Dutch Treat?
Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law

Dennis D. Hirsch
Geraldine W. Howell Professor of Law
Capital University Law School
dhirsch@law.capital.edu
(614) 236-6685

July 19, 2012

Paper Submitted for the
Future of Privacy Forum
Privacy Papers for Policy Makers Initiative 2012

TABLE OF CONTENTS

I. Introduction

Privacy regulation in the United States is at a crossroads. The revolutions in information and communication technology have put individual privacy at risk.[1] Corporate tracking of purchases, online activities and location,[2] the commercial aggregation, use and sale of massive databases of personal information, and the data security breaches and identity theft to which these practices give rise, have convinced many that government should do more to rein in the private sector and protect personal information. They have called for laws that will give individuals more control over how companies collect, handle and disclose their personal information.[3]

Yet others strongly oppose such government intervention. They maintain that government officials cannot keep up with the rapid changes in information and communications technology and that regulation will therefore impede growth in this increasingly important economic sector. They insist that only industry, which knows the emerging technologies and business models far better than government, is in a position to establish workable rules. They believe that industry self-regulation should provide the framework for protecting individual privacy interests.[4]

---

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

[2] *See* Federal Trade Commission, *Privacy Online: A Report to Congress* iii (June 1998) (FTC research "shows that the vast majority of Web sites – upward of 85% -- collect personal information from consumers"); *accord* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1629-31 (1999) (describing how and why web sites collect personal information) [hereinafter Schwartz, *Cyberspace*].

[3] 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.")

[4] *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"); Strauss & Rogerson, *supra* note ___, at 181 (discussing those who hold this view).

Over the past decade the government regulation and the industry self-regulation camps have largely fought each other to a standstill. Members of Congress have proposed numerous bills to regulate the commercial use of personal information, but the opponents of regulation have defeated them.[5] At the same time industries have tried self-regulation, but NGO and government evaluations of these efforts have repeatedly found them to be lacking.[6] Creative proposals that might bridge the gap between the opposing sides and provide a way to move forward have been largely missing from the debate.

Until recently, that is. The latest Congressional bills,[7] and a long-awaited 2012 White House policy paper on privacy regulation (the "White Paper"),[8] each contain a kernel of something new. Each proposes that government and regulated industries, and possibly other stakeholders, work *together* to draft commercial privacy rules. As both the bills and the White Paper envision it, Congress will pass legislation that imposes broad privacy requirements on businesses.[9] Yet government regulators will not necessarily draft the rules that spell out what

---

[5]*See* Marcia S. Smith, *Congressional Research Service for Congress, Internet Privacy: Overview and Pending Legislation* 18 (2006) (describing Internet privacy bills 109th Congress and concluding that while some such bills were introduced in the House and Senate, none have passed);

[6]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* iii (Dec. 2010) (Industry self-regulation has been "too slow, and up to now [has] failed to provide adequate and meaningful protection.);" Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation?,* 34 SEATTLE L. REV. 439, 455-464 (2011) (describing industry efforts at self-regulation and explaining how they have come up short).

[7]Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011) [hereinafter Kerry-McCain Bill].

[8]The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012) [hereinafter White Paper]; Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (2010) [hereinafter Green Paper].

[9]Kerry-McCain Bill, *supra* note ___, Titles I-III; *Green Paper*, *supra* note ___, at 23-30 (calling for adoption of a set of a baseline commercial data privacy framework and noting that many commentators favored doing this through legislation).

industry must do to comply with these broad requirements. Instead, the statute will authorize industry representatives, possibly joined by other interested parties,[10] to draft the rules that flesh out the statutory provisions and to spell out how they apply to their business area. Such groups will then submit their rules – often referred to as an industry "code of conduct" – to regulators for approval.[11] If the regulators agree that a given code meets the statutory requirements, and approve it, then individual firms that meet the terms of the code will be deemed to be in compliance with the statute. They will be granted a legal "safe harbor."[12] The Congressional bills call this a "safe harbor" approach.[13] The White Paper calls it "voluntary, enforceable codes of conduct."[14] But the basic concept is the same. Companies that comply with the approved code of conduct inhabit a legal safe harbor. This article will use the terms "safe harbor program" and "codes of conduct program" interchangeably.

Safe harbor or code of conduct programs do not constitute direct government regulation

---

[10]The three bills and the White Paper differ somewhat on this point. The White Paper clearly calls for codes to be developed by "multi-stakeholder groups" consisting of industry representatives and other stakeholders such as "privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups." White Paper, *supra* note ___, at 23. The bills, however, are far less clear on this point. The Rush and Stearns bills refer to the safe harbor organizations as "self-regulatory programs." Rush bill § 401; Stearns bill § 9. This language suggests that the groups will be made up of business representatives, as is generally the case in a self-regulatory initiative. The Kerry-McCain bill somewhat ambiguously says that "nongovernmental organizations" will administer the safe harbor programs. Kerry-McCain bill § 501. It offers no further definition of this term. While a privacy advocacy group would likely qualify as an NGO, so would an industry trade association. Thus, the Kerry-McCain bill does not make clear whether business representatives will administer the safe harbor programs alone, or whether they will be joined by privacy advocates and other interested parties.

[11]*Green Paper*, *supra* note ___, at 42; Kerry-McCain Bill, *supra* note ___, § 501 (the bill refers to these industry-drafted rules as "safe harbor programs" and would allow any non-governmental organization, including but not limited to industry associations, to develop such a program).

[12]*Green Paper*, *supra* note ___, at 43, 44; Kerry-McCain Bill, *supra* note ___, § 502(a).

[13]Kerry-McCain Bill, *supra* note ___, Title V.

[14]*Green Paper*, *supra* note ___, at 41.

since industry representatives, not government officials, draft the rules that spell out how the statute applies to particular firms. But neither are they pure industry self-regulation since Congress sets the baseline requirements and a regulatory agency must approve the rules as meeting the terms of the statute. Safe harbors are a blended form of regulation that combines elements of direct government regulation and industry self-regulation and requires regulators and businesses to work together to produce the rules that will guide corporate behavior. It is an example of what scholars have called "collaborative governance" – a hybrid form of regulation in which government, industry and, potentially, other stakeholders collaborate on the drafting and/or enforcement of rules. The proponents of collaborative governance claim that it can combine the flexibility and business savvy of industry self-regulation, with the accountability and public-spiritedness of government rules. Such a blended approach might provide a way to transcend the current political impasse and pass comprehensive legislation to protect individual privacy in the digital economy.[15]

But is collaborative governance good policy? Will bringing industry into the rule drafting process really allow it to infuse government rules with flexibility and business knowledge? Or, will industry use the opportunity to draft rules that favor its own interests? If the latter, will the government approval process be enough to innoculate the rules against industry bias? The safe harbor bills, and the momentum that they are gathering, requires us to ask whether or not the turn towards collaboration is a good one.

How to figure this out? One place to look for an answer is the scholarly literature on collaborative governance. As Part III will explain, scholars have analyzed the questions just

[15]Indeed, that may be one of the reasons why each of the current bills incorporates this alternative.

posed. Unfortunately, they fundamentally disagree with one another. Proponents, such as Professor Jody Freeman of Harvard Law School, maintain that collaborative methods can fundamentally change the relationship between traditional adversaries in the regulatory process. Instead of pitting industry, public interest stakeholders, and government against one another, as traditional regulation does, collaborative methods can allow them to put their heads together and generate solutions that are both workable for industry and protective of social interests. The critics are far more pessimistic. They believe that industry will seek to manipulate the rules to serve its own interests and that the government approval process will not be able to check this behavior. They forecast one-sided rules that favor industry over the public. The literature alone does not tell us whether collaborative regulation is a good choice for information privacy law, or a bad one.

How, then, to assess the new Congressional and regulatory proposals for safe harbor programs and enforceable codes of conduct? Is there a body of practical experience on which we can draw? Has anyone tried using collaborative governance to protect personal information?

The Dutch have. In 1989, the Dutch government began using a method of privacy regulation that is very similar to the one that Congress and the White House have proposed.[16] It involves a privacy statute with broad requirements; industry drafted "codes of conduct"; government evaluation and approval of these codes; and a legal safe harbor for those firms that follow the approved, industry code. The main difference between the Dutch approach and the American proposals is that the Dutch have been implementing their program continuously for more than twenty years. During this time, they have approved more than eighteen codes of

[16] *See infra* Part IV (describing this Dutch regulatory program).

conduct for banks, insurance companies, direct marketers, pharmaceutical companies, and many other industry sectors. The Dutch experience represents the most comprehensive body of experience to date on how a collaborative approach actually works – or fails to work – as a means of protecting personal information in a developed, Western economy. Studying this real-life experience can shed light on whether and how to implement such a program, and on potential stumbling blocks and pitfalls that it might encounter.

In the spring of 2010, I served as a Fulbright Professor at the University of Amsterdam where I studied the Dutch "code of conduct" approach to privacy regulation. I conducted face-to-face interviews with the regulators, industry representatives and privacy advocates who had drafted and negotiated the codes.[17] I sought to learn what the program, as implemented, could tell us about how collaborative governance could function as a tool for protecting personal privacy. I publish the results of that research, for the first time, in this article. Here, I synthesize and draw insights from my interviews. I then make normative recommendations, grounded in the Dutch experience, as to whether the U.S. should employ a collaborative approach to commercial privacy regulation and, if so, how it should go about this.

The article proceeds as follows. Part II will describe the recent Congressional bills and White House policy papers that propose the using a collaborative, safe harbor approach to regulate commercial privacy. Part III will synthesize the literature on collaborative governance. It will describe both the proponents' optimistic vision of this method, and the critics' pessimistic one. As suggested above, it will conclude that the literature raises more questions than it answers.

---

[17]Note on citation of interviewees: Until such time as the interviewees have had a chance to review this article and correct any inaccuracies in the statements attributed to them, they will be referred to by number, not by name (e.g. Interviewee 1, Interviewee 2, etc.). The published version of this article will cite interviewees by name.

It therefore makes sense to look, not just to theory, but also to actual experience with the safe harbor approach to privacy regulation. Part IV will describe the Dutch safe harbor program. It will set out the program's legal foundations and describe its central components. It will show that the Dutch program resembles the American proposals and that, like them, it constitutes a form of collaborative governance. Drawing on interviews, Part V will then explore whether the Dutch experience provides reason to be optimistic, or pessimistic, about using collaborative governance for privacy regulation. Part VI will draw on both collaborative governance theory and the Dutch experience with privacy safe harbors to make concrete, normative recommendations as to whether, and how, the United States should implement a collaborative safe harbor approach to privacy regulation.

II. Recent U.S. Proposals Incorporate the Safe Harbor Approach

In recent years, Washington, D.C. has been abuzz with the question of how best to protect individual privacy in the commercial realm. Congressional committees have held hearings on the topic; agencies have hosted roundtable discussions and issued reports; and members of Congress have proposed legislation. The most significant current developments are the three commercial privacy bills pending in Congress and a recently-issued White House report (the "White Paper") that expresses the Obama Administration's views on the topic. The bills and the White Paper differ from each other in some respects. But what is striking about them is what they have in common. Each would have Congress pass comprehensive privacy requirements. Each would then rely, at least in part, on *the safe harbor approach* to implement these broad

legislative requirements.[18] Collectively, the bills and the White Paper represent a rather remarkable and bi-partisan[19] embrace of the safe harbor approach to privacy regulation by both the legislative and executive branches. They suggest that the relatively untested safe harbor approach is fast becoming the dominant model for future commercial privacy law. Due to their similarity, it makes sense to describe the bills and the White Paper as a unified approach and then note such differences as exist.

A. Baseline Privacy Rights

The three bills and the White Paper each envision broad, legislatively-established privacy requirements that would apply to a wide variety of commercial entities.[20] Like the original Fair Information Practice Principles (FIPPs),[21] the bills and White Paper begin with notice and choice. Each would require regulated companies to notify individuals that they are collecting, using and/or disclosing their personal information,[22] and to do so in a way that is "clear," "concise" and

[18]White Paper, *supra* note ___, at 23 (Administration encourages multistakholder groups to develop codes of conduct to implement broad statutory principles.)

[19]The bills have sponsors from both parties.

[20]White Paper, *supra* note ___, at 9-22 (setting forth these rights).

[21]U.S. Dep't of Health, Educ., and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computer and the Rights of Citizens* (July 1973).

[22]Stearns Bill §4(a); Rush Bill § 101, 102; Kerry-McCain Bill § 201; White Paper, *supra* note ___, at 14-15 (transparency). The Stearns and Kerry-McCain bills would also require such notice when a company makes a material change to its privacy policy. Stearns §401(a)(2); Kerry 201(a)(2).

"timely."[23] Each would further require these entities to provide individuals with either opt-out[24] or opt-in[25] choice as to the collection, use, sale and disclosure of their information.[26]

Having stated these requirements, the bills and White Paper go beyond notice and choice to include other important privacy protections. They require companies to take reasonable steps to ensure that the personal information they collect is accurate[27] and to provide individuals with access to their personal information and the opportunity to correct it.[28] They require regulated entities that collect personal information to articulate the purpose for which they intend to use it[29]

---

[23]Stearns Bill §4(b) ("clear and conspicuous" notice); Rush Bill §102(a) (notice that is "concise, meaningful, timely, prominent, and easy-to-understand"); Kerry Bill 201(a) (notice that is "[c]lear, concise and timely"); DOC GP at 31 (notice must be "accessible, clear, meaningful, salient and comprehensible to its intended audience.") The Stearns Bill would further require covered parties to establish and make public a privacy policy that governs the company's "collection, sale, disclosure for consideration, dissemination, use, and security of the personally identifiable informaiton." Stearns Bill §5.

[24]Rush Bill §103(a) (opt-out of collection and use of personal information); Stearns §6(a) (opt-out of the sale or disclosure of personally identifiable information to a non-affiliate); Kerry-McCain Bill 202(a)(1) (opt-out of unauthorized use of personal information); Kerry-McCain Bill 202(a)(2) opt-out of use by third parties for behavioral advertising or marketing).

[25]Rush §104(a)(1) (opt-in required for disclosure of personal information to third-party); Kerry-McCain §202(a)(3)(opt-in required for transfer to third party for unauthorized use where such use carries risk of economic or physical harm); Rushy §104(b), Kerry-McCain §202(a)(3) (opt-in required for collection, use or disclosure of sensitive information); Rush §104(c) (opt-in required before entity can "monitor all or substantially all of the individual's Internet browsing or other significant class of Internet or computer activity and collect, use, or disclose information concerning such activity"); Rush §105(a) (opt-in required before making material change in privacy practices governing previously collected covered information or sensitive information from that individual).

[26]*See generally* Kerry-McCain Bill § 202; Stearns Bill §6; Rush Bill §§ 103, 104; White Paper, *supra* note ___, at 11-14 (individual control).

[27]Rush Bill §201 (regulated entities must establish "reasonable procedures" to ensure the accuracy of the information they collect); Kerry-McCain Bill § 303(a) (same);White Paper, *supra* note ___, at 19-20 (access and accuracy).

