript{134} Doubleclick temporarily shelved its plans.\textsuperscript{135} Shortly thereafter, the Network Advertising Initiative came into existence and announced a set of “Self-Regulatory Principles for Online Preference Marketing By Network Advertisers.”\textsuperscript{136}

As might be expected, the 2000 NAI Principles focus on the merger of non-personally identifiable information (Non-PII), such as the clickstream data that network advertisers collect, and personally identifiable information (PII), such as the offline purchasing data that Abacus Direct had collected. The Principles draw a line between clickstream data collected prior to the publication of the Principles, and that collected after publication. They require network advertising firms to get specific consent (“opt-in” consent) before combining pre-publication clickstream data with PII\textsuperscript{137} but require that they provide users only with notice and an opportunity to opt out of combining of their post-publication clickstream data with


\textsuperscript{132}Hiawatha Bray, \textit{DoubleClick Backs Off on Net Data, Bows to Protests on Use of Personal Information}, \textit{The Boston Globe}, March 3, 2000 at C1; Chris O’Brien, \textit{DoubleClick Looks to Regain Surfers’ Trust}, \textit{San Jose Mercury News}, February 27, 2000, Sunday Morning Final Edition at 1D.

\textsuperscript{133}Miller, \textit{supra} note \textsuperscript{132}.

\textsuperscript{134}Bray, \textit{supra} note \textsuperscript{132}.

\textsuperscript{135}Miller, \textit{supra} note \textsuperscript{132}. DoubleClick does not appear to have ever followed through on the plan.


\textsuperscript{137}\textit{Id.} at 1.
Going forward, then, the Principles allow the merger of clickstream data and PII unless the user accesses a Web site’s privacy policy, reads and understands it, and affirmatively opts out of such merger. Moreover, they place no limits on secondary use of the information so long as individual has notice and an opportunity to opt out. This would appear to place a large burden on the individual user.

The Principles also required NAI members to post privacy policies that give users notice that they will be collecting their personal information and, with respect to PII at least, explain how the information would be used and/or distributed to third parties. This requirement would appear to satisfy the Fair Information Practices requirements of “notice” and “choice.” However, as the FTC’s survey demonstrated, users often fail to read the full privacy policy and, even when they do, frequently do not understand it.

---

138 Id. (the Principles phrase 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.”

139 Id. at 1 (the Principles phrase 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. NAI 2000 Principles, supra note ___, at 3 (defining “sensitive” PII as personally identifiable information about “medical or financial data, sexual behavior or sexual orientation, [and] social security numbers.”)

140 See supra notes ___-___ and accompanying text.

141 Center for Democracy and Technology, supra note ___, at 4; Alecia M. McDonald and Lorrie Faith Cranor, The Cost of Reading Privacy Policies (Sept. 2008).

142 FTC May 2000 Report 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 it with numerous other parties such as “business partners, sponsors and other third parties.” Id. at 25.
As the critics of self-regulation might have predicted, the NAI faced its biggest challenges in the realms of compliance and enforcement. The 2000 Principles represented that a third-party (later deemed to be TRUSTe, the privacy seal organization) would enforce the Principles through random audits and investigation of consumer complaints. The NAI further promised to sanction members determined to be out of compliance by revoking their NAI membership and/or notifying the FTC and the public. As time passed, it became increasingly clear that the NAI would not follow through on these commitments.

To begin with, by 2003 membership in the organization had fallen from twelve companies to two. Enforcement followed a similar trajectory. TRUSTe began by reporting user complaints in its online “Watchdog Reports” and by specifying the number, nature and resolution of these complaints. Between 2003-2005, however, it ceased providing the number and description of complaints filed, reporting only the number of complaints that had

---

143 See supra notes ___-___ and accompanying text.

144 See generally www.TRUSTe.org (last visited May 1, 2009); see Dixon, supra note ___, at 32-33 (NAI selects TRUSTe as third-party enforcement organization).

