BEFORE THE
DEPARTMENT OF COMMERCE
INTERNET POLICY TASK FORCE

Request for Comments

COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK

DOCKET # 101214614–0614–01

COMMENTS OF

PROFESSOR IRA RUBINSTEIN, NEW YORK UNIVERSITY SCHOOL OF LAW
AND
PROFESSOR DENNIS HIRSCH, CAPITAL UNIVERSITY LAW SCHOOL

Professor Ira Rubinstein
New York University School of Law
40 Washington Sq. South—Room 326
New York, NY 10012
(212) 992- 8909
Rubinstein@exchange.law.nyu.edu

Professor Dennis Hirsch
Capital University Law School
303 E. Broad Street
Columbus, OH 43209
(614) 236-6685
dhirsch@law.capital.edu

January 28, 2011

I. Introduction

These comments focus on Part II.C of *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (the "Policy Framework"), the portion that addresses voluntary, enforceable codes of conduct. As law professors, we have studied existing programs in the U.S. and abroad that have employed enforceable codes of conduct to protect

information privacy. In these comments, we draw lessons from these existing programs and apply them to the Internet Policy Task Force's proposal.

II. Existing Programs Utilizing Enforceable Codes of Conduct

Regulators have for some time employed voluntary, enforceable codes of conduct to protect information privacy. In the United States, the two most significant initiatives are the COPPA Safe Harbor Program and the U.S.-E.U. Safe Harbor Framework. In Europe, they are the Dutch Data Protection Act, which was among the first to use enforceable codes of conduct to protect personal information; and Article 27 of the 1995 European Data Protection Directive, which built on the Dutch approach and extended it to all E.U. member states. These initiatives are similar to, and hold important lessons for, the Task Force's codes of conduct proposal. Yet the Policy Framework does not make sufficient use of this past experience. It briefly discusses the Network Advertising Initiative (p. 42)[1] and U.S.-E.U. Safe Harbor Agreement (SHA) (p. 44), but does not mention at all the COPPA Safe Harbor or the Dutch and E.U. code of conduct programs—regulatory initiatives that are, if anything, even more relevant to the Task Force proposal. As law professors, we have studied all four of these important initiatives. Professor Ira Rubinstein's research on privacy and regulatory innovation has focused not only on the COPPA Safe Harbor Program and the U.S.-E.U. Safe Harbor Agreement, but also on the environmental covenanting approach and its implications for privacy codes of conduct.[2]

[1] Although the Task Force contends that the NAI code is "the *only* significant example of a voluntary code of conduct developed through a collaborative industry effort," two other examples come to mind: the Anti-Spyware Coalition (*see* various documents *available at* http://antispywarecoalition.org/documents/index.htm; and the Global Network initiative (*see* http://www.globalnetworkinitiative.org/index.php), which exemplifies the multi-stakeholder process discussed in the Proposed Framework.

[2] *See* Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, I/S JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (forthcoming Winter 2011), *also available at* http://ssrn.com/abstract=1510275.

Professor Dennis Hirsch recently returned from a Fulbright Professorship during which he studied both the Dutch code of conduct program and the 1995 Data Protection Directive's use of this regulatory method. In addition, he was an early proponent of looking to environmental "covenants" with industry sectors (an approach similar to enforceable sector-based codes of conduct) and other innovative environmental policy tools as a model for privacy regulation.[3] In the remainder of this section, we describe the four regulatory programs in the U.S. and in Europe that have used enforceable codes of conduct to protect personal information – the COPPA Safe Harbor, the SHA, the Dutch code of conduct program, and the 1995 European Data Protection Directive's use of such codes. In the subsequent sections, we draw on our research into these programs to offer insights about enforceable codes of conduct and the role they can play in Internet privacy regulation.

A. The COPPA Safe Harbor Program

Congress created the only privacy safe harbor in US law in 1998, when it enacted the Children's Online Privacy Protection Act (COPPA). The COPPA safe harbor encourages industry representatives to issue self-regulatory guidelines, which must be approved by the FTC, subject to a notice and comment procedure. The goal of this safe harbor provision is to facilitate industry self-regulation in two ways: first, by granting enforcement-related benefits (Web sites that comply with approved self-regulatory guidelines are deemed to be in compliance with the law); and second, by allowing greater flexibility in the development of self-regulatory guidelines in a manner that takes into account industry-specific concerns and technological developments. FTC approval of a COPPA safe harbor program turns on whether self-regulatory guidelines: (1)

---

[3] Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation can Learn from Environmental Law*, 41 GEORGIA L. REV. 4, 50-57 (2006).

meet or exceed statutory requirements; (2) include an effective, mandatory mechanism for the independent assessment of compliance with the guidelines; and (3) contain effective incentives to ensure compliance with the guidelines. The self-regulatory guidelines are, in effect, codes of conduct and the four approved COPPA safe harbor programs are the only US examples of enforceable privacy codes of conduct in existence today.