[28]Rush Bill § 202(a) (requiring "reasonable access to, and the ability to dispute the accuracy or completeness of, covered information or sensitive information about that individual"); Kerry-McCain bill § 202(a)(4) (same).

[29]White Paper, *supra* note ___, at 15-19 (respect for context); Kerry-McCain bill § 201(a)(1)(B); Rush bill § 101(3), (4).

and to employ it only for that intended purpose.[30] They further require companies to retain the personal information only for so long as it takes to accomplish the intended purpose,[31] and to notify and obtain consent from individuals before using the data for a purpose other than the one originally specified.[32] In sum, the bills and White Paper establish an expanded set of FIPPs that include, not only notice and choice, but also purpose specification, data minimization, opportunities for access and correction, and other protections.

The bills and White Paper also share another feature. Each states its requirements in broad, ambiguous language. For example, the bills and White Paper require companies to notify individuals that they are collecting, using and sharing their personal information and to do so in a way that is "concise, meaningful, timely, prominent, and easy-to-understand."[33] Fair enough. But how is a company to tell whether its notice is sufficiently "clear" or "conspicuous" or "meaningful" or "timely" or "easy-to-understand"?[34] The bills' and White Paper's other main

---

[30]White Paper, *supra* note ___, at15-19 (respect for context); Rush bill § 104(d) (third party recipients of information limited to originally specified purpose).

[31]Rush Bill § 303 (covered entity can retain data "only as long as necessary to fulfill a legitimate business purpose or comply with a legal requirement"); Kerry-McCain Bill § 301 (same); *cf.* White Paper, *supra* note ___, at 21 (giving example where party would have to make sure that it does not retain personal data beyond time needed to achieve stated purpose).

[32]White Paper, *supra* note ___, at 16 (enahanced choice required).

[33]Rush Bill § 102(a); *see also* White Paper, *supra* note ___, at 14 (notice must be "easily understandable and accessible); Stearns Bill § 4(b) ("clear and conspicuous" notice); Kerry Bill § 201(a) (notice that is "[c]lear, concise and timely").

[34] Must a company provide a shorter notice to those who access its Web site on a mobile device than to those who access it on a computer in order to make the notice "easy-to-understand"? If it does so, is the shorter notice still "meaningful"? If a company provides only rudimentary notice on its home page with a link to a more detailed notice, does this qualify as "conspicuous"? Or, must the firm provide the entire notice all at once? If the notice is available in the company's privacy policy, which is on an interior page of its Web site, is that "conspicuous" enough? How does a data broker or other company that does not directly interact with the individuals whose data it holds provide them with "clear" and "timely" notice of its information practices? Can a third party or service provider provide the notice on behalf of the covered entity, or must the entity provide the notice itself?

requirements are similarly open-ended. Companies are to provide the consumer with a choice mechanism that is "easy to access and use"[35] and that offers "reasonable means to exercise an opt-out right and decline consent for such collection and use."[36] Regulated parties may, as a condition of providing a given service or other benefit, require their customers to provide a "*reasonable*" amount of information about themselves, but not more.[37] Companies must institute "*reasonable* procedures to assure the accuracy of the covered information or sensitive information it collects, assembles, or maintains."[38] And they must provide "*appropriate and reasonable*" access to their personal information and mechanisms to correct it.[39] Each of these requirements is stated in very general terms that would make it difficult for a regulated party, even one with good intentions, to know what it needed to do in order to achieve compliance.

Why would the Administration and Congress use such open-ended language? The Administration White Paper suggests a reason. It explains that "in domains involving rapid changes in technology and business practices," it is better to use "flexible standards" that can keep up with the changes rather than to adopt narrow rules that are specific to "technologies and

---

[35]Stearns bill § 7(1); *see also* Kerry-McCain bill § 202(a)(1) (requiring "clear and conspicuous mechanism for opt-out consent.")

[36]Rush bill §103(a)(2).Is it sufficient for a company to post an opt-out notice on its Web site? Does it have to be on the opening page of the site, or can it be on an interior page? Does it matter whether the company provides its primary service or product on the Web, or not? Must the company provide a single opt-out option for all data collection and use, or can it require separate opt-outs for its various data practices? Must each affiliate of the covered entity offer its own opt-out? Or can a parent company offer a single opt-out opportunity that covers all of its subsidiaries? Once again, the questions, and the need for guidance on how to comply, are substantial.

[37]Rush bill § 103(f) (emphasis added).

[38]Rush § 201(a) (emphasis added); *see also* Kerry-McCain bill § 303(a) (requiring "reasonable procedures to ensure that personally identifiable information that is covered information and maintained by the covered entity is accurate.)

[39]Kerry-McCain § 202(a)(4)(A),(B); *see also* Rush § 202(a) (requiring reasonable access to, and the ability to dispute the accuracy or completeness of, covered information.")

practices that exist at the time."[40] While that make sense, it does not answer the question of how regulated parties, faced with such broad, flexible standards, are to figure out how to comply with them.[41]

B. Privacy Safe Harbors

The bills and White Paper provide two mechanisms for clarifying the broad statutory provisions. First, each would authorize the Federal Trade Commission (FTC) to promulgate rules that will flesh out and interpret the statutory requirements.[42] This is traditional agency rulemaking of the type that can be found in many regulatory statutes. Second, the bills and White Paper would authorize the safe harbor approach. That is, each would allow a non-governmental organization–referred to as a "safe harbor program"[43] or a "multi-stakeholder proces"[44]–to draft a set of rules that interprets the statute and spells out how it will apply to a particular sector or

[40]*See, e.g.,*White Paper, *supra* note ___, at 36.

[41]The Department of Commerce acknowledged this point in its Green Paper. *See* Green Paper at 41 ("FIPPs are designed to be comprehensive and general. . . . adopting a FIPPs-based framework would not necessarily help companies determine when they have adequately implemented the principles, leaving the complaint about the lack of certainty in the current commercial data privacy framework unaddressed.")

[42]Stearns bill § 10(b) (rules that say what constitutes compliance with the Act); Rush bill § 102(b) (rulemaking on notice requirements), 201(a) (rulemaking on what constitutes reasonable accuracy); Rush bill § 202(k) (rulemaking on access and correction); Rush bill §§ 301, 302 (. . Rulemaking on security Safeguards), Rush Rush bill § 404 (rulemaking to set forth guidelines for safe harbor program); Kerry-McCain bill § 101 (rulemaking to set security requirements); Kerry-McCain bill § 201(a) (rulemaking to define notice requirements; Kerry 202(a) (rulemaking to define choice mechanisms); Kerry-McCain bill § 501(a) (rulemaking to set requirements for Safe Harbor program).

[43]This is the term that the Kerry-McCain bill uses. Kerry-McCain Bill § 501. The Stearns Bill refers to "self-regulatory programs," Stearns Bill § 9, the Rush bill to "Choice Programs," Rush Bill § 401 and the White Paper to "multi-stakeholder processes," White Paper at 23. For the sake of simplicity, we will refer to all of these as "safe harbor programs."

[44]White Paper, *supra* note ___, at 23.

group of firms.[45] The bills and White Paper then instruct the FTC[46] to evaluate the safe harbor rules to determine whether they are "substantially equivalent to or superior to the protection otherwise provided under" the statute.[47] If the FTC finds that the rules meet this test and formally approves them, then firms that follow the approved rules are deemed to be in compliance with the statute.[48] They inhabit a legal "safe harbor." Companies would be able to choose whether to sign up for a safe harbor program and be governed by its rules, or to stay outside these programs and be subject to the default FTC rules. Those firms that voluntarily committed to follow a given safe harbor program's rules, and then failed to do so, would be subject to FTC Section 5 enforcement for engaging in an "unfair and deceptive" business practice[49] or, potentially, for violating the underlying terms of the Act itself.[50] Safe harbor programs would accordingly be

---

[45]Kerry-McCain bill § 501(a)(1); Stearns bill § 9(c)(1); Rush bill § 403. The rules are sometimes referred to as a "code of conduct." *See* White Paper.

[46]Stearns bill §9(b); Rush bill § 402; DOC GP at 43

[47]Kerry-McCain bill § 501(b)(3); *see also id.* § 502(a) (safe harbor rules must be "substantially the same as or more protective of privacy of individuals"); Stearns bill § 9(c)(1) (self-regulatory programs must contain guidelines and procedures that are "substantially equivalent" to or "greater" than protections that statute itself sets out); Rush bill § 403(2)(d) ("program must establish guidelines and procedures requiring a participating covered entity to provide equivalent or greater protections for individuals and their covered information and sensitive information as are provided under titles I and II.")

[48]Kerry-McCain bill § 502(a); Stearns bill § 9(a)(1), (2); Rush bill § 401; White Paper, *supra* note ___, at 37 (FTC to have authority to grant "safe harbor.")

[49]The White Paper affirms the FTC's ability to use its Section 5 enforcement authority in this way. *See* White Paper, *supra* note ___, at 29 ("companies' failures to adhere to voluntary privacy commitments, such as those stated in privacy policies, are actionable under the FTC Act's (and State analogues) prohibition on unfair or deceptive acts or practices. . . . The same authority would allow the FTC to enforce the commitments of companies under its jurisdiction to adhere to codes of conduct developed through the multistakeholder process"); Federal Trade Commission Act § 5, 15 U.S.C. § 45.

[50]*See* Kerry-McCain bill § 402 (FTC can bring enforcement actions against regulated entities that engage in "knowing or repetitive" violations of Act; Stearns bill § 10 (FTC can bring enforcement actions against regulated entities that violate the Act); Rush bill § 602(a), (b) (same); White Paper at 36 (Congress should authorize the FTC to enforce the Privacy Bill of Rights).

The bills and the White Paper do appear to provide some additional protection for companies that participate in safe harbor programs – perhaps as an incentive to get them to do so. The Stearns bill states that such

both "voluntary" and "enforceable."

These are the common elements. But the bills and White Paper also differ in some respects in their approach to the safe harbor method. To begin with, the bills appear to give industry representatives the lead role in the safe harbor programs that will draft the codes of conduct. The House bills call the entities "self-regulatory programs," a term that suggests that the regulated parties–i.e. business representatives–will take the lead.[51] The Senate bill calls them "nongovernmental organizations."[52] While this term opens the door to many types of private sector and public interest groups, it could certainly encompass an industry trade association. By contrast, the Obama Administration White Paper makes clear that "multi-stakeholder groups" are to draft the codes, and that these groups are to include not only industry representatives but also "privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups."[53]

The bills and White Paper also differ on the scope of the safe harbor. The Stearns bill would extend the legal safe harbor to all of the legislation's substantive provisions–notice, choice, access, data security, etc.[54] The Rush bill would extend the approach to notice, choice and

---

firms should only be subject to enforcement if their violation of the Act results from "willful noncompliance" with the requirements of the self-regulatory program. Stearns bill § 9(a)(2). The Rush bill provides that, in determining amount of civil penalties, a court should take into consideration whether the company participates in a Choice Program. Rush bill § 603(b)(4). The White Paper states that, in enforcement action related to subject matter of codes, "the FTC should consider the company's adherence to the codes favorably." White Paper at ???.

[51]Rush bill § 401; Stearns bill § 9.

[52]Kerry-McCain bill § 501.

[53]White Paper, *supra* note ___, at 23.

[54]Stearns bill § 9(a)(1).

access, but not to data security or data minimization.[55] The Kerry-McCain bill would narrow the safe harbor still further. It expressly extends the it only to the opt-out choice that companies must provide before transferring personal data to a third party[56] and not to the bill's other substantive requirements such as notice, access, correction, and data minimization, although the text is somewhat ambiguous on this point.[57]

The bills and White Paper also diverge with respect to monitoring and enforcement. Each gives the FTC the power to enforce the Act against companies that violate it.[58] The House bills would also require the safe harbor program itself periodically to review whether its participants were in compliance with its rules[59] and to impose consequences on them if they were not.[60] The Stearns bill would go even further and require the program participants annually to self-certify their compliance with the program requirements.[61]

Finally, the White Paper diverges from the bills by calling for multi-stakeholder processes to develop codes of conduct even in the absence of privacy legislation.[62] In such a situation, the

---

[55]Rush bill § 404(6).

[56]Kerry-McCain bill § 501(a)(1), (c). However, a later section of the bill would appear to extend the safe harbor approach to all of the bill's substantive provisions. Kerry-McCain bill § 502(a). Congress will need to clear up this ambiguity should it decide to pass this bill into law.

[57]A later section of the bill would appear to extend the safe harbor approach to all of the bill's substantive provisions. Kerry-McCain bill § 502(a). But this is in conflict with the provision just discussed, § 501(a)(1). Congress will need to clear up this ambiguity should it decide to pass this bill into law.

[58]*See supra* notes ___-___ and accompanying text.

[59]Stearns bill § 9(c)(2)(E).

[60]Rush bill § 403(2). The White Paper also envisions that self-regulatory will provide the first line of enforcement. White Paper, *supra* note ___, at 29.

[61]Stearns bill § 9(c)(2)(B), (C)

[62]White Paper at 24.

safe harbor program would function as a way to identify "best practices" rather than as a vehicle for interpreting statutory requirements. The FTC would use its Section 5 authority to enforce a code of conduct against a company that agreed to abide by it and then failed to do so.[63]

These differences aside, the bills and White Paper display a remarkable consistency in that each embraces the safe harbor approach to privacy regulation. Why do they do this? Why do they depart from the traditional model that relies primarily on agency rules? The Administration White and Green Papers provide a rationale. They explain that the technologies and business models in the information economy are evolving at an unusually rapid pace. This poses two problems for traditional regulation. Slow-moving, notice-and-comment rulemaking will not be able to keep up with rapidly changing technologies, business practices and consumer expectations.[64] Moreover, the regulators themselves will not be able to learn enough about quickly evolving industries to design intelligent rules for them. The Administration papers see codes of conduct as a way to address these problems. As the Administration presents it, stakeholder groups will be able to modify codes of conduct far more quickly than regulators can revise traditional rules. This will help regulation to keep pace with changing business and consumer realities.[65] In addition, codes will bring industry members and consumer advocates to the rule drafting table and so will enable to regulatory process to tap into these parties' superior

---

[63]White Paper at 27.

[64]Green Paper at 47 ("the rate at which new services develop, and the pace at which consumers form expectations about acceptable and unacceptable uses of personal information, is measured in weeks or months. In contrast, a rulemaking can take years and often results in rules addressing services that may be long abandoned."

[65]White Paper at 27 (the safe harbor approach will "enable stakeholders to modify privacy protections in response to rapid changes in technology, consumer expectations, and market conditions, to assure they sufficiently protect consumer privacy"); Green Paper at 20 ("[t]he premise behind this approach was that industry codes would develop faster and provide more flexibility than legislation or regulations").

knowledge about evolving business, technological and consumer realities.[66] The result should be more responsive and intelligent rules that do a better job of keeping up with rapidly changing conditions.[67]

III. Collaborative Governance Theory and the Questions that it Raises

The safe harbor approach sounds great on paper. But will it work the way that the Administration papers and (implicitly) the Congressional bills say that it will? One way to explore this question is to see what scholars have had to say about it. Recent years have seen the emergence of a substantial literature on collaborative governance.[68] These writings use the term to refer to those regulatory processes in which government officials and the regulated parties expressly share responsibility for the drafting and/or enforcement of rules.[69] Privacy safe harbor

---

[66]Green Paper, *supra* note ___, at 5 ("Commercial data privacy policy must be able to evolve rapidly to meet a continuing stream of innovations. A helpful step would be to enlist the expertise and knowledge of the private sector . . . in order to create voluntary codes of conduct that promote informed consent and safeguard personal information.")