145 NAI 2000 Principles, supra note ___, at 12.

146 Id. at 12. The document does not specify which sanctions will follow which violations. EPIC, Principles, Not Privacy, supra note ___. In addition, the Principles neither provide individuals with a mechanism to follow up their complaints, nor specify a remedy for their injuries. EPIC, Principles, Not Privacy, supra note ___.

147 These initial members represented over ninety percent of industry revenue and ads served. FTC July 2000 Report at 10.

148 Dixon, supra note ___, 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 30. Associate members soon outnumbered full members.

149 Id. at 35. The Watchdog Web site is still available at See https://www.truste.org/consumers/compliance.php#c1 (describing Watchdog process) (last visited April 29, 2009).
been resolved. During this time, TRUSTe itself became an associate member of the NAI for a year. This directly conflicted with the NAI’s earlier statements that the enforcement entity would be completely “independent.” Finally, in 2006, TRUSTe simply stopped reporting on NAI complaints as separate, identifiable category. There is no evidence that TRUSTe ever conducted random audits of members as the Principles required it to do. According to one commentator, TRUSTe’s enforcement was “neither independent nor transparent” and so failed to serve as an effective measure of the NAI Principles’ value.

Acknowledging the flaws in its original effort, the NAI published revised Principles in 2008. While the new Principles contain several improvements they appear to have

150 Id. at 30.

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

152 Id. at 30.

153 Id. at 39. The FTC, too, appears to have been less than pleased. Initially, the FTC expressed some optimism about the NAI principles, “commend[ing] the member companies “for the innovative aspects of their proposal and for their willingness to adopt and follow these self-regulatory principle. FTC July 2000 Report at 9. Even at that point, however, the Commission was not ready to 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. 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 improvement, the Commission released a set of “Guidelines” for how to design acceptable self-regulatory principles. See http://www.ftc.gov/os/2007/12/P859900stmt.pdf; FTC 2009 Staff Report at 1, 45 (describing proposal). Taking the hint, the NAI in 2008 released a revised set of Principles.


155 The NAI allowed members of the public to comment on the 2008 Principles, and provided an expanded definition of “sensitive information.” See Center for Democracy and Technology, Response to the 2008 NAI Principles: The Network Advertising Initiative’s Self-Regulatory Code of Conduct for Online Behavioral Advertising 2-3 (Dec. 16, 2008). The organization also promised (again) to publish its enforcement data. See
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.\(^{156}\) This is a clear conflict of interest that may well repeat the enforcement failings of the initial effort.

The past decade of self-regulation has not been encouraging. 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 tend to 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.\(^{157}\)

III. Is Co-Regulation a Viable Alternative?

The market has a blind spot with respect to online privacy\(^ {158}\) and self-regulation is not working.\(^ {159}\) Detailed government regulation, too, may not be well-suited to this fast-moving, disorganized technological environment.\(^ {160}\) Ideally, a workable regulatory scheme would strike a balance between market self-regulation and some governmental oversight, but there is little indication that the existing regulatory landscape is capable of achieving that goal.

---


\(^{157}\)See supra notes ____-____ and accompanying text.

\(^{158}\)See supra notes ____-____ and accompanying text.

\(^{159}\)See supra notes ____-____ and accompanying text.
complex part of the economy and, in any event, faces major political obstacles.\textsuperscript{160} In the meantime, Web-based firms are collecting and storing more and more personal information with every passing day.

Co-regulation is a third approach that has the potential to combine the strengths of the first two.\textsuperscript{161} Yet not enough is known about how this method would fare with respect to the protection of information privacy. This Part will begin to fill this gap. It will provide a general introduction to co-regulation and explain how it might be employed to protect online privacy. In so doing, it will examine proponents’ claims about co-regulation’s virtues, and critics’ concerns about its potential weaknesses. Part IV will begin to analyze the most prominent real-world experience with a co-regulatory approach to data protection – the European experiment with industry codes of conduct. It will analyze the national laws that provide for industry codes of conduct and so provide insight into how the Europeans have implemented this initiative.

A. What is Co-regulation?

Co-regulation may be distinguished from governmental and self-regulation by looking at who sets and enforces regulatory goals and standards.\textsuperscript{162} 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

\textsuperscript{160}See supra notes ___-___ and accompanying text.