B. The US-EU Safe Harbor Agreement

In 2000, the US and the EU entered into a Safe Harbor Agreement (SHA) spelling out Privacy Principles that would apply to US companies and other organizations receiving personal data from the EU. The SHA creates a voluntary mechanism enabling US organizations to demonstrate their compliance with the EU Directive for purposes of data transfers from the EU. They must self-certify to DOC that they adhere to the Privacy Principles that mirror the core requirements of the EU Directive, i.e., notice, choice, onward transfer, security, data integrity, access and enforcement, and repeat this assertion in their posted privacy policy. Under the terms of the SHA, the FTC agreed to treat any violation of the Privacy Principles as an unfair or deceptive practice. But the SHA also defines the mechanism that firms should use to ensure compliance with these principles. These include (a) readily available and affordable independent recourse mechanisms for investigating and resolving individual complaints and disputes; (b) verification procedures regarding the attestations and assertions businesses make about their privacy practices, which may include self-assessments (which must be signed by a corporate officer and made available upon request) *or* outside compliance reviews; and (c) remedies for failure to comply with the Privacy Principles including not only correction of any problems but various sanctions such as publicizing violations, suspension or removal from a seal program, and compensation for any harm caused by the violation. Truste, BBBOnline, and several other self-

regulatory privacy programs already in operation when the SHA took effect developed Safe Harbor programs specifically designed to satisfy (a) and (c). The verification requirement is satisfied by self-assessment or third-party compliance reviews. These programs also represent a form of enforceable voluntary codes of conduct.[4]

C. Dutch Codes

The Dutch were among the first to employ negotiated, enforceable codes of conduct as a regulatory instrument for the protection of personal data. The 1995 European Data Protection Directive later adopted this approach and extended it to all EU member nations. In the spring of 2010, Professor Hirsch spent a semester as a Fulbright Senior Professor at the University of Amsterdam's Institute for Information Law. His Fulbright research project centered on the Dutch experience with data protection codes of conduct and, to some extent, on the European initiative.

In 1989, the Netherlands passed its first privacy statute, the Law on Personal Data Files or Wet Persoonsregistraties (WPR). This legislation imposed broad requirements for the protection of personal data. It also created a regulatory agency, the Registration Chamber, to implement and enforce these requirements. However, it did not authorize the Registration Chamber to promulgate rules in furtherance of the statute. Instead, it contemplated that specific industry sectors would generate their own rules in the form of an industry code of conduct. The Chamber would review these codes, evaluate whether they met the terms of the statute and, if so, approve them. Compliance with an approved code would constitute a legal safe harbor with respect to compliance with the statute, at least where the Chamber was concerned. By 1995, at least sixteen sectors had drafted and submitted such codes, and the Chamber had approved the

[4] The enforceability of voluntary codes is discussed below in Section III.F.

majority of them. In 2000, the Dutch Parliament passed a new statute, the Law on the Protection of Personal Data or Wet Bescherming Persoonsgegevens (WBP) ("the Data Protection Act.") The 2000 Data Protection Act supplanted the 1989 law. It replaced the Registration Chamber with an Office for the Protection of Personal Data (College Bescherming Persoonsgegevens, or CBP) also referred to as the Data Protection Commission. The 2000 law, like its predecessor, relied on voluntary industry codes of conduct as the main source of sector-specific rules. Article 25 of the Data Protection Act provided that industry sectors could "request the Data Protection Commission to declare that, given the particular features of the sector or sectors of society in which these organizations are operating, the rules contained in the said code properly implement this Act." Such a declaration would have the force of a regulation. This model shares much in common with the Task Force's voluntary, enforceable code of conduct proposal. The main difference is that the Dutch have been implementing this approach for more than 20 years and have already approved codes for a wide variety of sectors.