[67]Green Paper at 47 ("A dynamic system in which private and public stakeholders participate would yield privacy practices that are more responsive to evolving consumer privacy expectations than would a traditional rulemaking system.")

[68]*See, e.g.,* Jody Freeman, *Collaborative Governance in the Administrative State,* 45 UCLA L. REV. 1 (1997) [hereinafter Freeman, *Collaborative Governance*]; Philip J. Harter, *Collaboration: The Future of Governance*, 2009 J. DISP. RESOL. 411 [hereinafter Harter, *Future of Governance*]; NEIL GUNNINGHAM & DARREN SINCLAIR, LEADERS AND LAGGARDS: NEXT GENERATION ENVIRONMENTAL REGULATION 134-156 (2002); JOSEPH V. REES, REFORMING THE WORKPLACE: A STUDY OF SELF-REGULATION IN OCCUPATIONAL SAFETY (1988); LYLE SCRUGGS, SUSTAINING ABUNDANCE: ENVIRONMENTAL PERFORMANCE IN INDUSTRIAL DEMOCRACIES (2003).

[69]Freeman, *Collaborative Governance*, *supra* note ___, at 6 (shared responsibility at all stages in rulemaking process); *id.* at 30 (shared responsibility in monitoring and enforcement). Collaborative governance can be distinguished from government-centered regulation, in which government holds the primary responsibility for drafting and enforcement of rules, and from industry self-regulation, in which industry bears this primary responsibility. Defining collaborative governance in this way is not intended to suggest that industry plays no role in traditional, government-centered rulemaking. It does play a role through written comments and other, more informal contributions. It is also not to say that government plays no role in industry self-regulation. Government frequently

programs are a form of collaborative governance. Regulatory negotiations (reg-neg) would be another, more familiar example of this regulatory approach.

One group of scholars, led by Professors Jody Freeman of Harvard Law School and Philip Harter of the University of Missouri School of Law, argue that the collaborative approach will perform better than traditional administrative rulemaking.[70] Another group criticizes the method. The debate between proponents and critics focuses on four, key areas: (1) whether collaborative methods are procedurally superior to notice-and-comment rulemaking; (2) whether they produce substantively better rules; (3) whether they engender better compliance; and (4) the true motivations behind the recent interest in collaborative methods. This section will set out the proponents,' and then the critics', views on these topics in order to assess what the literature can tell us about this regulatory approach.

A. The Proponents of Collaborative Governance

The proponents' arguments center on four areas: process, substance, compliance, and the reasons for the interest in collaborative governance.

1. *Process*.

As the proponents see it, the central problem with traditional rulemaking is that it is

---

gives industry feedback on its self-regulatory efforts. The point is that collaborative governance expressly and intentionally puts the emphasis on shared responsibility for rule drafting and enforcement. Government-centered rulemaking emphasizes the regulators' role, and industry-self regulation stresses that of the industry itself. The categories are not pure types but rather matters of degree. One way to think about it is that collaborative governance stands in the center of a continuum that begins with pure industry self-regulation, and ends with entirely government-driven prescriptions. Other forms of governance do not often inhabit the extreme ends of this continuum but they lie along it at a different place than collaborative governance.

[70] *See* Freeman, *Collaborative Governance, supra* note ___; Harter, *Future of Governance*, *supra* note ___; REES *supra* note ___, GUNNINGHAM *supra* note ___, SCRUGGS *supra* note ___ .

adversarial in nature.[71] Interested parties in a notice-and-comment rulemaking occupy a position similar to litigants in a court proceeding. They stand at arms length from the neutral arbiter (here, the agency) and submit written briefs (comments) that they hope will convince it to adopt their position.[72] Each group seeks to push the agency as hard as it can in its own direction, believing that it must do so in order to offset its opponents' equally vigorous advocacy.[73] This has a number of negative effects. It prevents parties from revealing their true priorities, instead leading each to put forth a one-sided, extreme version of its position.[74] It deters parties from sharing information about the nature of the regulatory problem, and possible solutions to it, for fear that others might use the information to undermine their position.[75] Thus, even where companies know of a cost-effective way to achieve social goals they may not reveal it for fear of undermining their argument that the anticipated regulations will prove too costly and should be eliminated altogether. Finally, it often leads interested parties to challenge final rules in court

---

[71]Freeman, *Collaborative Governance*, *supra* note ___, at 19 (traditional regulation assumes that relationships are adversarial).

[72]Freeman, *Collaborative Governance* at 11-12, 19; citing Harter.

[73]*See* Philip J. Harter, *Negotiating Regulations: A Cure for Malaise*, 71 GEO. L. J. 1, 19-23 (1982) (in traditional regulation both agencies and parties take extreme positions).

[74]Freeman, *Collaborative Governance, supra* note ___, at 11-12 (Interest groups "often take extreme positions in notice and comment, preferring to posture in anticipation of litigation than focus on the regulatory problem posed by the agency"); Harter, *Negotiating Regulations*, *supra* note ___, at 19-23 (parties do not express their true concerns).

[75]Freeman, *Collaborative Governance, supra* note ___, at 15-16 (under the traditional model, the agency and the regulated party "typically adopt an adversarial posture toward each other" and this results in a failure to share useful information); Harter, *Negotiating Regulations*, *supra* note ___, at 19-23 (parties do not want to share information that may reveal weaknesses). Freeman, *Collaborative Governance,* at 11 n. 26, citing Harter.

Where they do share information, they are likely to do so in rulemaking comments that often come so late in the process that agencies cannot make good use of it. Freeman, *Collaborative Governance, supra* note ___, at 12-13. Rulemaking process itself also works against timely sharing of information. Opportunity for public comment only after Notice of Proposed Rule Making published. This often too late to reshape fundamentally the rule that the agency as already proposed. Freeman, *Collaborative Governance, supra* note ___, at 12.

resulting in further delays and the "ossification" of the rulemaking process.[76]

As the proponents see it, collaborative processes are not adversarial. Instead, they confront the government and interested parties with a regulatory problem and get them to work together on finding a mutually acceptable solution to it. They thereby "reorient the regulatory enterprise around joint problem solving."[77] In this sense they are closer to dispute resolution than to litigation. This change alters the dynamic in highly positive ways. By requiring parties to interact face-to-face over multiple meetings, collaborative methods force them to respond to each others' arguments and to offer positions of their own that the other parties might actually find to be convincing. This deters the posturing and extreme positions that are so characteristic of adversarial rulemaking.[78] The frequent interactions can have another salutory effect. They can build an atmosphere of familiarity and trust among the participants.[79] This can make them more willing to share important information.[80] It can also lead them to reveal their true, bottom-line positions and so increase the chance of finding a solution that allows each to meet its core

---

[76]Thomas O. McGarity, *Some Thoughts on "Deossifying" the Rulemaking Process*, 41 DUKE L. J. 1385, 1397-98 (1992).

[77]Freeman, Collaborative Governance, *supra* note ___, at 22; Leaders and Laggards at 109.

[78]Freeman at 23; Scruggs at 143 (where trying to build consensus, must acknowledge some information that contrary to their own original positions).

[79]Freeman, *Collaborative Governance, supra* note ___, at 24 (process of working together itself forges trust, good faith, civility. Improved relationships); Scruggs at 143 (reduces "ill will").

[80]More information sharing and collaborative deliberation. (Freeman UCLA 22-24) (see Harter arguments for reg-neg?); More information sharing than traditional regulation. Agency as engaged facilitator of multi-stakeholder processes. UCLA at 22, 23 Fewer incentives to hide industry secrets. Scruggs at 145. Scruggs at 146 ("produce a great deal of valuable and effective information for industry and regulators. Government and industry can get a better idea of the likely costs and benefits of particular policies and may be able to negotiate more efficient regulation in the process.") Greater generation and diffusion of information. Leaders and Laggards at 109. Leaders/Laggards at 97 ("assumption that industry knows best how to abate its own environmental problems.")

needs.[81]

The proponents further point out that the parties to a collaborative negotiation have a hand in drafting the rules and so will be less likely to challenge them in court. They are also free to arrive at initial solutions, and revise them over time, without having to observe the lengthy formalities of notice-and-comment rulemaking.[82] These two factors should make collaborative methods more nimble and adaptive than traditional rulemaking processes.[83] This is particularly important in areas where technologies, business realities and consumer expectations change rapidly. In sum, the proponents claim that collaborative *processes* will generate a problem-solving rather than an adversarial mentality, promote trust, information sharing and consensus-building, and respond quickly to changing technologies and circumstances.[84]

2. *Substance*

The proponents also maintain that collaborative methods will generate better rules.[85] To

---

[81]Freeman, *Collaborative Governance, supra* note ___, at 7, 22, 23; Leaders and Laggards at 109 (multiple parties working together will learn from each other and so will come up with more creative solutions than any single party working alone); Scruggs at 144 (allow firms to innovate in figuring out ways to meet these goals).

[82]Freeman, *Collaborative Governance, supra* note ___, at 14, 22, 26, 28. They further recommend that such initiatives build in feedback mechanisms for evaluating and reassessing the existing rules on an ongoing basis.

[83]Freeman, *Collaborative Governance, supra* note ___, at 9, n. 19 ("There appears to be consensus that the rule-making process is excessively costly, rigid, and cumbersome) (citing sources).

[84]Freeman, *Collaborative Governance, supra* note ___, at 26 (collaborative methods will be more likely to produce "creative, implementable regulatory solutions capable of adaptation and revision than [will] informal notice and comment.")

[85]Some go the next step and argue that collaborative methods will produce better social results. For example, Scruggs looked at national performance on a number of key environmental indicators. He found that those nations in which strong economic interest groups and government collaborated and sought to reach consensus on environmental standards (neocorporatism) consistently outperformed nations that employed more pluralist, adversarial systems. Some have claimed improved outcomes. Scruggs at 15, 123, 146. Scruggs claims that "[t]he results are dramatic. Countries with corporatist institutions have systematically higher environmental performance than do countries with more pluralist arrangements." Scruggs p. 153. He maintains that they "call into question the claim that neocorporatist institutions necessarily undermine better environmental policies and performance." Scruggs at 124.

begin with, by bringing regulated companies into the rule drafting process and making them more willing to share information, collaborative methods tap into these parties' superior knowledge about technology, industry realities and low-cost compliance solutions. They can then use this information to produce more tailored, workable, and cost-effective rules than those that traditional rulemaking would generate.[86] By getting regulators and interested parties to reveal their bottom-line needs in a problem-solving environment, collaborative methods should also tend to generate more creative, win-win solutions.[87] Finally, proponents argue that nimble collaborative methods will be more likely to produce rules that keep up with changing realities than will cumbersome, notice-and-comment rulemaking.

Another study reached a similar conclusion with respect to workplace safety. It examined the Cooperative Compliance Program (CCP), a co-regulatory alternative to traditional OSHA regulations in which unions, management, and regulators negotiated and reached consensus on workplace safety standards. The study found that CCP sites had significantly lower accident rates than comparable, traditionally-regulated sites, Rees at 2, 224, 233, and that all participants responded favorably to the program. Rees at 233. The claim that collaborative instruments yield better social results than traditional ones is a controversial one and is not universally accepted. *See* Leaders and Laggards at 106 (mixed results) Much further study will be required to validate it. The studies just cited are important, not because they prove the claim, but because they show it to be a serious one that deserves further investigation.

[86]Freeman, *Collaborative Governance, supra* note ___, at 22, 27. Freeman, *Collaborative Governance, supra* note ___, at 26 (Generate solutions that work on the level of implementation); Leaders and Laggards at 104 (use this method so as not to put industry at competitive disadvantage). Scruggs at 152 (Creates "a regime where flexible, cost-effective implementation of high standards can occur"); Leaders and Laggards at 104 (flexibility of standards, and innovation it encourages, allows firms to come up with lower cost solutions). Scruggs at 146 (more upstream, preventative solutions that are less costly than end of pipe); Leaders and Laggards at 104 (firms have more information and so can come up with lower-cost, better tailored means of achieving).

Proponents further argue that such combined efforts comport better with democratic principles than the traditional method that seeks to insulate government decision-making. Participation of interested parties at various stages of decision-making process. UCLA at 22. Independent democratic value. Also, can play a transitional role leading to more effective traditional regulation. Leaders and Laggards at 107. Use when premature to regulate directly. Problem at early stages. Regulators do not yet know enough. Through co-regulatory process, regulators can learn more about nature of the issue and possible solutions to it. When time is ripe, can transition to more direct regulation.

[87]Freeman, *Collaborative Governance*, *supra* note ___, at 11 n. 26 citing Harter, 12 & n. 29, 19. Some even claim that, in exchange for the greater flexibility that comes with collaborative rulemaking, industry will be more likely to accept ambitious standards. For this reason, they believe that collaborative governance can yield more stricter standards than traditional regulation otherwise would. Scruggs at 146-47.

3. *Compliance*

The proponents claim that collaborative governance also improves compliance and enforcement. They start with the idea that, due to limited enforcement resources, any system that relies exclusively on government inspections will necessarily produce only partial compliance.[88] To achieve something closer to full compliance regulatory systems must activate the attitudes and social norms that generate pro-social behavior even when no one is looking. The proponents maintain that collaborative processes will do a far better job of this than will traditional administrative rulemaking. Imposing rules from the outside tends to breed resistance. Bringing regulated parties into the rule drafting process, by contrast, gives them a sense of ownership over the rules [89] and tends to generate rules that they find workable.[90] Businesss should comply more readily with such rules than with those that regulators impose on them.[91] The proponents further maintain that collaborative mechanisms will generate greater industry self-policing either because those who helped to draft and intend to comply with the rules want to bring potential

---

[88]*Cf.* Freeman, *Collaborative Governance, supra* note ___, at 16 (discussing EPA's difficulty in monitoring hundreds of thousands of permitted facilities).

[89]Freeman at 12, 24.

[90]Leaders and Laggards at 109 (lower cost regulation more politically acceptable generally). Scruggs at 146 (increased flexibility and efficiency of standards makes easier to accept).