\textsuperscript{161}See supra notes ___-___ and accompanying text.

\textsuperscript{162}See REES, supra note ___, at 9 (regulation consists of setting rules and enforcing them and types of regulation may be defined in terms of who performs these functions).
parties share responsibility. They may split 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 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. Most co-regulatory programs include some joint endeavor of this sort. In addition to the term “co-regulation,” scholars have referred to such initiatives as “collaborative governance” or “contractual regulation.”

Co-regulation is no stranger to the administrative state. In negotiated rulemaking (reg-neg), agency representatives and stakeholders negotiate consensus-based rules. The Environmental Protection Agencies’ Brownfields and Habitat Conservation programs involve negotiated, site-specific compliance arrangements that fit the circumstances of particular firms or parcels of property. Various agencies draw on industry standards for safety or product standards and, if they measure up to agency review, incorporate them into

---

163 See Bredow Institut Report, supra note ___, at 17 (June 2006) (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.”)

164 See Freeman, Collaborative Governance, supra note ___.

165 See Richard B. Stewart, A New Generation of Environmental Regulation?, 29 CAP. L. REV. 21, 63, 80 (2001) (using the terms “micro-contracts” and “macro-contracts”).

166 Jody Freeman, The Private Role in Public Governance, 75 NYU L. REV. 543, 547 (2000) [hereinafter Freeman, Private Role].


168 See Stewart, supra note ___, at 68-80; Freeman, Collaborative Governance, supra note ___ at 657-664.
The California Occupational Health and Safety Administration (CAL-OSHA) 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. Each of these initiatives involves some type of collaborative government-industry effort either in the setting of goals, the formulation of standards and rules, and/or the enforcement of these rules. This 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. 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. This should yield goals that are more realistic and rules and standards that are

---

169 Freeman, Collaborative Governance, supra note ___ at 638-640. 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. However, it first offers the broadcasting and movie industries a chance to develop “voluntary standards.” If the FCC finds these to be acceptable, it is to use them instead of developing its own. Telecommunications Act of 1996, Public Law 104-104, § 551.

170 See Freeman, Collaborative Governance, supra note ___ at 651-53.

171 Gunningham & Sinclair, supra note ____, at 97 (“assumption that industry knows best how to abate its own environmental problems.”)

more cost-effective,\textsuperscript{173} workable,\textsuperscript{174} and adaptive to changing business realities,\textsuperscript{175} than those that government would be able to set on its own.\textsuperscript{176} It should also give regulated businesses more of a sense of ownership over the rules that govern them so that they comply more readily with these requirements and resist them less.\textsuperscript{177} This will reduce the delays and administrative costs associated with industry challenges to government regulation.\textsuperscript{178} These features should also make co-regulation more politically feasible than direct government requirements.\textsuperscript{179}

For proponents, co-regulation also promises advantages that self-regulation does not. There is an extensive literature on this and it is worth summarizing here. According to those who endorse co-regulation, government officials will push business to prioritize public goals over their own interests. Moreover, by bringing to government and business together in a collaborative enterprise co-regulation should also 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.\textsuperscript{180} Proponents further argue that government and industry working together should be able to come up with more creative

\textsuperscript{173}GUNNINGHAM & SINCLAIR, supra note ___, at 104; JOHNSON, supra note ___, at 240.

\textsuperscript{174}Freeman, Collaborative Governance, supra note ___, at 26;

\textsuperscript{175}\textit{Id.}; JOHNSON, supra note ___, at 236, 240; Stewart, supra note ___, at 82-83.

\textsuperscript{176}SCRUGGS, supra note ___, at 152 (cooperative approaches can create “a regime where flexible, cost-effective implementation of high standards can occur.”)

\textsuperscript{177}\textit{Id.} at 146.

\textsuperscript{178}GUNNINGHAM & SINCLAIR, supra note ___, at 104.

\textsuperscript{179}\textit{Id.} at 109.