D. The 1995 Directive

The drafters of the 1995 European Data Protection Directive were familiar with the Dutch model and incorporated it into the Directive itself. As the Task Force may already be aware, Article 27 of the Directive requires member states to "encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions . . . taking account of the specific features of the various sectors." It further calls upon the national data protection authorities to "ascertain whether [a given code is] in accordance with the national [data protection act]." Once again, the idea is to allow industry sectors to write their own implementing rules subject to the approval of the national data protection authority. In addition to calling for national codes of conduct, Article 27 also authorized the Article 29 Working Party

to consider and approve sectoral codes on behalf of the entire European Community. Such "Community Codes" would constitute a safe harbor with respect to the national data protection laws of all member states. To date, the Article 29 Working Group has approved only one Community Code, that of the Federation of European Direct and Interactive Marketing (FEDMA). Recently, the Article 29 Working Group approved an annex to the FEDMA Community Code that specifically addressed *online* direct marketing

III. Lessons from the US, Dutch and European Experiences with Codes of Conduct.

As noted above, Professor Rubinstein's research has focused on COPPA and the SHA, while Professor Hirsch's research focused on the Dutch code of conduct initiative and the 1995 European Data Protection Directive. Most of the lessons identified here arise from these settings. Where relevant, this discussion will also make reference to negotiated environmental covenants, which bear a strong resemblance to enforceable codes of conduct. We begin with some general comments on codes of conduct and the Task Force proposal. We then address specific questions that the Task Force raised in its report.

A. General Comments on Codes of Conduct and the Task Force Proposal

The Task Force proposes *enforceable,* voluntary codes of conduct, rather than purely voluntary codes. Our research suggests that this is the correct approach. Regulatory theory makes it clear that industry self-regulation and direct government regulation are not the only options. Rather, they are opposing ends of a regulatory continuum. A variety of other regulatory schemes – often referred to as "co-regulation" -- inhabit the middle ground. Enforceable voluntary codes of conduct are an important co-regulatory approach. All four of the programs that we studied utilize this approach in one form or another. This wide-spread, international use

of enforceable codes of conduct supports the Task Force's choice of regulatory mechanism and shows that it fits comfortably within regulatory practice.

By contrast, pure self-regulation has not yet proven to be an effective means for protecting Internet privacy. Industry proponents of self-regulatory solutions typically argue that this approach protects privacy in a more flexible and cost-effective manner than direct regulation without impeding the rapid pace of innovation in Internet-related businesses. However, critics of self-regulation emphasize its shortcomings, including weak or incomplete realization of Fair Information Practice Principles (FIPPs), inadequate incentives to ensure wide scale industry participation, ineffective compliance and enforcement mechanisms, and an overall lack of transparency. The FTC recognized these weaknesses in its recent staff report on Protecting Consumer Privacy in an Era of Rapid Change.[5] We believe that *enforceable* voluntary codes of conduct, in which regulators play some role in the code drafting and enforcement process, represent a better approach.

Our research shows that enforceable codes of conduct possess several valuable attributes. First, rules generated through the code drafting process draw on industry knowledge and so tend to be more tailored to the particular features of the industry, and more workable, than standards that government regulators would be able to draft on their own. Professor Hirsch saw many examples of this in his review of Dutch industry codes of conduct. Second, the very process of drafting a code of conduct raises business awareness of privacy issues. In the Netherlands, industry representatives stated that the drafting process forced companies to understand more deeply what information they were collecting, how they were using it, and who they were sharing it with. They further stated that they, and their member companies, were more willing to

[5] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, Preliminary FTC Staff Report, at iii (2010).

accept rules that they themselves had had a hand in drafting. Third, the use of codes of conduct can promote administrative efficiency. In the Netherlands, industry representatives drafted the codes. This meant that regulators did not have to invest their own resources in this task. Given the many sectors that process personal data, and the amount of work that drafting rules for all of them would entail, government officials saw this as a significant benefit.

Our research also strikes some cautionary notes with respect to the use of enforceable codes of conduct. To begin with, the process of drafting and negotiating codes of conduct can take far longer, and require a greater commitment of resources, than many assume to be the case. This was true in the Netherlands where the code negotiation process typically involved many meetings and the exchange of multiple drafts. Second, codes are not always the nimble and adaptive instruments that some have claimed them to be. The Dutch Data Protection law requires sectors to revise their codes and seek new approval every five years. Many sectors missed this deadline and their codes lapsed. In some instances, this situation persisted for years before industry and government representatives finally revised and re-approved the relevant code. Professor Hirsch concluded that costs of renegotiating a code posed an obstacle to quick adaptation.