[91]Freeman, *Collaborative Governance, supra* note ___, at 12, (23?). Other factors also contribute to acceptance. Where government collaborating with an entire sector, then the sectoral representatives can arrange to compensate losers, and so reduce resistance to regulatory change. Scruggs at 14, 149. Corporatist groups can establish processes for compensating distributional losers from regulatory advances. This reduces chance that concentrated parties will resist regulatory change. Reduce likelihood that small groups will intensely resist collective environmental interest. Helps to overcome collective action problem where diffuse benefits make it hard for beneficiaries to organize to promote policy change, but concentrated costs encourage losers to fight hard against change. Thus, corporatism can facilitate regulatory change by working out mechanisms for compensating losers.

free-riders up to this standard,[92] or because they feel a sense of mutual accountability with the other parties engaged in the process and want to make good on this.[93]

4. Reasons for choosing a collaborative approach:

Governments must make a real effort to depart from ingrained, traditional rulemaking processes and shift to collaborative governance. Proponents believe that they do this where they have a strong need for the virtues of this regulatory approach, as just described. They believe that the recent shift to an information economy, with its rapid changes in technologies and business models, exacerbates the problems with slow, costly, traditional rulemaking processes. They argue that this shift is one of the reasons that governments are more interested today in collaborative models of governance which promise more adaptive, intelligent and cost-effective rules.[94] This claim resonates strongly with the Obama Administration's rationale, described above,[95] for utilizing a this alternative form of regulation.

B. The Critics' View

The critics take issue with the proponents' claims on all four levels – process, substance,

---

[92]Scruggs at 14, 144, 147, 148, 150, 151. If industry association ("peak interest groups," in Scrugg's terminology) encompasses most of industry, then can bring on board those who would otherwise free ride. Leads to maximization of public benefits, rather than individual rents. See Mancur Olson. Ensure that industry group acts as a whole. Instead of individual sub-groups acting in own interest and "rent-seeking." Some maintain that the relationships formed between industry leaders and government regulators during the course of negotiations will cause the parties to feel accountable to each other for the success of their agreed-upon framework. Freeman, UCLA at 22.

[93]Freeman at 30.

[94]Dennis D. Hirsch, *Lean and Green? Environmental Law and Policy and the Flexible Production Economy*, 79 INDIANA L.REV. 611 (2004).

[95]*See supra* notes ___-___ and accompanying text.

compliance and the reasons for the recent interest in this approach.

1. *Process*

The critics believe that industry will use its place at the drafting table to push for rules that serve its own interests[96] and that, due to industry's informational superiority and political clout, regulators will not be able to check this tendency sufficiently. They accordingly compare collaborative processes, not to dispute resolution, but to the proverbial "fox guarding the hen house." They prefer notice-and-comment rulemaking which requires all parties to work through formal, written channels, reduces ability to bring pressure on regulators, and levels the playing field.

The critics express particular concern about those collaborative processes – such as the Dutch code of conduct program and, potentially, the recent Congressional proposals for privacy safe harbors[97] – that allow industry alone to draft the rules and negotiate them with the regulators before bringing public interest stakeholders into the process. They see such industry-government negotiations as opportunities, not for cooperative problem solving, but for backroom deal-making that will favor industry and undermine the public interest. Some take this argument a step further and assert that the road of collaborative governance leads, ultimately, to "agency capture" – the scenario in which the regulators come to serve industry's interests rather those of the broader society.[98] They note that the conditions that lend themselves to industry-government

---

[96]Leaders and Laggards at 105.

[97]While the Obama Administration policy papers expressly call for a *multi*-stakholder process, the commercial privacy bills do not and could be read to allow an industry-only group to draft a set of safe harbor rules and submit them to the FTC for approval.

[98]Scruggs at 128; Rees at 12, 236; Leaders and Laggards at 105. On regulatory capture, see sources cited at Rees p. 20.

collaboration – frequent, confidential meetings to discuss key issues of policy – are the same as those that have led in the past to improper influence and even agency capture.[99]

The critics further maintain that collaborative methods will not produce the productive, new dynamics that the proponents claim. They believe that industry will share information only where doing so suits its purposes and will not be as forthcoming as the proponents predict. They further question whether businesses, driven by the need to increase shareholder value, will drop their adversarial stance and truly engage in good faith problem-solving.

2. *Substance*

The critics believe that these procedural flaws will undermine the substance of the rules that these mechanisms produce. They question the proponents' claims of information-rich, creative rules that meet everyone's core interests. Instead, they predict that collaborative processes, stacked as they are in industry's favor, will tend to generate overly lenient rules that place business interests over those of the public.[100] They further point out that industry representatives are likely to come from well-established firms. As such, they will have an incentive to promote rules that increase the barriers to entry and secure their own competitive position. This will be particularly damaging for the fast-changing information economy which relies so heavily on innovation and entrepreneurial energy.

3. *Compliance*

As the critics see it, collaborative governance will require regulators to establish a more cooperative relationship with industry. This will make it more difficult for them to take hard-

[99]Leaders and Laggards at 105 (quoting Responsive Regulation).

[100]Scruggs: But perceived zero-sum trade-offs are often false. P. 137.

nosed enforcement positions that could damage these relationships. Industry members will perceive this decreased enthusiasm for enforcement and, acting rationally, will put less effort into compliance. The result will be a decrease in compliance, not the increase that the proponents predict. The critics further doubt whether industry trade associations, which must look to their membership for support and funding, can be counted on to police their own members and fill this gap.

4. *Reasons for choosing a collaborative approach*

In sum, the critics believe that proponent's dream of collaborative governance will turn out to be a nightmare of industry influence, lenient standards and loose enforcement, with the public paying a heavy price. They prefer traditional notice-and-comment processes in which the rulemaking power remains squarely in the hands of government regulators. They view recent government moves away from this tried-and-true method, and towards collaborative approaches, not as a response to the information economy but as an extension of the deregulatory movement that seeks to tear down the vital structures of the administrative state. They maintain that such efforts should be resisted.

IV. Dutch Data Protection Codes of Conduct: An Experiment in Collaborative Governance

Collaborative governance theory crystalizes the questions about this regulatory method but does not answer them. It does not tell us whether to embrace, or reject, the collaborative approach to privacy regulation. To figure this out we need to look beyond theory, to practice. The Dutch data protection codes of conduct program gives us an excellent opportunity to do so.

They represent more then twenty years of regulatory experience with the very instrument – industry codes of conduct and safe harbor agreements – that federal legislators and policymakers are getting ready to use to protect Internet privacy. While the Netherlands and the United States are different countries, the Dutch experience should shed at least some light on the merits of collaborative governance in the privacy area. This part will introduce the Dutch code of conduct program. It will outline the initiative's legal and programmatic foundations and will explain why the Dutch decided to use this form of regulation in the first place. It will show that the Dutch codes of conduct are, indeed, a form of collaborative governance and that they are similar in nature, though not identical, to the U.S. "safe harbor" programs. Part V will draw on interviews with Dutch regulators, industry representatives and privacy experts to determine what the Dutch experience can tell us about the merits of collaborative privacy regulation. Based on this analysis, Part VI will make normative recommendations for U.S. privacy law and policy. Readers who are already familiar with European data protection law and the Dutch code of conduct program, and are particularly interested in the research findings and policy recommendations, can move directly to Part V.

A. Legal Foundations

Just as the proposed U.S. privacy bills would establish a safe harbor initiative, so Dutch Data Protection Act authorizes and establishes the Dutch code of conduct program. In order to understand the codes, it is accordingly important to begin with European data protection law and the Dutch data protection statutes that implement it on a national level.

1. *European Data Protection Law*

There have been two generations of European data protection statutes. The first, passed in

the 1970s and 1980s, focused on *stand-alone databases* of personal data.[101] These statutes regulated the "data users" who ran these databases. They sought to protect the "personal data files" that made up the databases and that contained personal information about specific individuals.

Over time, organizations developed new ways of storing and manipulating personal data. Instead of using stand-alone databases, they began to employ more networked, dispersed and transient systems.[102] These new realities did not fit well with the first generation statutes which assumed the existence of stand-alone databases. By the early 1990s, European nations needed a new, updated set of data protection laws. At about this time, the European Commission began work on a data protection directive that would harmonize data protection laws throughout the European Union.[103] Like other EU directives, this one would be a legislative act of the European Union. It would set out broad standards and require the E.U. member nations to pass implementing statutes to incorporate these standards into national law.

In 1995 the Commission proposed, and the European Parliament and the Council of the European Union formally adopted, the Directive on the Processing of Personal Data (the "1995 Data Protection Directive"). The Directive required each member state to pass implementing legislation and to establish a Data Protection Authority to administer these laws.[104] Unlike the

---

[101]KORFF, DATA PROTECTION LAWS, *supra* note ___, at 13; Koops, *Evolution*, *supra* note ___, at 4.

[102]Koops, *Evolution*, *supra* note ___, at 4.

[103]The Commission hoped that the new directive would facilitate the free flow of information within the E.U., and to ensure protection of the right to privacy that the European Convention on Human Rights had recognized as fundamental. ECHR Art. 8. The 1995 Directive states, in Article 1(1), that "Member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

[104]95/46/EC Art. 28.

first generation statutes, the Data Protection Directive took account of the new type of decentralized and networked information systems. It took as its organizing principle, not the personal data file in the stand-alone database, but rather the "processing" of personal data no matter where that data happened to be located.[105] It targeted its requirements, not at the owner or user of a particular computer, file or filing system, but rather on the "controller" of a given processing operation, a term of art that referred to the entity that "determine[d] the purposes and means of the processing of personal data."[106] It sought to protect, not the personal data file, but rather the "data subject," by which it meant the individual whose personal data the controller was employing in the processing operation which could involve many data files.[107] To implement the 1995 Data Protection Directive, European Member states passed a second generation of data protection statues. These second generation laws adopt the Directive's basic concepts and structure. They focus on data processing, regulate data controllers, and seek to protect data subjects.

2. *The 1989 Law on Personal Data Files*

The Dutch have passed two data protection acts, the 1989 Law on Personal Data Files or Wet persoonregistraties and the 2000 Personal Data Protection Act or Wet bescherming persoonsgegevens. This section will treat these two statutes separately. Later sections will refer

[105]KORFF, DATA PROTECTION LAWS, *supra* note ___, at 13. The Directive defined the "processing" of personal data to encompass "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking erasure or destruction." 95/46/EC Art. 2(b).

[106]Directive 95/46/EC Art. 2(d); KORFF, DATA PROTECTION LAWS, *supra* note ___, at 13.

[107]95/46/EC Art. 2(a).

to them collectively as the"Data Protection Act" when discussing Dutch data protection law more generally. The two Dutch statutes follow the general European pattern. The 1989 Law on Personal Data Files followed the first generation model.[108] As its name suggests, it sought to protect the "personal data files" contained in large, stand-alone databases.[109] To this end, it established regulatory requirements for "data users" which it defined as the parties "with control over personal data files."[110] It also set up a regulatory agency, the Registration Chamber (Registratiekamer), to oversee the implementation of the Act.[111]

The Law on Personal Data Files established many requirements for data users. For example, it required data users, each time they opened a new personal data file, to "register" that file with the Registration Chamber.[112] To do so, they had to submit a form that stated, among other things, the purpose for which they had opened the personal data file and the types of data they would be entering in it.[113] The Law further allowed data users to employ the personal data in their files *only* for the purpose for which they had collected the data (as stated in their registration form) and for other purposes that were "compatible" with the initial purpose.[114] The Law also regulated the relationship between the data user and the data subject. It required a data user to

---

[108]Koops, *Evolution*, *supra* note ___, at 4; KORFF, DATA PROTECTION LAWS, *supra* note ___, at 13.

[109]Law on Personal Data Files, § 1; NUGTER, *supra,* note ___, at 148.

[110]Law on Personal Data Files, § 1; NUGTER, *supra,* note ___, at 148-49.

[111]Law on Personal Data Files, § 37; NUGTER, *supra,* note ___, at 173.

[112]Law on Personal Data Files, § 24; NUGTER, *supra,* note ___, at 165. In theory, this would make the Registration Chamber the repository of a vast database of its own that would contain information about the existence of many of the personal data files created throughout the country.

[113]Law on Personal Data Files, § 24; NUGTER, *supra,* note ___, at 165.

[114]Law on Personal Data Files, § 6(1); NUGTER, *supra,* note ___, at 168.

notify each data subject individually the first time that it recorded information about that person in a data file.[115] Where a data subject requested it, the Law further required the data user to provide an overview of the information that it held about that data subject;[116] to let that person correct or erase inaccurate data;[117] and to tell the data subject whether it had disclosed information about him to a third party.[118] Technological advances and the issuance of the 1995 Data Protection Directive soon rendered the 1989 Law on Personal Data Files, a first generation statute, out-of-date.[119] The Dutch needed a new data protection law.

3. *The 2000 Personal Data Protection Act*

In 2000, the Dutch Parliament passed the Personal Data Protection Act or Wet bescherming persoonsgegevens. The Personal Data Protection Act implements the 1995 European Data Protection Directive[120] and follows the second generation model as we have described it. It applies to all "processing" of personal data and does not limit itself to personal data files or stand-alone databases.[121] It targets "responsible parties," which it defines as the persons or organizations that "determine[] the purpose of and means for processing personal data" (a term directly analogous to the 1995 Directive's term "controller.") It seeks to protect

---

[115]Law on Personal Data Files, § 28(1); NUGTER, *supra,* note ___, at 161.

[116]Law on Personal Data Files, § 29(1); NUGTER, *supra,* note ___, at 157.

[117]Law on Personal Data Files, § 31(1); NUGTER, *supra,* note ___, at 158.

[118]Law on Personal Data Files, § 32; NUGTER, *supra,* note ___, at 159.

[119]Koops, *Evolution*, *supra* note ___, at 4; Korff, *The Dutch Data Protection Law*, § 1.

[120]Korff, *The Dutch Data Protection Law,* § 1 (2000 law replaces the 1989 law in order to implement the 1995 Directive).

[121]Personal Data Protection Act, Ch. 2 (establishing "Conditions for the Lawful Processing of Personal Data"); Korff, *Dutch Law,* § 2..

data subjects.[122] It creates a Data Protection Authority known as the College Bescherming Persoonsgegevens (CBP).[123] From this point forward, and for the sake of simplicity, this article will refer to both the Registratiekamer, which the 1989 Law created, and the CBP, which the 2000 law established, as the Dutch Data Protection Authority ("DPA").

The 2000 Law's most important provisions are those that define the line between acceptable, and unacceptable, processing of personal data. Following the 1995 Directive, the 2000 Dutch Personal Data Protection Act draws the line by means of five broad *principles*, and a complementary set of six *criteria*.[124] To be legally acceptable, a given data processing operation must comply with all five of the principles, and satisfy at least one of the criteria.

Under the five data processing principles, responsible parties may process data only where: (1) they do so "fairly and lawfully";[125] (2) the data were collected for defined purposes, and the processing is "not . . . incompatible" with these purposes;[126] (3) the data are "adequate, relevant and not excessive" in relation to the purposes for which they are being processed;[127] (4) the data are as accurate and current as they need to be to serve the defined purpose;[128] and (5) the

---

[122]Korff, *The Dutch Data Protection Law,* § 2.

[123]The official name for the DPA is the College Bescherming Persoonsgegevens. This article will refer to it as the Dutch DPA.

[124]Korff, *Dutch Law*, § 4 (2000 law incorporates the principles and criteria laid out in the 1995 Directive).

[125]Personal Data Protection Act, Art. 6; 95/46/EC Art. 6(1)(a).

[126]Personal Data Protection Act, Arts. 7, 9; 95/46/EC Art. 6(1)(b).