\textsuperscript{180}Freeman, Collaborative Governance, supra note ___, at 22-24; SCRUGGS, supra note ___, at 143.
solutions to social problems than either party could on its own. They believe that parties that have engaged in a collaborative process will feel accountable to each other, adding a layer of shared responsibility that would not exist under a pure governmental approach. They claim that, due to these various advantages, collaborative governance will ultimately yield better social performance than direct government regulation. If these claims are correct, then co-regulation may be able to address some of shortcomings of the market, self-regulation and government rules. This would make it well worth considering as a potential alternative or supplement to these other mechanisms for protecting privacy on the Internet.

However, others are more skeptical of co-regulation. Their arguments, too, deserve attention. Privacy advocates argue that industry will not reveal insider knowledge to regulators but will instead use its informational superiority to obtain weaker standards. They assert that the public has fewer opportunities to participate in co-regulatory initiatives than in traditional rulemaking, leading to less creativity, not more. They further point out that collaborative discussions often take place outside of the public eye and worry that this can facilitate agency “capture” – the situation where industry representatives become too

---

181 Id. at 22-24
182 Id. at 22; SCRUGGS, supra note ___, at 144, 148.
183 Id. 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); REES, supra note ___, 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).
184 GUNNINGHAM & SINCLAIR, supra note ___, at 105.
185 SCRUGGS, supra note ___, at 135, 139 (discussing critics’ argument that the public has fewer opportunities to participate in co-regulation than in traditional rulemaking).
cozy with their government regulators and lead them to sell short the public interest. They question whether business representatives will enforce the rules vigorously and suggest that, in the absence of such enforcement, some firms will free-ride on the efforts of others. They argue that established firms may use collaborative negotiations to establish standards that discriminate against new entrants. Finally, privacy advocates assert that industry representatives have a strong incentive—and even a legal obligation to their shareholders—to put bottom-line concerns ahead of the public interest. They therefore express profound skepticism of the idea that co-regulatory processes, which give industry a greater voice than government regulation, will yield improved social outcomes. Those who advocate for pure industry self-regulation also find fault with the co-regulatory approach. They maintain that the government’s review of industry-drafted rules will suffer from the same information deficits as its rulemaking efforts and that its processes for approving codes will present the same delays as its rulemaking procedures. Co-regulation, like direct government regulation, will accordingly yield deficient and out-of-date rules.

While the arguments of the proponents suggest that it is well worth exploring co-regulatory solutions to the Internet privacy problem, those of the critics make it plain that it would be unwise to head down this path without careful consideration of the possible

---

186 GUNNINGHAM & SINCLAIR, supra note ___, at 105 (describing this argument); SCRUGGS, supra note ___, at 128 (same); REES, supra note ___, 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. GUNNINGHAM & SINCLAIR, supra note ___, at 105.


188 GUNNINGHAM & SINCLAIR, supra note ___, at 103.

189 SCRUGGS, supra note ___, at 136 (describing this argument).

190 Id. (describing this argument).
negative consequences and of ways to avoid them. This makes it highly important to study how co-regulation actually works in the area of privacy protection.

IV. European Codes of Conduct: The Legal Framework

A ready-made laboratory for exploring this currently exists: the E.U. member nations’ data protection codes of conduct. As was explained above, pursuant to the 1995 Data Protection Directive each of these nations has passed into law a comprehensive data protection statute.\footnote{191}{See supra notes ___-___ and accompanying text.} Article 27 of the Directive requires member nations to incorporate a co-regulatory mechanism into their statutes. It requires member nations to give industry sectors the option of drafting a “code of conduct” that spells out how the broad requirements of the statute will apply to their particular industry.\footnote{192}{1995 Data Protection Directive, supra note ___, art. 27(1).} Sectors submit the code to the national Data Protection Authority. The Authority evaluates it, negotiates its terms with the relevant sector, and ultimately determines whether the code meets the requirements of the statute. If the Authority approves the code, then the code becomes the official guide by which industry, and the Authority, determine what industry members must do to comply with the statute. Codes of conduct accordingly allow government and industry to negotiate and develop together the specific standards that govern how industry must protect personal data. This is co-regulation applied to the field of data protection. The European experiment offers a testing ground on which to evaluate how this approach works in the privacy field. Yet scholars and policymakers have not yet evaluated this relatively new initiative. For now, the
most comprehensive resource for those who wish to learn about it is the data protection statutes themselves. 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 states to adopt legislation governing the collection, use and disclosure of personal information. According to the Directive, these statutes must establish a national data protection authority;\textsuperscript{193} identify the conditions under which it is appropriate to collect personal information, and those under which it is not;\textsuperscript{194} require firms to notify the data protection authority prior to commencing data processing operations;\textsuperscript{195} prohibit (with certain exceptions) the collection and use of sensitive personal information such as race, religion or sexual orientation;\textsuperscript{196} and require that firms provide notice to individuals, and get their informed consent, before collecting and processing their personal data.\textsuperscript{197} U.S. law provides no counter-part to these ambitious, comprehensive protections.