Third, some code programs have experienced problems with monitoring and enforcement. With respect to the SHA, a number of studies have found that a very high percentage of participating firms did not incorporate all of the agreed upon Privacy Principles in their own posted privacy policies. Moreover, the SHA exhibits serious free rider problems (many firms self-certify their adherence to the Privacy Principles without even revising their posted privacy policies in accordance with SHA requirements and only a tiny fraction of firms that transfer data from the EU to US have signed up). Oversight and enforcement have been lacking

despite what one study referred to as "frequent and even flagrant inconsistencies and violations in implementation." Indeed, it was not until the summer of 2009 that the FTC announced its *first* enforcement action against a US company for violation of the SHA. The Dutch initiative suffered from some of the same problems. In some sectors neither the government regulators nor the industry trade associations effectively monitored or enforced compliance with the codes. One sector did utilize independent, third-party auditors. This seemed to have a positive effect. The Task Force appears not to favor third-party audits (p. 27, note 73). We encourage the Task Force to rethink this position and to consider integrating third-party audits into its proposal. Finally, some code programs have not successfully integrated privacy NGOs into the code drafting or approval process. In the Netherlands, this stemmed more from the NGO community's lack of resources than from any formal impediments to such participation. Nonetheless, it yielded a process that was not very inclusive or transparent.

B. Motivating Industry Sectors to Draft Codes of Conduct

The Task Force has asked for input on how to encourage the development of industry codes of conduct (pp. 48-49). It specifically seeks input on the use of "carrots and sticks" to encourage the development of industry codes (p. 49). Professor Rubinstein's research suggests the importance of using *both* sticks and carrots as incentives and suggests what these carrots and sticks might look like in the privacy setting.[6] In other regulatory settings such as environmental law, sticks typically include a threat of stricter regulations or imposition of higher pollution fees. In contrast, carrots often take the form of more flexible regulations, recognition of better performance by the government, and cost-savings such as exemptions from mandatory reporting, or easier and quicker permitting.

[6] Rubinstein, *supra* note 2 at 48-50.

The COPPA safe harbor does not appear to have achieved the right mix of carrots and sticks. Professor Rubinstein's research showed that the initiative had a very low rate of participation, with fewer than 100 firms having been certified under the four approved programs. This may be because deemed compliance is too weak an incentive to persuade many firms to bear the costs of joining a safe harbor program. It also may stem from a lack of regulatory flexibility. Even though the implementing rule includes language encouraging such flexibility, in practice, the approved self-regulatory programs all have nearly identical requirements to those of the COPPA statute. The lack of regulatory flexibility in the COPPA safe harbor program may have deterred some firms from entering the program.

As to sticks, advocacy groups and privacy scholars have long favored a private right of action and liquidated damages as enforcement mechanisms in any new privacy legislation. Not surprisingly, industry has argued that such remedies are both unnecessary and ineffective. This suggests that an excellent stick might be devised around a *tiered* liability system. Under this new approach, privacy legislation would allow civil actions and liquidated damages awards against firms that engage in prohibited practices and did not participate in an approved safe harbor program. In sharp contrast, compliance with approved self-regulatory guidelines would not only serve as a safe harbor in any enforcement action but exempt program participants from civil lawsuits and monetary penalties. Other sticks for non-participating firms might include broader opt-in requirements; external and independent audits of regulatory compliance and mandatory reporting to the FTC; and much stricter requirements for firms engaged in online behavioral advertising, such as a total ban on the use of sensitive information in behavioral targeting and a data retention limit of one month.

In addition to these sticks, privacy legislation might also offer safe harbor participants a number of carrots including exemptions from civil actions and liquidated damages; cost-savings such as compliance reviews based on self-assessments rather than external audits by an independent third party; regulatory flexibility in the form of tailored requirements addressed to specific business models such as online behavioral advertising; government recognition of better performing firms (e.g., an FTC "seal of approval" under which firms that meet safe harbor requirements are duly recognized); and government procurement preferences for the products or services of participating firms.