[127]Personal Data Protection Act, Art. 11; 95/46/EC Art. 6(1)(c).

[128]Personal Data Protection Act, Art. 11; 95/46/EC Art. 6(1)(d).

responsible parties retain the data no longer than is necessary for the purpose.[129] Processing operations that do not satisfy each of these principles are illegitimate and can violate the Act.

In addition, processing operations must satisfy at least one of the following criteria which focus on data subject consent, or exceptions to it. The criteria, at least one of which must be met, are: (1) the data subject unambiguously consented to the processing;[130] (2) the processing is necessary for "the performance of a contract" into which the data subject entered;[131] (3) the processing is necessary for "compliance with a legal obligation" to which the data controller is subject;[132] (4) the processing is necessary "to protect the vital interests of the data subject;"[133] (5) the processing is necessary for the performance of a task that the controller carries out "in the public interest;"[134] or (6) the processing is necessary to accomplish the legitimate purposes of the controller, unless the data subject's "fundamental rights and freedoms" override these purposes.[135]

It is beyond the scope of this article to describe more fully the provisions of 2000 Personal Data Protection Act, or of the 1989 Law on Personal Data Files. Other excellent resources already serve this purpose. Instead, this Article focuses on two things that 1989 and 2000 laws have in common. First, as was true with the proposed Congressional bills described

---

[129]Personal Data Protection Act, Art. 10; 95/46/EC Art. 6(1)(e).

[130]Personal Data Protection Act, Art. Art. 8(a); 95/46/EC Art. .

[131]Personal Data Protection Act, Art. 8(b); 95/46/EC Art. .

[132]Personal Data Protection Act, Art. 8(c); 95/46/EC Art. .

[133]Personal Data Protection Act, Art. 8(d); 95/46/EC Art. .

[134]Personal Data Protection Act, Art. 8(e); 95/46/EC Art. .

[135]Personal Data Protection Act, Art. 8(f); 95/46/EC Art. .

above,[136] both statutes employ broad language that requires extensive interpretation before it can be applied to specific industries and firms. For example, the 1989 law and the 2000 law each require that data users and controllers employ personal data only for the purpose for which they had initially collected it, or for purposes that were *compatible* with that purpose.[137] However, they do not clarify how the user is to tell whether a given use is, or is not, "compatible" with a given purpose. For example, if a company that owns both a bank and an insurance company collects financial information from its bank customers and uses it to market banking products to them, can it also use this information to market insurance products to these customers? Is that a "compatible" use because both uses involve marketing, or an incompatible one because one involves the banking side of the business and the other the insurance side? The 1989 and 2000 Laws, with their broad language, do not define "compatible" or spell out how it applies to the banking industry. They therefore leave points such as this one unclear and open to interpretation.[138]

The 2000 Law's broadly worded principles and criteria open up a host of other ambiguities and interpretative questions. How is a given data controller to know whether the data employed in a given processing operation are "adequate, relevant and not excessive" in relation

---

[136]*See supra* notes ___-___ and accompanying text.

[137]Law on Personal Data Files, § 6(1); NUGTER, *supra,* note ___, at 168; Personal Data Protection Act, Arts. 7, 9.

[138]The 2000 Act does offer a bit more guidance on how to tell whether purposes are compatible or not. It instructs responsible parties to take into account: "a. the relationship between the purpose of the intended processing and the purpose for which the data have been obtained; b. the nature of the data concerned; c. the consequences of the intended processing for the data subject; d. the manner in which the data have been obtained, and e. the extent to which appropriate guarantees have been put in place with respect to the data subject." Personal Data Protection Act, Art. 9(2). These additional guidelines remain quite broad and do not resolve many of the ambiguities about how this requirement applies to specific businesses and their uses of data.

to the purposes for which they are being processed?[139] How is it to know whether they are as accurate and current as they need to be to serve the defined purpose,[140] or whether it is retaining the data for longer than is necessary for the purpose?[141] How is it to determine whether the processing is required to protect a "vital interest" of the data subject,[142] or whether the data user's legitimate purposes override the data subject's "fundamental rights and freedoms"?[143] Each of these very basic issues requires a judgment call. Each requires that someone interpret the statute's broad principles and apply them to particular business sectors, firms and situations.[144]

Yet–surprisingly from an American point of view– the Dutch statutes do not provide an administrative mechanism for supplying these interpretations. They do not require, or even authorize, the Data Protection Authority to promulgate regulations fleshing out and interpreting the statutes. Instead – and this is the second main thing that these statutes have in common – the Dutch laws delegate this task to the industry sectors themselves. As was briefly explained above, each statute allows industry representatives to draft a "code of conduct" that specifies how the

[139]Personal Data Protection Act, Art. 11; Interviewee 12 (16:00) (raising this issue).

[140]Personal Data Protection Act, Art. 11.

[141]Personal Data Protection Act, Art. 10.

[142]Personal Data Protection Act, Art. 8(d).

[143]Personal Data Protection Act, Art. 8(f).

[144]Interviewee 12 16:00 (Broad provisions. Much room for interpretation. e.g. can use for original purpose, but not incompatible purpose. What is incompatible? Varies from sector to sector. e.g. Can store only so long as is necessary for original purpose. What is necessary period of time? Varies from sector to sector."A very vague law. How long may I store this data? Three years? Five years? Seven years? Those are the gaps that [the codes] are filling." Interviewee 12 16:15.

statutory requirements apply to their specific sector[145] Sectors often start this process by figuring out how they collect and use personal data in their operations. They then review the Data Protection Act, apply this law to their industry circumstances, and identify the main questions or areas that need interpretation.[146] Finally, they draft a code that would provide "an interpretation of these questions."[147] Often, the sector meets with the regulatory agency along the way to talk through issues and discuss their progress.[148] Once the sector has drafted the code, it submits it to the Data Protection Authority for approval.[149]

The Act requires the Authority to reach a preliminary decision within thirteen weeks of

---

[145]An industry trade association generally drafted the code on behalf of the sector. For example, the Netherlands Bankers Association created a data protection committee, made up largely of lawyers, and gave them the task of drafting the code. Interviewee 1 (21:00).

In some instances, sectors hired "specialists" to handle the drafting. Interviewee 12 (1:13, 1:16); Interviewee 7 (16:00). These individuals had prior experience with, and had developed expertise in, data protection law. Some were former CBP employees. Others had broken into the field as advocates for the public interest. Still others were industry lawyers or consultants who had been involved in data protection compliance and training. Interviewee 7 (18:00). Where specialists were involved, the drafting and negotiation process often went more smoothly. Interviewee 2 (25:30).

[146]Interviewee 10 (38:00; 47:00).

[147] Interviewee 1 (30:00).

[148]Compare Interviewee 1 (29:00, 34:00) (banking sector drafted code first and then met with authority), with Interviewee 10 (37:00, 46:00) (representatives of the private investigators sector met first with the Authority in order to define the main topics and to get an early sense of the regulators' views on them.)

[149]For example, the 2000 Personal Data Protection Act states that "[a]n organization or organizations planning to draw up a code of conduct may request the Data Protection Commission to declare that, given the particular features of the sector . . . the rules contained in the said code properly implement this Act or other legal provisions on the processing of personal data." 2000 Personal Data Protection Act, Art. 25(1). The 1989 Law on Personal Data Files was similar. It provided that industry sectors may develop a code of conduct and then may formally request that the Registration Chamber declare that "in the Chamber's judgment the code concerned conforms with the provisions of . . . this Act and meets reasonable requirements for the protection of the privacy of data subjects." Law on Personal Data Files § 15; NUGTER, *supra* note ___, at 175 (providing the unofficial translation just quoted).

submission.[150] During this period, the Authority reviews the draft to assess whether it properly implements the statute.[151] The agency may conduct on-site reviews of data practices and files and "field test" whether the code that the industry has drafted actually addresses the data protection issues that the sector presents.[152] At this point, the Authority also engages the industry representatives in a face-to-face discussions in an attempt to arrive at a mutually agreeable text. These negotiations can be very time-consuming. As described by a former DPA Offiical, the negotiation "always involved at least two to three meetings. That was the standard. But some involved more. The process could involve 10, 20 meetings during three, four years.[153] In one,

---

[150]Personal Data Protection Act, Art. 25(4). According to one former Data Protection Authority official, these procedural requirements and timelines have the unintended effect of encouraging the sector and the Authority negotiate the code informally *before* the sector formally applies for approval. Interviewee 12 interview. This prevents the 13-week clock from beginning to run and so allows the Authority more time to consider the proposed code and negotiate changes to it. The result is that the real substantive work takes place before the sector even applies for approval. Interviewee 12 interview. By the time that it does apply, the Authority and the sector have usually worked through all their differences and reached agreement on the key provisions. This, in turn, reduces interested parties' ability to influence the Authority with their comments since, by the time the comment period occurs, the Authority has already been working on the proposed code for many months and is quite set in its views about it. Interviewee 12 interview. This makes public's opportunity to comment less meaningful than it might otherwise be.

[151]Each statute specifies that the Authority may approve only those codes that correctly embody the provisions of the data protection statute and other relevant laws. For example, the 2000 Personal Data Protection Act states that the Authority should only approve a code where "given the particular features of the sector . . . the rules contained in said code properly implement this Act or other legal provisions on the processing of personal data." Personal Data Protection Act, Art. 25(1). The wording in the 1989 Law is similar. Law on Personal Data Files, § 15 (code must "conform[] with the provisions of, or passed pursuant to, this Act") (unofficial translation); Nugter, *supra* note ___, at 175 (quoting and discussing this provision). The 1989 Law goes on to say that a code must also "meet reasonable requirements for the protection of the privacy of data subjects." Law on Personal Data Files, § 15. This latter phrase apparently refers to obligations that exist independent of the Law itself, but it is not clear whether the source of these additional obligations is the Constitution, other statutes, or some other law.

[152]Interviewee 10 38:00. One former DPA Offiical described the process this way: "Let's see your files. This is the code. When we apply the code to these files, do they cover all the problems. That was an important way. Real testing. And we had discussions at the same moment with private investigators. If we saw problems in the files that the code did not address, then we went back and revised the code." Interviewee 10 39:00.

[153]Interviewee 2 36:00. *See also* Interviewee 12 1:31:30 (former DPA regulator states that her "personal experience is that it takes a lot of time and effort from the branch organizations that are trying to get a code approved, and from the agency too.")

particularly lengthy example, it took the agency and the banking sector a full five years to reach agreement on relevant code.[154]

While the negotiations are lengthy, they can also provide a very useful forum for identifying and working through questions about how properly to interpret the statute. As a former Data Protection Authority official explained it, "the discoveries of these problems, and the solutions developed for them, were quite often a secondary benefit of the negotiations of the code of conduct. It was not generated by complaints; it was not generated by requests for information. It was developed in the context of codes of conduct. What does this mean, in that situation? Oh, we haven't thought about that. Well, come up with texts on it for next time. Through the process of negotiating the code, the Authority learned more about the industry it was regulating."[155] A lead negotiator for the banking industry expressed a similar view, explaining that if industry engages in open discussions with the regulators and tells them that "they are not bound by what they say, then you have good dialogue and the outcome is realistic."[156]

Following the negotiation period, the Authority declares whether the code complies with the statute. In so doing, it must publish notice of its draft decision in the Government Gazette,[157]

---

[154]Interviewee 11 9:00. This may have been due to the way that this sector approached the process. Soon after the enactment of the 1989 law, the banking sector created its own code and presented it to the Registration Chamber as a done deal. "They said, this is our contribution; you only have to approve it. This led to a history because what they proposed, of course, was not in all respects perfect. It took about four or five years and endless meetings so push some of this back. It showed some of the good sides, but also some of the weak sides of self-regulation, the one-sidedness." Interviewee 2 12:00. The process may have gone more quickly had the sector and the agency met first to discuss preliminary ideas before the sector went ahead and put pen to paper.

[155]Interviewee 2 30:30-31:00.

[156]Interviewee 1 1:28:30.

[157]The Personal Data Protection Act states that the Authority should follow the procedures laid down by the General Administrative Regulations Act. Personal Data Protection Act, Art. 25(4). The General Administrative Regulations Act, in turn, requires administrative authorities to publish notice of draft decisions. General

make the draft decision available for public inspection,[158] give interested parties six weeks to comment on the draft decision,[159] and declare no later than six months after having received the initial application whether the code properly embodies the statute.[160] This declaration has the status of a final agency decision under Dutch administrative law, must be published in the Official Gazette (Staatscourant),[161] and is subject to judicial review.[162] Since the passage of the 1989 law, the Dutch have approved at least 18 codes for sectors that include banking, pharmaceuticals, information bureaus, direct marketing, medical research, and others.

Once the Authority has approved a code, it considers companies that follow the code to be in compliance with the statute.[163] Such firms essentially occupy a legal safe harbor similar to the one that the proposed American bills would create for those who follow the rules of a safe harbor program.[164] By contrast, the Authority considers firms that sign up for a code but then fail

---

Administrative Regulations Act, Art. 3:12. Thus, the Personal Data Protection Act, by way of the General Administrative Regulations Act, requires the Authority to publish notice of its draft decision. The other requirements mentioned immediately after this footnote derive from the same source.

[158]Personal Data Protection Act, Art. 25(4); General Administrative Regulations Act, Art. 3:11.

[159]Personal Data Protection Act, Art. 25(4); General Administrative Regulations Act, Art. 3:15, 3:16.

[160]Personal Data Protection Act, Art. 25(4); General Administrative Regulations Act, Art. 3:18.

[161]Personal Data Protection Act, Art. 25(4), (6); Law on Personal Data Files, Art. 15(4); Korff, *The Dutch Data Protection Law*, § 8; Interviewee 12 Interview 30:10.

[162]An interested party (a citizen, a competitor) could potentially bring a legal challenge the DPA's formal approval of a code. Interviewee 12 21:15.

[163]According to one former CBP official, when the CBP does an audit, and there is an industry code of conduct, "you have to take the code of conduct into your frame of reference, into the body of norms that you look to in order to make a legal judgment. You look at the facts, the law and the code of conduct, and then you make your judgment. You cannot ignore it." Interviewee 12 3:09.

[164]Interviewee 2 21:00 (also 23:00?) ("if you follow the guidance of the code, that provides a safe haven, a safe harbor [with respect to the Authority].") Interviewee 4 I 13:00; Interviewee 11 (39:00-43:00).

to follow it to be in violation of the statute.[165] The Authority will subject such firms to written compliance orders and financial penalties.[166] The data user can challenge such an enforcement action in court. Interestingly, while the DPA must accept a code of conduct that it itself has approved to be a valid interpretation of the Data Protection Act, the courts need not do so. They remain free to interpret the Act for themselves.[167]

An approved code of conduct remains in place for five years.[168] After that, the code lapses and the sector must seek the Authority's approval of a new code, or of a new term for the existing one. Parliament believed that this requirement would keep codes up to date with changing legal and commercial realities.