Article 27 of the Directive instructs member states to incorporate codes of conduct into their statutes. It reads as follows:

\textsuperscript{193}Id. art. 28.
\textsuperscript{194}Id. arts. 6, 7.
\textsuperscript{195}Id. art. 18.
\textsuperscript{196}Id. art. 8.
(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.

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.

(2) 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.  

This language tells us a number of things about how E.U. member nations are to incorporate codes of conduct into their privacy laws. First, Article 27 provides some insight into 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.” In other words, the sectoral codes are to elaborate how generic data protection laws should apply to the “specific features” of a particular sector. They should set out a tailored set of rules that adjust the national standards to fit sectoral realities. Second,

---

197 Id. arts. 10, 14.
198 Id. art. 27.
199 Id., art. 27(1)
200 Korff, *Comparative Summary* at 196 (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.”)
Article 27 instructs member states and the European Commission to “encourage” sectors to draw up codes of conduct. 201 This instruction is ambiguous. What does it mean to “encourage” a sector to draw up a code? Should a member state leave this 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 provide a clear instruction on this point. As we shall see, the national laws reflect this ambiguity. 202

Third, as already mentioned above, Article 27 affirms that sectors can submit their draft code of conduct to the national Data Protection Authority (“Authority”), and that the Authority should offer its opinion as to whether the code is consistent with the underlying national data protection law. 203 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 minimum, defer to the Authority’s expert assessment that the code accurately expresses the law? As we shall see these areas of ambiguity, too, find their way into the member states’ data protection laws. Some treat the codes as legally binding. While others, clearly, do not.

Fourth, Article 27 provides that the Authority “shall, if it sees fit, seek the views of data subjects or their representatives” when determining whether the code is consistent with

---

201 1995 Data Protection Directive, supra note ___, art. 27(1).
202 See infra notes ___-___ and accompanying text.
203 1995 Data Protection Directive, supra note ___, art. 27(2).
the underlying data protection law. This mixed signal (“shall, if it sees fit”) appears to encourage the Authority to meet with data subjects and their representatives but ultimately makes this function discretionary. National legislatures have interpreted the provision in different ways. Some require the national Authority to meet with this important constituency. Others make it discretionary, or avoid the topic altogether. This, too, adds to the diversity of national laws regarding codes of conduct. Finally, Article 27 makes clear that there are actually two types of codes. National codes of conduct apply to a specific sector in a particular EU 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 a sector as it exists throughout the entire European Community. Representatives of that sector from throughout the E.U. draft the code and submit it to the Article 29 Working Party for review. The two types of codes thus 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. To begin with, as should be clear from the foregoing, all of 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

\[204\, Id.\]
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 draw up 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.” Other national laws are similar. At least one nation goes beyond this 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.” This suggests that nations will look for codes to be more rigorous than the data protection statutes that they interpret and apply.

Third, following the language of Article 27, 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.” The Belgian law says that “the Commission shall

206 See, e.g., Luxembourg-Loi du 2 aout 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) (sectors draw up codes of conduct “in order to apply this Law correctly”).
207 Resolution No. 7/99 (emphasis added), quoted in KORFF, DATA PROTECTION LAWS, supra note ___, (analysis of Portuguese law in supplementary CD).
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.”