In applying various sticks and carrots to encourage safe harbor participation, it is important to emphasize that safe harbor benefits should be limited to firms demonstrating superior performance and not be available to firms that merely satisfy default privacy requirements. These higher performance standards might include the use of data governance practices (i.e., a system for assigning rights and accountabilities within a company for all information-related processes); advanced privacy methodologies (such as the adoption of a "Privacy by Design" approach to building privacy protection into any product or service that uses personal data, as FTC recommends in its recent report);[7] and industry-wide best practices (such as mandatory privacy training for all staff with privacy responsibilities, providing online guidance on privacy and security issues to employees and consumers, and implementing a complaint-handling procedure).

[7] FTC, *supra* note 5, at 44-52.

C. Baseline Privacy Legislation

Our research also suggests that baseline privacy legislation can play an important role in encouraging firms to adopt a voluntary code of conduct. This is an important reason to favor such legislation.

The Dutch experience bears this out. The Dutch Data Protection Act speaks in broad terms and poses many interpretive issues. But the Dutch Data Protection Commission has not promulgated clarifying regulations. In interviews, industry representatives stated that the primary reason they wanted a code of conduct—their main motivation for drafting such a code—was that it brought a degree of clarity to the statutory scheme. The *code* interpreted the statute in light of the specific realities of the sector. That was a major benefit for businesses that place a high value on regulatory certainty. Broadly worded legislation thus motivates firms to produce an industry code of conduct as a way to construe and clarify the statutory scheme. Thus, baseline privacy legislation and incentives for industry to develop codes of conduct can go hand-in-hand.

Baseline privacy legislation is also important for another reason. Without it, those firms that do not commit to the industry code will be able to free-ride on the efforts of the more responsible companies that do agree to abide by the code. This will provide a competitive advantage to companies that do not commit to a code, and so will sap firms' motivation to sign up for such a code.

D. Global Interoperability

The Task Force expressed its desire to encourage global interoperability in commercial data privacy frameworks (pp. 53-57). Codes of conduct could play an important role in this. As

was mentioned above, Article 27 of the 1995 European Data Protection Directive allows industry sectors to propose, and the Article 29 Working Group to approve, *community-wide* codes of conduct that would create a safe harbor with respect to all member state laws. Industries could utilize this mechanism to produce global codes of conduct that would harmonize E.U. and U.S. requirements. To produce such an instrument, an industry sector would have to arrive at a single code that met both U.S. and E.U. commercial data privacy standards. It would then submit the code both to the FTC for U.S. approval, and to the Article 29 Working Group for European approval. If each of these two regulatory authorities approved the same document this would yield a single code of conduct that would meet both European and American legal standards. It would harmonize the EU and US commercial data privacy regimes.

Achieving this would likely require extensive consultation and cooperation among European and American companies in the same business sector. It would further require the FTC and the Article 29 Working Group to work closely together to ensure that their independent approval processes did not yield separate, incompatible codes. Assuming that such cooperation were possible, industry codes could serve as a vehicle for harmonizing its U.S. data protection laws with those of the EU.

Industries could take this even one step further. As the Task Force points out (p. 55), APEC's cross-border privacy rules initiative is developing self-regulatory seal programs that appear to share some features in common with enforceable voluntary codes of conduct. Were an industry to develop a code that was consistent, not only with an EU Community Code, but with an APEC seal program as well, the code could function as a truly global set of commercial data privacy standards. This would facilitate cross-border data flows, reduce costs to business, and

provide consumers with more consistent levels of data protection as their information travels the globe.

E. FTC Rulemaking Authority

The Task Force asks whether the failure of the code drafting process should trigger FTC rulemaking authority (p. 51). Professor Hirsch's research in the Netherlands suggests that it should. Dutch firms appear to value the opportunity to draft the rules that will govern their sector. The threat that, should they fail to do so, the government might step in and complete the task, could provide a useful incentive for industry action. Thus, the FTC should, at a minimum, have rulemaking authority when the code drafting process fails.

The free-rider problem suggests that this rulemaking authority should extend further. Even where an industry sector has drafted a code and the FTC has approved it, the Commission should still be able to promulgate rules for firms that to do not commit to comply with the code. This would give such firms a choice between complying with an industry-drafted code, or a government-drafted one. Most will likely choose the industry code. That will address the free-rider problem. As the next section argues, however, the FTC's existing rulemaking authority is quite limited, so these suggestions would almost certainly require new legislation.