B. Comparing the Dutch and Proposed American Safe Harbor Programs

The Dutch code of conduct program, just described, shares many features with the safe

---

[165]In such an enforcement action the Authority would assert that the firm was violating the statute, not the code. Interviewee 2 (1:02) (If the CBP brings an action it is for violation of the statute, not of the code. It is the Act which applies. An approved code is not replacing anything); Interviewee 4 (the CBP enforces the statute, not the code) (II 10:00). This follows from the fact a code is an approved interpretation of the statute, and that failure to abide by a code accordingly constitutes a violation of an approved interpretation of the statute. Interviewee 1 (1:46) (If the code interprets the act in a particular way, and a bank violates that interpretation, then it is also supposed to be unlawful.) A former DPA official explained that the Authority had, in fact, used the codes in just this way to build the case that a firm was in violation of the statute. (Information bureau that trading in all kinds of personal information. In building the case, we used the codes of conduct and argued that they were not in compliance with these codes. The code works as a yardstick for complaint handling, and for raising awareness, and it could have an effect on the way the Authority enforces the Act.) Interviewee 2 (1:00-1:02). On occasion, the Authority has also ordered firms that had agreed to comply with a code to honor their commitment or face enforcement action under the statute.

[166]Personal Data Protection Act, Art. 65; *accord* Korff, *The Dutch Data Protection Law,* § 7. If the violation is a failure to notify, then the Authority can assess an immediate administrative fine. Personal Data Protection Act, Art. 66(1); Korff, The Dutch Data Protection Law, § 7.

[167]Law on Personal Data Files, Art. 15(6); Nugter, *supra* note ___, at 176; Personal Data Protection Act, Art. 25(1) (giving Authority's decision the status of a "declaration" which is not binding on the courts); Korff, *The Dutch Data Protection Law,* § 8.

[168]Personal Data Protection Act, Art. 25(5); Law on Personal Data Files, Art. 15(5).

harbor programs that the U.S. bills and White Paper propose.[169] Each allows private entities, rather than administrative agencies, to draft the rules that implement the statute; each requires an agency to evaluate these rules and approve them if they are consistent with legal requirements; and each creates a safe harbor for firms that sign up for and follow the code. Moreover, the Dutch code of conduct and the proposed U.S. Safe Harbor programs each require the regulators and the regulated to work together and share responsibility for the drafting of rules. Each thus constitutes a form of collaborative governance.

The programs are not identical, however. The Dutch program differs from its proposed American counterparts in at least five ways. First, the Dutch codes each correspond to a particular industry *sector, e.g.,* the banking sector, the pharmaceuticals sector, etc.[170] By contrast, the American bills do not require safe harbor programs to be sector-specific. They allow any non-governmental organization to propose a safe harbor program. Second, in the Netherlands the industry sector drafts the code and then negotiates it with the agency. Public interest groups and other stakeholders do not weigh in on the document until it is proposed for public comment[171] and, even at that stage, typically do not provide much input.[172] The Obama Administration White Paper, by contrast, calls for wide-ranging, multi-stakeholder groups to draft the codes[173] and the

---

[169]*See supra* notes ___-___ and accompanying text.

[170]Dutch law is quite clear on this point. It provides that the sector must be "sufficiently precisely defined," 2000 Personal Data Protection Act, Art. 25(3); 1989 Law on Personal Data Files § 15, and that the organization representing sector and drafting code must be "sufficiently representative" of that sector, 2000 Personal Data Protection Act, Art. 25(3); 1989 Law on Personal Data Files § 15. The Authority will not consider a code that fails to meet both of these threshold criteria.

[171]Interviewee 2 45:00 (Third party stakeholders were never involved in the negotiation).

[172]Interviewee 2 41:00 (CBP has typically received very few comments); Interviewee 12 (?) 48:45 (same).

[173]White Paper at 23.

Congressional bills, too, appear to allow for such a process.[174] This is a departure from the Dutch model where industry and government negotiate the codes.

Third, Dutch industry and government negotiate their codes against the background of a comprehensive data protection statute which the codes are supposed to interpret. While the bills discussed above do propose comprehensive legislation for the U.S.,[175] Congress has not yet passed such a statute and may not do so for some time. Recognizing this, the Administration White Paper calls for the negotiation of voluntary multi-stakeholder codes even in the absence of comprehensive legislation. This differs from the Dutch approach. Fourth, the Dutch codes of conduct are themselves comprehensive. They implement, and create a safe harbor with respect to, all statutory requirements. The U.S. bills that propose safe harbor programs, on the other hand, extend the safe harbor only to certain statutory requirements and reserve the rest for traditional agency rulemaking. Finally, the Dutch have been negotiating and approving codes since 1989, while the American proposals have yet to be implemented. This twenty-three-year experience with data protection codes of conduct provides an empirical basis on which to assess the merits of the collaborative approach to privacy regulation. We turn now to that assessment.

---

[174]The Congressional bills say that "non-governmental organizations" and "self-regulatory organizations" will draft and sponsor the safe harbor programs. This could allow for a sector-based approach similar to the Dutch model. However, it could equally permit multi-stakeholder safe harbor programs that are not focused on a particular sector.

[175]*See supra* notes ___-___ and accompanying text.

V: What the Dutch Experience Can Tell Us About Collaborative Privacy Regulation

In the spring of 2010, I lived in the Netherlands and interviewed regulators, industry representatives, public advocates and academics who had been directly involved with, or had studied, the Dutch data protection codes of conduct. I organized the interviews around the four central areas on which collaborative governance theorists disagree: the reasons why governments adopt collaborative methods; the merits of the collaborative process itself; the quality of the substantive rules that it produces; and the effects that it has on compliance. This presentation follows this same structure. It also adds a final section with findings on topics not directly related to the first four. At each step, it draws on the Dutch experience to shed light on the merits of collaborative privacy regulation.

A. Why the Dutch Government Utilized, and Dutch Industry Embraced, Data Protection Codes of Conduct

The initial drafts of the legislation that became the Law on Personal Data Files did not utilize industry codes of conduct. Instead, they proposed a prescriptive approach in which the government would issue regulations and would license particular company data operations.[176]

1. *Why the Dutch government utilized codes of conduct*

The Dutch Ministry of Justice (which drafted the legislation) and Parliament ultimately moved towards the code of conduct model. They did so for four principal reasons. The first was administrative efficiency. The Ministry of Justice recognized early on that it would take a great

[176]Interviewee 2 (9:00). For example, see the early Swedish data protection law.

deal of time and resources to develop sector-specific rules[177] and that this would be beyond the means the small agency (the Registration Chamber).[178] It accordingly sought to achieve a "division of labor"[179] in which the government would lay down broad principles and promote compliance but industry associations would draft specific rules for their sectors, subject to regulatory approval.[180] According to one who was present at the time,"we needed to speed up the implementation process. One way was to let the sectors help."[181] Second, the Reagan Administration's emphasis on deregulation during the 1980's had an "echo" in Europe at the time that the Ministry was drafting the 1989 Law on Personal Data Files. This contributed to the move away from a prescriptive model to a code of conduct approach that contemplated a smaller, more cooperative role for government.[182] Third, the Ministry believed that sectors could draft and update codes of conduct more quickly than government officials could draft and update rules.[183] Codes would therefore do a better job of keeping up with the fast-changing information

[177]Interviewee 2 (5:00).

[178]Interviewee 12 (55:00) (while the Authority could also have fleshed out the statute, "it takes a lot of energy to do that. With a small Authority of 70 people, you cannot do that.")

[179]Interviewee 2 (17:30).

[180]Interviewee 2 (:10) (A lot of the economy to cover. CBP is relatively small agency. How to cover so much without too much delay. Draw on industries themselves to draft code. This clearly a more efficient way to work.)

[181]Interviewee 2 (10:30).

[182]Interviewee 2 (7:00); (9:30, 18:00) ("[I]n light of the deregulatory moment it moved towards a self-regulatory model. You will see this if you compare the first proposed Act in the 1970's, and the one that was ultimately passed.)"

[183]Interviewee 14 (1:25) (Government regulation cannot keep up with pace of technological change).

economy.[184] This reason for utilizing codes of conduct corresponds to that which the Obama Administration, and some proponents of collaborative approaches, have articulated.[185]

Finally, a number of interviewees explained that the Dutch history of constructing "polders" – land reclaimed from the sea – generated a culture of cooperation that has contributed to the choice of a consensus-based regulatory method. In the Netherlands, significant amounts of land lie below sea level. Such land is currently habitable because, over the generations, the inhabitants have built a system of dikes and pumps to push the sea back and reclaim the land. Historically, the construction of these "polders" was a massive task that required close cooperation among members of each local community responsible for a given system of dikes. As a result, negotiation and consensus-building became an integral part of Dutch daily life and culture. Scholars believe the cooperative, Dutch approach to regulation owes much to this tradition. They see a similarity between the cooperation and consensus-building needed to maintain the system of dikes, and the attempts by the Dutch government to engage regulated industries and build consensus on regulatory measures. The approach can be found in many parts of the Dutch administrative state and has come to be referred to as the "polder model" of regulation.[186]

---

[184]As one former DPA official explained, "[s]ociety changes constantly, so if you make a rule very concrete and specific then it might describe a certain situation in the year 1980, but five years after that there is something completely different and the rule doesn't apply anymore. For example, e-mail. For example, access. It used to be people went directly to company to ask for access to information about them. Now they can ask by e-mail. If you put that in law and made it specific but did not mention e-mail, you would make this less possible." Interviewee 12 (42:00, 44:00-46:00).

[185]*See supra* notes ___-___ and accompanying text.

[186]The government has for many years met with representatives of management and labor to negotiate and reach consensus on the issues that divide these groups. It has negotiated environmental "covenants" with industry sectors that set out how firms in that industry will go about reducing greenhouse gases or meeting other

These cultural factors appears to be at work in the Dutch approach to data protection regulation. Many interviewees referenced the polder approach in explaining why they felt that data protection codes of conduct worked well in the Netherlands. For example, a leading regulator stated that "In Holland we accept the concept of codes very well. Under our Polder model we try to get agreement with all organizations involved, a consensus oriented approach, that is a very high standard in Holland. In Holland it is a normal way of thinking to try to reach agreement. It's in our culture."[187] A representative of the banking sector echoed this sentiment, explaining that "Holland is a small country that works with consensus. That is what we call the 'polder model.' The same goes for this type of problem. We always try to find solutions which are acceptable for everyone. That is the way we work."[188] This link between codes of conduct and Dutch history and culture raises questions about whether the model is transferable to the United States. A later section of this article will return to this question.[189]

2. *Industry's reasons for participating*

The safe harbor approach relies on voluntary industry participation. Thus it is equally important to know why industry sectors decided to invest time and resources in drafting a code.[190]

---

environmental goals.

[187]Interviewee 10 (3:30). Confirming the point, a lead drafter of the 1989 Law explained that while some countries used more prescriptive regulation, "[i]n the Netherlands it went different. That is in part because it made sense in terms of division of labor. But it is also part of the culture which is very much a culture of seeking consensus. Working it out together is a characteristic of Dutch culture." Interviewee 2 (19:30).

[188] Interviewee 11 (16:15).

[189]*See infra* notes ___-___ and accompanying text.

[190]The Department of Commerce recognized the importance of this question. In its 2010 Green Paper, in which it proposed that the U.S. utilize codes of conduct for privacy regulation, the Department of Commerce asked for suggestions as to how it could convince industry sectors to draft and commit themselves to such a code. Green Paper, *supra* note ___, at 51.

Dutch industry's primary reason was to clarify the broad terms of the Data Protection Act. As was explained above, the Data Protection Act speaks in broad, ambiguous terms.[191] Yet it does not authorize the DPA to promulgate regulations fleshing out these provisions and, in any event, the Authority does not have the staff or resources to do so.[192] Companies accordingly found themselves facing a new, broadly-worded set of legal obligations without sufficient instructions on how to comply. One industry lawyer compared the situation to "feeling our way in the dark."[193] This was an untenable situation for larger, more visible sectors that utilized a great deal of personal information. These sectors put resources into codes so as to gain clearer guidance on what the statutes required of them.[194] In its 2010 Green Paper, the Obama Administration sought comment both on how it could encourage the private sector to draft enforceable codes of conduct, and on the need for privacy legislation. The Dutch experience suggests that these two questions are linked. Broadly-worded privacy legislation gives the private sector an incentive to invest in producing codes of conduct as a way to interpret the statute and achieve more regulatory

---

[191] *See supra* notes ___-___ and accompanying text.

[192] The Authority did, over time, generate a number of guidance documents. For example, it produced "reports" on specific sectors that analyzed the main data protection issues raised by that industry's practices and gave some indication of the Authority's views on those topics.

[193] Interviewee 12 (1:18).

[194] As a lawyer for the banking industry explained it, "legislation is very general and it is often not clear how to apply it to specific issues. So the code serves as an interpretation of the Data Protection Act in its application in specific banking situations." Interviewee 1 (4:30). This attorney, who played a leading role in the drafting and negotiation of the banking code, provided a number of examples of how the code clarified the legislation. "The Act says that there has to be a purpose for the possession of personal data, and the code says what the purpose exactly is. We sought clarification on voice logging and on the processing of video pictures. The Act says nothing on this. The code says what we do in these areas. We wanted clarity about how use security cameras, and how inform the public that we were using them. The code helps to clarify this. The Act says nothing about direct marketing. The code makes explicit what type of customer marketing is permitted in groups of banks, and for what purposes. The Act says that can process data to be in compliance with other legislation. The code says what that legislation is. Interviewee 1 (5:00-6:30, 9:00).

certainty.

B. The Process of Producing Codes of Conduct

As was described above, the proponents and critics of collaborative governance disagree on whether it constitutes an effective process for producing rules.[195] The Dutch experience provides some support for each viewpoint.

1. *Information sharing*

The Dutch codes did appear to build trust between the regulators and the sectors and so to facilitate the sharing of business information. For example, a DPA official recounted that, in the course of negotiating the private investigator sector code, industry members allowed the agency to enter their offices and review their files in order to "field test" the draft code against actual client records. They did this even though they knew that this inspection would likely reveal some violations of the Act. He explained that the code negotiation process created the trust that made this possible. "We were not there in our role as regulator. Our aim was not to inspect. It was to see whether the code will work for reality. Why did they allow us? We trusted each other. It came down to personal trust. The process of negotiating the code helped to build that trust. . . Our approach was we want to reach a common solution to allow them to do their work on a legal basis. When you show that you are really interested in the way that they operate, then they trust you."[196] Business representatives explained that, for their part, they shared information so as to

[195] *See supra* notes ___-___ and accompanying text (setting out this argument and citing sources).

[196] Interviewee 10 (40:–43:00)

correct regulators' misconceptions about their industry's data practices.[197]

While these interviews painted an optimistic picture, others suggested that government should not rely exclusively on code negotiations to learn about industry data practices. One former regulatory official recounted how a DPA investigation of the trade information bureau sector (roughly equivalent to our credit rating agencies) unearthed valuable information that the code negotiation had not revealed. As the official explained: "You learn most by doing an investigation of a complaint, not by negotiating a code. You are on the spot in a company. You can interview people on work floor and can read internal memos. You can see the computer programs they use. You can even review the buying and selling of information. Then you see how do they make their money. Do they buy information? From whom? That gives you an idea of the network. By negotiating a code of conduct you do not get that information."[198] This suggests that while code negotiations may provide valuable information, regulators should carry out independent investigations as well.