Other national laws contain
similar language. These provisions make it clear that the national authority has a non-
discretionary obligation to review a code and to determine whether it conforms to the national
data protection law.

While each of the statutes contains such a provision, they 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. They appear to treat it much like agency “guidance” in the U.S., i.e. an
authoritative, but not binding, statement of the Authority’s view on what the law requires.

_ at http://www.sweden.gov.se/content/1/c6/02/56/33/ed5aaf53.pdf._

_Belgium-Law of 8 December 1992 on the protection of privacy in relation to the_
processing of personal data, art. 44._

_Germany-Bundesdatenschutzgesetz [Federal Data Protection Act], May 22, 2001,
BGBl. I at 904, § 38a(2) (“[t]he supervisory authority shall examine the compatibility of the
submitted draft[ ] [codes of conduct] with the applicable law on data protection.”); KORFF,
DATA PROTECTION LAWS, _supra_ note ___._

(Commission must evaluate whether code meets the requirements of the act); Italy-Codice in
materia di protezione dei dati personali [Personal Data Protection Code], Decreto Legislativo
available at http://www.privacy.it/privacycode-en.html (Authority shall verify codes’
“compliance with laws and regulations”); KORFF, DATA PROTECTION LAWS, _supra_ note ___.
(analysis of French law in supplementary CD) (Authority must provide opinions on drafts of
“professional codes”); Luxembourg-Loi du 2 aout 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(g) (Authority
“to receive and where applicable . . . approve codes of conduct”); Malta-Att Dwar Il-
Protezzjoni U L-Privatezza Tad-Data [Data Protection Act] art. 40(g), Mar. 22, 2002
(Authority should “ascertain that the provisions of such codes are in accordance with the
provisions of this Act”); Netherlands- Wet bescherming persoonsgegevens [Personal Data
Protection Act] art. 25(1), Stb. 2000 (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”); Spain-Organic Law 15/1999 of 13 December on the Protection of Personal
Data, art. 32(3) (Authority to evaluate whether or not the “code comp[i]es] with the legal and
regulatory provisions on the subject”).

53
For example, the Danish statute states only that approved codes of conduct are “intended to contribute to the proper implementation of the rules laid down in this Act.” Other statutes implicitly suggest that the opinion is binding on the Authority itself. For example, 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.” The entry of the code in the Register “indicates that the Data Protection Authority agrees that the provision 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.” A few statutes go even farther 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

---


212 Spain—Organic Law 15/1999 of 13 December on the Protection of Personal Data, art. 32(3).

213 KORFF, DATA PROTECTION LAWS, supra note ___, (analysis of Spanish law in supplementary CD). 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 is to refuse to enter it in the General Data Protection Register and may “require the applicants to make the necessary changes.” Spain—Organic Law 15/1999 of 13 December on the Protection of Personal Data, art. 32(3). For other laws of this type, see Netherlands-Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(1), (4) Stb. 2000 (Authority’s positive opinion “shall be deemed to be equivalent to a decision within the meaning of the General Administrative Regulations Act”); Portugal (the statute provides that the authority must “declare whether the drafts are in accordance with the laws and regulations,” Lei da Protec o de Dados Pessoais [Law to Protect Personal Data] ch. V, art. 32(3) (1998), Diario da republica 67/98, and the Authority has decided to make these declarations in the form of Resolutions which “constitute binding administrative decisions.” KORFF, DATA PROTECTION LAWS, supra note ___, (analysis of Portuguese law in supplementary CD); Luxembourg (statute says that Authority should “approve” codes of conduct submitted to it, Loi du 2 aout 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(g), and 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, DATA PROTECTION LAWS, supra note ___, (analysis in supplementary CD).
example, the Italian law states that the Authority (the Guarante) 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. Where this occurs, the code “becomes part of the legal obligations of controllers in
the relevant sector.” While these various laws differ as to the precise legal meaning 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; or, phrased in the language
of Article 27, the degree of force with which they “encourage” the sector to adopt such a
code. Other elements tend to “cluster” around this central feature. We accordingly use it as
an organizing principle and group the laws into three categories: (1) industry choice, (2)
balance of power, and (3) government choice.