F. Does the FTC Have Authority to Enforce Voluntary Codes of Conduct?

The Task Force envisions a new Privacy Policy Office (PPO) at Commerce. The PPO would call for tailored industry codes of conduct; convene relevant multi-stakeholder groups to propose new codes of conduct, subject to comment and review; and, if the codes are approved, they would be enforced by FTC. This proposal raises two related legal issues. First, the Task

Force assumes without much discussion that FTC has the power to "enforce" voluntary codes. But it is uncertain whether the Commission has the legal authority to do so if this means taking action against firms solely because they do not adhere to a voluntary code. The main basis for FTC action against a firm that does not adhere to a voluntary code is likely to be the prohibition on "deceptive" acts in Section 5 of the FTC Act. In interpreting Section 5, the Commission has long maintained that an act or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances and it affects consumers' behavior or decisions about the product or service. Thus, a deceptive practice claim requires a false statement. The FTC has taken action against websites for violating their own privacy policies and in a few such cases, the Commission has also alleged that the respondent was a licensee of Truste (an organization that certifies the privacy policies of online businesses) and displayed the Truste seal. But these cases turned on a misrepresentation in the company's posted privacy policy and not on whether the company had failed to live up to the Truste privacy guidelines.[8]

More recently, a company's false statement that it participated in a voluntary code was treated as a deceptive practice.[9] This opinion contains much broader language as it enjoins defendants from misrepresenting "the extent to which they are members of, adhere to, comply with, are certified by, are endorsed by, or otherwise participate in any privacy, security, or any other compliance program sponsored by any government or third party." Despite this broad

[8] *See, e.g.,* FTC v. Toysmart.com, No. 00-11341-RGS (D. MA. 2000)(alleging that Toysmart, a Trustee licensee, misrepresented its data sharing activities and obtaining consent order prohibiting such misrepresentations); *see also In re* Microsoft Corp. (alleging that Microsoft, a Truste licensee, misrepresented its data collection activities and obtaining consent order prohibiting such misrepresentations).

[9] *See* FTC v. Javian Karnani, and Balls of Kryptonite, No. 09-CV-5276 (D. C. CA. Aug. 6, 2009)(alleging that the firm misrepresented its participation in the SHA and enjoining such misrepresentations).

language, the deceptive practice claim hinges on the company's false statement, not its failure to adhere to the SHA.

In order to argue that a company engages in a deceptive practice when it truthfully represents its participation in a voluntary privacy code to but fails to live up to some aspect of that code, the Commission would, at the very least, need to demonstrate that consumers rely on whether a firm participates in the SHA (or a similar voluntary program) in deciding whether to use the company's products or services. This seems like a stretch given the mixed reputation of SHA and other privacy seal programs. Perhaps the enforceable voluntary codes envisioned by the Task Force would not only receive strong industry support but eventually achieve such success that consumers would come to rely on them as a virtual guarantee that participating companies have sound privacy practices. Until that happens, however, it seems more likely that the Commission would bring enforcement cases based on a material misrepresentation in a participant's own privacy policy than the mere fact that the participating firm does not fully adhere to a voluntary code.

Second, the Task Force does not provide much detail on how the multi-stakeholder process might work. Although the FTC has developed appropriate rules governing the substantive requirements of COPPA safe harbor programs, the process for submitting proposed programs for review, and the criteria for approving such programs, it did so under an explicit statutory grant of rulemaking authority. But absent a new privacy law authorizing enforceable codes of conduct under a safe harbor or similar approach, FTC's rulemaking authority under Section 18 of the FTC Act is very limited. In fact, it seems doubtful that the Commission's existing powers extend to prescribing the multi-stakeholder process envisioned in the Policy Framework or broadly requiring that participating firms abide by such codes.

The implication of both of these legal concerns is that the FTC would be in a much stronger position to enforce voluntary codes of conduct if Congress enacts a new privacy law authorizing the Commission to issue implementing regulations for a safe harbor or similar program.

G. Timing of FTC Approval

The Task Force asks whether FTC approval of a code should be ex ante or ex poste (p. 53). The Dutch experience provides some support for the ex ante approach, although it also sounds some cautionary notes.

Ex ante approval creates the opportunity for a negotiation between regulators and regulated companies, a creative process that can generate solutions that neither party would have arrived at on its own. While Professor Hirsch did not see many examples of this in his study of Dutch data protection codes of conduct, he did see enough instances to suggest that such collaborations are possible. Ex ante approval will spark them. It will also enhance the value of the code in the eyes of the public and so increase its value as a trust-creating instrument for those firms that agree to abide by it. Finally, the Dutch experience suggests that government officials will push industry drafters to make a code more rigorous and protective of personal data than they would otherwise have done on their own.