The Dutch experience also showed that information sharing does not just go in one

---

[197]For example, the direct marketing industry believed that data protection authorities thought they were misbehaving in ways that they actually were not. "They think we do all kinds of things we do not do." Interviewee 8 (2:07:30). The sector wanted to develop a code, in part, because it presented an opportunity to engage the regulators and communicate more accurate information about what the industry did and did not do in practice. Interviewee 8 (2:12). As the industry's lead representative put it: "We are working 24 hours a day, 7 days a week in this field. We know everything about cookies. We know everything about flash cookies. We know everything about the techniques used. The [regulators] have to discuss on all kind of different topics in order to understand it. These kind of discussions are very good to tell them and inform them what you are doing. Interviewee 8 (54:00-55:00). Along these same lines, a lead negotiator for the banking industry stated that one of the main reasons the sector decided to develop a code was to provide "information for the Supervisor." Interviewee 11 (39:00).

[198]Interviewee 12 (23:00). The regulators found it particularly useful to be able to review company transactiosn related to personal data. This revealed that professionals such as lawyers and bailiffs, who had special rights to obtain personal information in their official capacities, were unlawfully sharing it with trade information bureaus in exchange for access to other information that these professionals found useful in their work as debt collectors. Interviewee 12 1:18-1:35. The bureaus were like "spiders at the center of a web" of information transactions, and the investigation allowed the regulators to see the Web.Interviewee 12 1:30 (?).

direction. Government officials, too, can share valuable information. During the course of negotiating a code regulators often explain how they view and interpret the law. This can help industry to understand where the lines are drawn and so to act with greater certainty. For example, banks typically shared with each other information on customers who had behaved fraudulently. During the negotiations over the banking industry's code of conduct regulators clarified that this would not violate the Data Protection Act's limitations on sharing personal information with third parties so long as the security personnel at each bank were the only ones given access to the data.[199] The parties memorialized this interpretation in the Financial Institutions Code.[200] One of the negotiators of the banking code explained the value of such clarifications. "Codes give certainty. . . . Every Supervisor has their own policy between the lines. So you have to know very well what the policy is. One of the ways to know that is to get into a discussion with them. A code like this is a very useful instrument for it. I think it is very important, especially because data protection is very general."[201] The lead negotiator for the private investigator industry provided several other examples of how code negotiation served as a vehicle for clarifying the statute.[202] He, too, identified that as "the added value of the code. . . . The industry is able to clarify what is in bounds and what is out of bounds in a way that is useful

[199]Interviewee 11 (48:00-53:00).

[200]Code of Conduct for the Processing of Personal Data by Financial Institutions § 5.2.2; Notes to the Code of Conduct for the Processing of Personal Data by Financial Institutions § 2.5; Interviewee 11 (52:20).

[201]Interviewee 11 (53:00, 55:00).

[202]It clarified the conditions under which private investigators could observe individuals through the windows of their home and could attach a GPS device to a subject's automobile. Interviewee 7 (2:07-2:16).

to the industry and that the agency approves."[203]

In addition to clarifying the statute, regulators also use the code negotiation process to flag potential legal issues that the industry drafters may have missed. For example, a former DPA official explained that, in the course of negotiating the medical research code, the Authority was able to identify a host of issues that the industry had not yet considered: "What is identifiable. What is anonymous? What is pseudo-anonymity? . . . It is not so easy. The discoveries of these problems, and the solutions developed for them, were quite often a secondary benefit of the negotiations of the code of conduct. It was not generated by complaints; it was not generated by requests for information. It was developed in the context of codes of conduct. What does this mean, in that situation? Oh, we haven't thought about that. Well, come up with texts on it for next time."[204] In this way the code negotiation process could serve as a vehicle for educating the industry on the statute and the legal issues that it raises.

2. *Joint problem solving*

The proponents of collaborative governance also predict that it will produce a problem-solving, rather than an adversarial, mentality. The interviews offered a few instances of this. For example, banks wanted to take their customers' personal and financial data, collected during the course of providing banking services, and use it to construct profiles of those who may be interested in certain banking products. Yet the Data Protection Act did not allow personal data to be processed for purposes that were "incompatible" with the one for which they were originally

[203] Interviewee 7 (2:13-2:14).

[204] Interviewee 2 (29:30- 30:30).

obtained.[205] Would taking data collected for the purpose of providing banking services, and using it to construct marketing profiles, be "incompatible" and hence contrary to the Act? The banks and the DPA debated this while negotiating the Financial Institutions Code.

According to a representative for the banks, the turning point came when each party expressed its bottom line need. For the regulators, the most important thing was that the banks not use data on individual customers to create profiles of *those individuals*.[206] That was not a problem for the banks. They wanted aggregate customer data that would help them to identify the type of customers who might be interested in certain products. They readily agreed to create only aggregate profiles, not individual ones.

Once the parties realized that their core interests could be reconciled, they were able to identify an interpretation of the Act that was consistent with this solution, and to build it into the Code. The Financial Institutions Code states that analysis of aggregate customer data is "processing for statistical purposes."[207] It then provides that processing for statistical purposes is not incompatible with the purposes for which the data were initially collected, so long as the bank makes "the necessary provisions to ensure that the further processing of personal data shall be effected for these specific purposes only."[208] The pharmaceutical sector and the DPA reached a very similar solution regarding that industry's desire to use the personal data of those

---

[205]Personal Data Protection Act, Art. 9.

[206]Interviewee 1 (1:32).

[207]Financial Institutions Code, § 5.3.2.

[208]Financial Institutions Code, § 5.3.1. To make matters perfectly clear, Section 5.3.3. says that "In order to target marketing activities at certain groups, personal data may be analysed that have been collected within the framework of marketing activities."

participating in clinical trials to construct profiles of the types of people who might best be able to benefit from new drugs.[209]

Articulation of bottom line interests in a way that allows these interests to be reconciled, is classic problem solving. The representative of the direct marketing sector, having himself negotiated such a solution with the DPA,[210] summed up the dynamic in this way: "I approached the representative of the CBP and I said, 'let's sit together. If you have specific needs, let's talk about those needs. And then we can give, on behalf of industry, what our needs are.' And so we aligned our work in such a way that we both were content. And we submitted it for approval, and it was approved."[211]

3. *Agency capture and industry influence*

The interviews did not provide any clear examples of full-scale agency capture. The DPA appeared to have well-defined institutional values that were independent of and different from industry interests.[212] Moreover, both government officials and industry representatives told of

---

[209]Interviewee 9 (36:00-38:30).

[210]According to the representative for the direct marketing industry, the initial disagreement concerned whether the industry should be prohibited from having any commercial communications with children at all, or whether it should be allowed to do so with parental consent. Interviewee 8 (1:31). After discussion, it emerged that the DPA's real concern was that the industry would condition online prizes on children's disclosure of personal data. The industry agreed not to do this, and this became part of the code. Interviewee 8 (1:32); FEDMA code § 2.6.4. "Once we learned what their real opinion was, we were able to address it." Interviewee 8 (101:40) (?).

[211]Interviewee 7 (24:00).

[212]For example, a former DPA official explained that the Authority's "reputation was at stake" in the codes that it negotiated. Interviewee 2 (32:00). "[T]he agency could not afford to approve and recommend a code, and then receive the next month a complaint. Have you overlooked this? How come? So the agency's reputation also was involved." Interviewee 2 (33:00). This sense of an agency reputation, and the need to protect and build it, suggests an independent set of values. Interviewee 2 43:00 ("[t]his is an independent government agency whose task it is to insist on adequate safeguards").

contested, protracted negotiations,[213] and industry representatives complained about regulators being too "technical" and "legalistic."[214] This does not indicate agency capture. The literature on agency capture suggests that it is more likely to occur when an agency regulates a single industry than when it regulates many different ones.[215] The Data Protection Act covers many different industries. Thus, the literature is consistent with the idea that agency capture had not occurred.

While the Dutch experience did not suggest agency capture, it did reveal one instance in which an industry sector seemed to exercise a disproportionate and unhealthy influence over the shape of its code. This involved the statutory obligation to notify a data subject that one is collecting data on her, and the private investigator industry's compliance with this requirement.[216] Private investigators complained that this requirement was especially burdensome when an employer hired them to investigate an employee who turned out to be innocent. In these instances the employer often insisted that the employee not be told of the investigation for fear of damaging the employment relationship. Despite concerns about data subject rights,[217] the DPA agreed to make it the employer/client's obligation, rather than private investigator's, to inform

---

[213]Interviewee 2 (11:00-12:00) (describing the difficult five-year process for negotiating the Financial Institutions Code); Interviewee 10 (55:00-56:30) (describing the "heavy discussions" between the DPA and the direct marketing industry over that sector's code).

[214]Interviewee 5 (1:02) (government officials do not understand the industry, take a "formal approach based on laws," and are not open to industry input).

[215]Scruggs at 147 (corporatist tradition that brings in extensive sets of interest groups leads to reduced risk of agency capture).

[216]2000 Personal Data Protection Act, *supra* note ___, §§ 33, 34.

[217]A DPA official involved in the negotiations made clear that the agency knew this was a weak solution. "We were always aware in advance that protection of rights of data subject was an illusion in terms of informing them of the investigation. But we did not push it. They were proposing texts. We said Ok. I always knew that it was a very weak point." Interviewee 10 (24:00).

the employee of the investigation so long as the employer provided the investigator with proof that it had done so. This problematic solution puts the burden of notifying the innocent employee in the hands of the one party that does not want that notification to occur – the employer. While it requires the employer to document the required notification, it does not require anyone to check the accuracy of this documentation. Supporting these concerns, a later study of the private investigator industry found widespread non-compliance with the notification requirement[218] and explained that most violations occurred "in cases where no evidence could be found" of the employee's malfeasance because, in those cases, the employer did not want to damage its relationship with the employee.[219]

The private investigator story is a troubling one. Yet the fact that industry got its way in this instance does not mean that it did so in every case. To the contrary, the DPA did stand its ground during difficult negotiations with the credit rating industry or, as they are known in the Netherlands, the trade information bureau sector (handelsinformatiebureaus). In the Netherlands trade information bureaus, such as Experian, use their large stores of personal information not only to generate credit ratings but also to provide information for other purposes such as debt collection. To carry out these functions industry members frequently ask third parties, e.g. a landlord, about a given individual's whereabouts, financial situation, etc. The DPA took the position that the industry had to obtain the individual's consent before doing so–a position that

[218]Regioplan Policy Research, *Evaluation of the Privacy Code of Conduct for Private Detective Agencies* (Oct. 2007) [copy on file with author].

[219]*Id.* at 88.

the industry believed would undermine its debt collection-related service.[220] In the face of strenuous industry argument, the DPA remained committed to its position. Negotiations over the renewal of the trade information bureau code broke down over this issue, and the code lapsed.[221] The trade information bureau and private investigator examples present different pictures of industry influence. For now, the most that can be said is that industry appears able to exercise undue influence in some, but not all, instances. The code negotiation process should be designed to minimize this possibility by, for example, including public interest stakeholders in the discussion.[222]

4. *Adaptability*

Both the proponents of collaborative governance and the Obama Administration claim that this method is more nimble and adaptive than traditional, notice-and-comment rulemaking[223] and that this quality is particularly important for regulation of the information economy. As was explained above, Dutch policymakers also articulated this idea when explaining why they opted for codes of conduct over traditional rules.[224]

The Dutch codes of conduct tell a very different story.[225] Government and industry

---

[220]Interviewee 5 (52:00-54:00). Explain that trade information bureaus occurred during Kohnstamm era. Interviewee 2 treated differently. Interviewee 5 58:30.

[221]Interviewee 5 (51:00, 55:00).

[222]*See infra* notes ___-___ and accompanying text (suggesting this).

[223]*See supra* notes ___-___ and accompanying text.

[224]*See supra* notes ___-___ and accompanying text.

[225]Some interviewees did describe codes as an adaptive form or regulation. Interviewee 8 (1:14); Interviewee 12 (1:19); Interviewee 9 (17:00). However, these statements were at odds with the facts that they and others described regarding the amount it time it took to negotiate codes, and the static nature of these documents once adopted., as described below.

representatives reported that while some negotiations could proceed smoothly and be wrapped up after two or three meetings[226] they were just as likely to require ten or even twenty meetings and from three to five years of work.[227]A former regulator explained that his "personal experience is that it takes a lot of time and effort from the branch organizations that are trying to get a code approved, and from the agency too."[228] A Ministry of Justice-funded evaluation of Data Protection Act cited observers' findings that "drafting codes of conduct is a long-term, time-consuming and expensive process."[229]

The Dutch experience is also at odds with the proponents' and Obama Administration's claim that stakeholder groups can quickly revise codes of conduct in response to changing realities. The Dutch sectors seldom revised a code during its five-year term. To the contrary, several codes lapsed after their initial five years had ended and, in some cases, it took years for

---

[226]According to one former regulator, the codes that took the least time to negotiate where those in which the industry's information practices were already heavily regulated since this gave the parties a legal foundation from which to work, Interviewee 2 (28:30), and the codes in which the industry hired an information privacy "specialist" to represent it during the code negotiation process. Interviewee 2 (25:30).

[227]Interviewee 2 36:00. The Financial Institutions Code was one of these. It took five years to reach agreement. Interviewee 11 (9:00); Interviewee 2 (11:00-12:00). One of the reasons that it may have taken so long as that the industry developed the code largely on its own and then presented it to the DPA as a finished product. "This led to a history because what they proposed, of course, was not in all respects perfect. It took about four or five years and endless meetings so push some of this back. It showed some of the good sides, but also some of the weak sides of [codes as a regulatory instrument]." Interviewee 2 (11:00-12:00). The process may have gone more quickly had the sector and the agency met first to discuss preliminary ideas before the sector went ahead and put pen to paper.

These time frames conflict with the Dutch Personal Data Protection Act which requires the DPA to reach a decision within 13 weeks of industry's submission of the draft code. Personal Data Protection Act, Art. 25(4). This disparity is explained by the fact that most of the negotiations occur before the sector formally submits the draft code to the DPA. Interviewee 12 34:45; 1:09. The time frames discussed here reflect the actual length of time that the sector and regulators worked on the code; not the formal 13-week period that the statute describes.

[228]Interviewee 12 1:31:30; *see also* Interviewee 2 (24:00) (describing "extensive meetings, sometimes negotiations, sometimes about texts, article by article. Some were very frustrating for both sides.")

[229]Ministry of Justice, First Evaluation of the Personal Data Protection Act, Summary at 3 (2007).

the industry and government to agree on a new version.[230] During this period, the lapsed code lost its legal status and the industry its safe harbor.[231] These are hardly the signs of a nimble and adaptive process. Instead, the Dutch experience suggests that both the industry and regulators must invest a great deal of time and resources in the drafting and negotiation of a code and that, once they have done so, they are loathe to re-open the discussion until they are absolutely forced to do so. That explains why many industries did not revise their codes until they had reached the end of their five-year term and, even then, allowed them to lapse before re-engaging with the DPA. The Dutch codes are relatively static regulatory instruments. While they may be no worse than notice-and-comment rulemaking in this regard, they do not appear to be much better.