______________

214Italy-Codice in materia di protezione dei dati personali [Personal Data Protection

215KORFF, DATA PROTECTION LAWS, supra note ___, (analysis of Italian law in
supplementary CD). At least one other nation provides a similar mechanism. KORFF, DATA
PROTECTION LAWS, supra note ___, (analysis of Irish law in supplementary CD) (Irish law
allows Minister of Justice to submit an approved code to 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.”
KORFF, DATA PROTECTION LAWS, supra note ___, (analysis of Irish law in supplementary
CD); cf. United Kingdom, Art. 52(3) (“The Commissioner shall lay before each House of
Parliament any code of practice prepared” at the behest of the Secretary of State).
1. Industry choice

This first category encompasses those laws that leave it entirely up to the sector to decide whether or not it wants 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.” Other laws in this group are similar. The laws that fall into this category interpret liberally Article 27’s instruction that the national laws should “encourage the drafting of codes of conduct.” They permit sectors to set out a code of conduct. But they do not push them to do so.


217 See Belgium-Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, art. 44 (professional associations and other organizations “may” submit draft codes of conduct to Authority); Denmark-Act on Processing of Personal Data, Act No. 429, § 74 (2000) (trade associations and other bodies “may” draw up codes of conduct); Finland-Personuppgiftslag [Personal Data Act], 523/1999, § 42 (amended 2000) (data controllers “may draft sectoral codes of conduct”); Germany-Bundesdatenschutzgesetz [Federal Data Protection Act], May 22, 2001, BGBl. I at 904, § 38a (associations “may submit draft rules of conduct”); Netherlands-Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(1), Stb. 2000 (organization planning to draft a code of conduct may request the Authority to review it).

218 1995 Data Protection Directive, supra note ___, art. 27.

219 Even 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. See supra note ___ (citing statutes that require this). Presumably, if Authority gives 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., Spain-Organic Law 15/1999 of
Laws that fit this category tend to be associated with other features. They are more likely to require (as opposed to allow) the Authority to consult with data subjects when formulating its consistency opinion.\textsuperscript{220} Moreover, one of the laws in this category gives the courts the ability to review the Authority’s consistency opinion.\textsuperscript{221} This should allow a trade association, firm, or citizens group to challenge in court the Authority’s opinion as to whether the code meets the terms of the statute. In each of these ways, this group of statutes appears to limit the Authority’s discretion at the same time as it expands the industry’s role (and, to some extent, that of the public). The unifying theme here appears to be one of tempering the authority’s power while at the same time emphasizing the interests of both the data controllers (the industry sector) and the data subjects.

\textsuperscript{13} December on the Protection of Personal Data, art. 32(3) (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.

\textsuperscript{220} 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.” Sweden-Personal Data Ordinance (SFS 1998:1191), issued Sept. 3, 1998, available at \url{http://www.sweden.gov.se/content/1/c6/02/56/33/ed5aaf53.pdf}; see also Belgium-Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, art. 44 (the Commission “shall . . . investigate, as far as possible, the standpoints of the persons concerned or of their representatives.”)

\textsuperscript{221} Wet bescherming persoonsgegevens [Personal Data Protection Act] art. 25(4), Stb. 2000 (Netherlands) (stating that 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. KORFF, DATA PROTECTION LAWS, \textit{supra} note \_, (analysis of Dutch law in supplementary CD).
2. Balance of Power

Statutes in the second group take more seriously the national government’s Article 27 duty to “encourage” sectors to draft codes. These statutes require the Authority to “call on”\(^{222}\) or “encourage”\(^{223}\) sectors to draft a code of conduct, although they do not spell out the lengths to which the Authority is to go in order to accomplish this.