That said, some industry representatives in the Netherlands reported that government officials may be overly legalistic and risk-averse in their assessment of draft industry codes. This can greatly slow down the code drafting process and drain a code of some of its flexibility. An ex post approach would avoid this. In sum, ex ante approval can have both positive and

negative effects. Much will depend on the spirit with which government and industry negotiators engage in the code negotiation process, as discussed further below.

H. Multi-Stakeholder Processes

As previously noted, the Task Force refers at various points to a multi-stakeholder process but says little about what such a process would look like or the difficult challenges that all such multi-stakeholder process must overcome. To begin with, how many and which firms and advocacy groups are allowed to participate? Are the meetings open or closed? What motivates participation and do the players have sufficient incentives to reach a compromise rather than blowing up the process with recriminations all around? What counts as agreement—unanimity or consensus? What happens when agreement is reached—does the FTC have to approve the agreement as negotiated (and under what authority) or may it unilaterally alter the negotiated agreement as a condition of approval?

In the US, the Negotiated Rulemaking Act provides one set of answers to these questions. Although "reg neg" has never been used in the privacy settings, environmental law scholars have identified a few situations where negotiated rulemaking succeeded reasonably well. For example, Andrew Morriss and his colleagues point to situations "where the substance of the regulation requires the credible transmission of information between the regulated entities and other interest groups, and where the agency's preference for a particular substantive outcome is weak."[10] Reg neg also requires "a relatively high degree of shared interest among the groups participating, the existence of gains from trade to allow parties to compromise, and a willingness by interest groups to reject the role of spoiler."[11] These views are largely consistent with the findings of

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

Daniel Selmi, who conducted a detailed study of the negotiation of a regional air quality rule. Selmi explained why the parties were willing to compromise as follows: industry believed that regulation was inevitable; the environmental groups recognized that even thought they preferred an outcome based on new and expensive technology, they lacked the political capital to achieve this result; while the agency was not locked into a rigid, initial position but remained open towards finding a solution that responded to information acquired during the negotiations. The Task Force should consider investigating these and other examples of negotiated environmental agreements if it plans to rely on multi-stakeholders to achieve privacy codes of conduct.

In the Netherlands, NGOs and public interest organizations did not participate much in the code drafting or negotiation process. This stemmed mainly from insufficient NGO resources, rather than from any formal barrier to such involvement. Nonetheless, some evidence suggests that this lack of third-party participation allowed business representatives to gain an upper hand in the code negotiation process. The United States does have highly knowledgeable and comparatively well-resourced privacy organizations. Their participation would bring additional transparency to the process. This could level the playing field between government and industry and increase the credibility of the resulting code in the eyes of the public. The Dutch experience suggests the importance of integrating privacy NGOs into the code development process.

Assuming that NGO representatives do participate in the code negotiation process, it is important to think carefully about *when* they do so. Some of the Dutch participants suggested that industry representatives would not be as forthcoming about their real issues and problems were privacy advocacy groups to be in the room. Early NGO participation might chill this important information exchange. One interviewee, a prominent industry lawyer, supported NGO participation but suggested that it occur at a separate stage in the negotiation process. In the first

stage, government and industry representatives would hold preliminary discussions, begin to share information and identify the general contours of a code. In the second stage, NGO participants would join the discussion and add their point of view. In a third stage, the parties would settle on a draft code and issue it for wider public comment. This differs from the process laid out in the Negotiated Rulemaking Act. But the key point is that these issues must be addressed and clarified at the outset before any multi-stakeholder process commences.

IV. Conclusion

In sum, based on our research as described above, we strongly concur with the Task Force's view that industry codes of conduct play a valuable role in privacy regulation and that enforceable codes are more likely to achieve their goals than purely voluntary codes. However, we also believe that enforceable voluntary codes raise a number of legal and policy issues—such as free rider problems, possible gaps in the FTC's rulemaking and enforcement authority, and the need for clearly defined rules governing any multi-stakeholder process—and that a statutory approach to voluntary codes is better able to resolve these issues than the informal approach envisioned by the Task Force.

Thank you for this opportunity to comment on the task Force report. If we can be of any further assistance, please do not hesitate to contact us.

Sincerely,

Ira Rubinstein
Adjunct Professor of Law
NYU School of Law

Dennis Hirsch
Geraldine W. Howell Professor of Law
Capital University Law School