Laws in this category are more likely to require that the sector consult with or “cooperate” with the authority when drafting a code of conduct. 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. The theme here seems to be a more equal sharing of power between the industry and the government. The Authority will do more to encourage an industry code of conduct and to advocate for more rigorous

\(^{222}\)See, e.g., Greece-Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/2000 and 2915/2001), art. 19(1)(b) (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”); Cyprus-The Processing of Personal Data (Protection of Individuals) Law 138 (1) 2001, § 23(b) (Authority shall “call on and assist professional organizations and other unions of natural or legal persons . . . in drawing up codes of conduct.”)

standards. But the Authority’s very involvement adds to the legal status of the code and so
gives more regulatory weight to an instrument that industry has helped to draft. This allows
industry to rely on the code more fully, once the agency has approved it. The statutes in this
group should give both the agency, and the industry, more reason 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 and final category push sectors to develop codes. Some of
the statutes in this category stipulate that, if a sector fails to avail itself of the opportunity to
draft a code, the Authority should draft the 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 with relevant trade associations and interested parties. The United
Kingdom appears to provide for a similar process in its data protection law. This approach
goes beyond mere encouragement and uses the threat of a prescribed code of conduct to force
sectors to develop their own set of rules. One commentator has referred to it as the “stick

224 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, DATA PROTECTION LAWS, supra note ___. (analysis of Portuguese law in
supplementary CD).

225 See KORFF, DATA PROTECTION LAWS, supra note ___. (analysis of Irish law in
supplementary CD) (explaining this feature of the Irish data protection law).

226 Data Protection Act, 1998, C. 29, § 52(3) (United Kingdom) (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 .
behind the door” strategy.\footnote{KORFF, DATA PROTECTION LAWS, supra note ___, (analysis of UK law in supplementary CD) (describing United Kingdom law).} 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. It \textit{requires} sectors to develop codes. The Romanian law states that “professional associations \textit{have the obligation} to elaborate and submit for approval, to the supervisory authority, codes of conduct.”\footnote{Law No. 677/2001 for the Protection of Persons Concerning the Processing of Personal Data and Free Circulation of Such Data, Monitorul Oficial 2001 no. 790, art. 28(1) (Romania).} It further provides that the Authority is to “approv[el]” the code, not just issue an “opinion” on it.\footnote{Id.} This increases the legal force of the Authority’s assessment and appears to make it, at 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 says that the purpose is to “protect the rights of persons” whose data is being processed.\footnote{Id.} It is altogether a more forceful provision that seems to have the rights of data subjects, rather than the convenience of industry, at its heart. To achieve this, the Romanian statute puts greater emphasis on the power of the Authority to require that the industry sector draft a code and to issue a binding legal approval of it. It is possible that the Romanian experience with Communist dictatorship both increases the desire to protect personal privacy, and encourages people to look to a strong data protection authority in order to achieve this. In any event, codes should take on even greater regulatory significance under this system.

\footnote{. . codes of practice for guidance as to good practice.”}
Which legal framework will prove most effective? The first, which gives the industry more discretion and downplays the legal significance of any code that it chooses to develop? The second, which puts more pressure on both the industry and agency to negotiate a code and enhances the importance of the document that results? Or the third, which requires the industry to draft a code and then gives the document even stronger legal force? To answer this question—to determine 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 approach 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. These are important areas for future research.

Conclusion

Even as Internet businesses are ramping up their collection and use of personal information the regulation of online privacy remains stuck in neutral. The dominant approach to this problem has been industry self-regulation. But self-regulation is not working. Some call for legislation to address the issue. Yet it is not clear that online privacy is an area that lends itself to a legislative solution and, in any case, Congress does not appear to be close to passing such a statute. In the meantime, with each passing day, Web sites, network advertisers, Internet service providers, and others collect and store more and more personal information. For all its wonderful benefits, the Internet is eroding personal privacy. If this dynamic does not change it could destroy user trust and so threaten the future of the
Internet 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 so 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 has described this debate in some detail, but has not tried to resolve it. It recognizes that further research must be done on co-regulatory initiatives in the privacy field before it is possible even to begin to reach such a conclusion. It identifies important areas for that future research. These research recommendations 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 described and analyzed the statutory provisions through which the various E.U. nations have implemented the co-regulatory initiative. 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. Future work, building on this article, will determine whether co-regulation is an effective way to protect online privacy.