This calls into question the Obama Administration's reliance on the adaptability of multi-stakeholder codes of conduct as one of its chief rationales for utilizing this regulatory method. Indeed, the Administration's intended multi-stakeholder processes, which require multiple parties to reach agreement on the codes, should prove even more difficult and time-consuming to negotiate than the Dutch codes which require only industry and government to come to terms. This should make the parties even more wedded to the codes that emerge from the process and less eager to re-open settled negotiations in order to revise them. If Congress and the Administration are to utilize codes of conduct they will need to develop ways to make them more adaptable than the Dutch codes have proven to be, not less.

---

[230]Interviewee 12 3:00-4:00; Interviewee 11 58:00 (describing how Financial Institutions Code lapsed for two years while negotiations over the revised code dragged on and concluding that '[i]t takes a long time to consider texts.")

[231]Interviewee 12 (5:45, 22:50, 28:45).

C. The Substance of the Codes of Conduct

As was discussed above, the proponents and critics disagree, not only about the value of collaborative processes, but also about the merits of the substantive rules that these processes are likely to produce.[232] The proponents argue that collaborative methods will tend to produce rules that are more tailored to business realities, cost-effective, workable, creative and up-to-date than those that notice-and-comment rulemaking generally yields.[233] The critics, on the other hand, maintain that collaborative processes will generate rules that are lenient and anti-competitive.[234] When we look at the substantive content of the Dutch codes, what do we see?

1. *Tailoring and workability*

The Dutch codes offer quite a few instances in which the negotiation process led to more tailored and workable rules. For example, the private investigator industry code of conduct recognizes that it would be impractical for members of this sector to comply with the Data Protection Act requirement that they notify data subjects *before* collecting data on them.[235] After all, the private investigator business is premised on collecting information about individuals without their knowing. The code accordingly allows investigators to notify the data subject *after*

[232] *See supra* notes ___-___ and accompanying text.

[233] *See supra* notes ___-___ and accompanying text. They also argue that such rules will better reflect the current privacy preferences of affected individuals. However, this attribute is assumes that the relevant collaborative process includes participants who represent these individuals. As explained above, the Dutch codes of conduct do not. Government and industry negotiate them without meaningful stakeholder input in most cases.

[234] *See supra* notes ___-___ and accompanying text.

[235] 2000 Data Protection Act, *supra* note ___, §§ 33, 34.

the investigation, rather than before. Assuming that investigators do provide such notice,[236] this should enable the notifications to serve their intended purpose–i.e., to allow data subjects to exercise their rights of access and correction–without unduly harming the private investigator business. This is a good example of tailoring.

Another example comes from the Financial Services Industry Code. While drafting its code the banking industry identified a conflict between its payment system procedures and the Act's requirement that parties could not transmit financial data without the data subject's prior consent.[237] Traditionally, if a customer made an error such that its payment went to someone other than the intended person, the bank would provide the customer with the name of the recipient so that the customer could undertake the steps required to get its money back. The DPA initially took the position that this information–i.e. receipt of the payment–was financial information and that the bank could only provide it to the customer if the mistaken payee consented. The banks protested that this was unworkable since few such payees would give their consent. After some negotiations, the parties worked out a solution. The Code states that banks can share personal data for the "normal settlement of payment transactions" and for "verification and reconstruction purposes."[238] This small clarification allowed the banks to interpret the law in a way that would fit with important business realities. A representative of the banking industry described the tailoring function in this way: "Negotiation of codes provides an opportunity to

---

[236]Above, I described some situations in which the investigators have not provided such notice at the conclusion of the investigation. *See infra* notes ___-___ and accompanying text. This is a separate, albeit highly important, issue.

[237]Interviewee 11 (31:30)

[238]Financial Institutions Code § 5.2.3.

educate the data protection authority about the specific features of the industry and how they relate to the data protection law. Regulators would not otherwise know enough about the industry to regulate it intelligently."[239]

2. *Cost-effectiveness*

The code negotiation process can also lead to more cost-effective rules. The Financial Institutions Code provides one such example. The Data Protection Act required that a company notify the DPA each time it began to process personal data.[240] Initially, the DPA took the position that each bank had to provide such notice for each bank product that involved the processing of personal data, and for each change in such bank product.[241] The financial industry believed that this would "cause an enormous burden of red tape."[242] It accordingly sought permission to consolidate and streamline the notification requirement in two ways. First, it sought the ability to develop a single, unified description of all of its activities that involve the processing of personal data and to notify the government of them in a single communication.[243] Second, large cooperative banks requested that they be able to make a single notification on behalf of their

[239] Interviewee 11 (:40, 2:25). A representative for the direct marketing industry expressed a similar sentiment, in slight more evocative language: "You know the Streets of San Francisco? There was a guy who always ended the briefing: 'let's do it to them before they do it to us.' So I say, let's do it to ourselves through a code, before they do it to us. This is better because then you get to more workable solutions." Interviewee 8 (1:04).

[240] DPA Article 28; Interviewee 1 (35:00).

[241] Interviewee 1 37:30.

[242] Interviewee 1 (35:20).

[243] Interviewee 1 (35:50).

hundreds of member banks, rather than requiring each member bank itself notify the DPA.[244] The banking representatives argued that these reforms would not only reduce compliance costs; they would also give regulators a more comprehensive picture the banks' information processing than multiple, piece-meal notifications would, and so would improve regulators' understanding of how a given bank handled personal data. Ultimately, the DPA accepted this interpretation of the statute and approved the code with language that allows for the unified notifications. This reduced the banks' compliance costs considerably. The pharmaceutical industry code offers another instance in which a code allowed for more cost-effective compliance.[245]

3. *Leniency*

The critics predict that industry domination of the negotiation process will result in overly lenient rules. As was already described, I did encounter one instance in which the private investigator industry pushed for, and achieved, a lenient interpretation of the Act.[246] That said, it would be unwise to draw sweeping conclusions from this one example. As was also described

---

[244]Interviewee 1 37:00. For example, Rabobank, a large co-opperative bank in the Netherlands, had one central bank and over 1000 member banks. The central office requested permission to file a single notification on behalf of all of these member banks.

[245]European law requires pharmaceutical companies to notify individuals taking their drugs of any adverse effects. Traditionally, this had meant that the independent health professionals who run clinical trials of new drugs had to share with the pharmaceutical companies that sponsor these trials personal information about the individual participants. Interviewee 9 (3:30). Originally, the DPA took the position that, under the Act, DPA approval was required for each such transfer of information, and that the pharmaceutical companies would have to obtain such approval each time they wanted to initiate a clinical trial.Interviewee 9 (7:15, 8:30). Industry believed that this approval requirement would delay its clinical trials and put the Dutch pharmaceutical industry at a serious disadvantage in an globally competitive market where "speed to market" is essential to success. Interviewee 9 (9:45, 12:15, 19:00). According to one business representative, "[i]f the approval process takes too long, then the head office might move the trial to another country." *Id.* at 14:00. The industry and the DPA used the code to resolve the issue. Interviewee 9 (4:30, 10:30). It provides that the DPA will "pre-approve" data transfer related to clinical trials where the sponsor follows specified procedures designed to minimize the amount of data transferred and protect participant privacy. Interviewee 9 (10:30).

[246]*See supra* notes ___-___ and accompanying text.

above, the DPA did not yield to the requests from an even stronger sector–the trade information bureaus–where it felt them to be insufficiently protective of individual privacy.[247] The strongest conclusion for which there is evidentiary support is that the code negotiation process can, at times, lead to overly lenient rules.

One additional comment bears mention here. A former DPA Offiical, who personally negotiated several of the codes of conduct, said the following about the agency's position in such negotiations: "Now we are more or less dependent on what the opposite party is proposing. That is the polder model. Don't take the initiative, let's start with the organizations themselves, what they think will be the best for the company. One of the weakest points is that we cannot stipulate we want it that way. . . . the initiative is to the other party. We do have to approve the code. At the end of the day, they can do nothing without that approval. But it is always a weak point for the regulator that he cannot take the initiative. . . . it is up to the company to start and to bring it further and to develop new texts. This leads to problems in the final product. You have to discuss to the bitter end."[248] This comment suggests that, where industry gets to draft the code, it is able to frame the terms of the discussion. Regulators have to react to industry's language. Such a structure could yield weaker rules than those that a regulator would have drafted. One way to assess this effect would be to compare Dutch codes with rules that regulatory agencies in other European nations have drafted using a more traditional rulemaking approach. Future research along these lines would be useful.

---

[247] *See infra* notes___-___ and accompanying text (describing this report).

[248] Interviewee 10 14:30, 16:30.

4. *Anti-competitiveness*

The interviews revealed one potential instance in which an industry may have employed the code to keep out new entrants. A DPA official explained that, as drafted, the pharmaceutical code went beyond the Data Protection Act protections for consumer data.[249] The Authority initially found this to be perplexing but did not object. Later, a party commenting on the draft code complained that foreign companies would find it harder than domestic ones to comply with the provisions in question, and that the provisions accordingly created a barrier to trade. In retrospect, the official believed that the extra-stringent provisions may have reflected a conscious industry attempt to prevent foreign companies from entering the Dutch market. At the time, however, however, the DPA did not require the industry to change the code. Thus the interviews provided limited, anecdotal evidence for the claim that industry associations can use codes of conduct to keep out new entrants.

D. Compliance and the Code of Conduct Approach

The proponents and critics of collaborative governance also disagree on its impact on compliance. As was explained in more detail above,[250] the proponents argue that traditional enforcement does not do a good job of ensuring compliance, and that collaborative methods will improve it by increasing both industry ownership and acceptance of regulations, and industry self-policing. The critics counter that collaborative approaches will encourage regulators to adopt a cooperative rather than an enforcement-oriented mind-set, and that most sectors will not have the will to enforce rules against their own members.

---

[249]Interviewee 4 (1:45).

[250]*See supra* notes ___-___ and accompanying text.

1. *Traditional enforcement*

The proponents of collaborative governance assert that, due to the limited number of inspectors, direct agency enforcement will often fail to produce adequate compliance. There is anecdotal evidence that this has been the case with respect to the DPA and the Data Protection Act. The DPA itself acknowledged several years ago that its previous enforcement efforts had been lacking. It promised a "change of direction" that would put greater priority on inspections and enforcement.[251]

It remains to be seen whether the DPA's new effort will make a difference. One former DPA Offiical predicted that it would not, for reasons that echo the proponents' concerns about the efficacy of government enforcement. He maintained that the DPA, which has fewer than 100 employees to handle policy development, compliance assistance, investigations and enforcement for the entire Dutch economy, would simply not have the resources to carry out comprehensive monitoring and inspection. "For real enforcement they are still too small. You have to monitor the whole society, to inspect, and that is impossible. So what they are doing is more enforcement actions, but it is relatively small actions. In most cases it is reacting to complaints; it is reactive."[252] This suggests that the Authority may lack the resources comprehensively to monitor data practices across the economy and that traditional agency enforcement may not be enough to ensure compliance with the Act.

3. Building awareness

Can the codes of conduct help to promote compliance? Business representatives and

[251]Data Protection Authority, Forward to 2007 Annual Report (2007).

[252]Interviewee 10 (31:00).

regulators reported an interesting development in this regard. They explained that the very process of developing a code of conduct forced companies to learn much more about their own data practices so that they could determine how the Personal Data Protection Act applied to them. In this way, the code development process raised industry awareness about how it collected, used and shared personal data. One of the lead drafters of the banking code explained how this happened in his sector: "In order to develop, and ultimately comply with, the Financial Institutions code, we had to find out what data our banks were using, how they were using it, and who was using it. . . . . we had to reconstruct the whole process of using personal information in the bank. . . . We had previously focused on the product relationship with the customer, not the back office processes. We had to make the back office processes visible."[253] As a result, "everybody, the back offices, front offices, the lawyers, they all learned a lot about their processes in relation to the data protection issue.[254] A DPA Offiical confirmed that the code drafting and negotiation process builds industry awareness of its data practices.[255] She also pointed out that publication of a code increases *public* awareness of an industry's data practices and so builds public expectations about how companies will handle personal information.[256] This, too, can promote compliance.

---

[253]Interviewee 1 (33:30).

[254]Interviewee 1 (38:00). The DPA Offiical in charge of negotiating the private investigator code suggested that a similar evolution had occurred there. Interviewee 10 32:00. He explained the industry had always assumed that its practices could not be reconciled with data protection, and so had spent little time thinking about the issue. "So, we gave explanations. It is allowed to do your work under certain conditions. Took them out of the dark. It gave them the opportunity to make clear what their practices were and under which conditions they could do what they wanted to do. The process of developing the code raised awareness. Interviewee 10 (33:00).

[255]Interviewee 4 (20:00) (stating that the need to draft a code forces companies and their industry associations to discuss the issue, and this helps to raise corporate awareness.)

[256]Interviewee 4 (20:30).

2. *Ownership and acceptance*

Companies' role in drafting codes of conduct appeared, not only to build awareness, but also to increase their acceptance of the rules that they had had a hand in writing. One industry representative reported that "[i]t's more acceptable to companies because they feel that they are involved.. If they like it, if they don't like it. They can come forward with their problems. . . . If it is imposed by government then they have to accept it but they will not comply because they were not involved."[257] A former regulator also observed this: "Out of experience, I know that if the regulator makes a code of conduct and drops it in that industry, they don't accept it. If you tell people this is how you should live then they say, well, *I* decide how I should live. . . . If they have a role in drafting a code, then they accept it. Their attitude is different. The members say, this is our document, we created it, and the authority approved it . . . [T]hey feel the code is part of them."[258]

Industry actions appeared to be consistent with these reports. For example, Philips Corporation, a multi-national electronics concern with Dutch origins and a headquarters in Amsterdam, formally adopted its industry code of conduct as company policy.[259] In addition, trade associations routinely held sessions for their members at which they presented the code that they had drafted, explained what firms needed to do to comply with it, and encouraged them to

---

[257]Interviewee 8 (1:07:15). A private investigator involved in the drafting of that industry's code of expressed a similar sentiment: "[c]ompanies are more likely to accept it if they have a role in shaping the Code. As long as we feel that we have been made part of it and we are listened to and our interests are taken at heart and something is construed with our interests in mind, then it is much more easy to accept and abide than it being forced upon us." Interviewee 3 (1:23).

[258]Interviewee 12 (55:00-58:30).

[259]Interviewee 14 (5:00) (or is it :05?).

do so.[260] These actions suggest a level of ownership over and acceptance of rules.

4. *Self-policing: bringing up the bottom*

Industry efforts at self-policing appeared to grow, not out of a sense of mutual accountability among the negotiating parties,[261] but out of a desire to rein in smaller, less responsible firms–the "cowboys," as several industry representatives called them.[262] Those industries that were particularly sensitive to their reputations—direct marketing, private investigators, trade information bureaus, banks–seemed to make the most efforts in this direction. In these sectors, the misdeeds of a small number of bad actors can damage the reputation of the industry as a whole. This can both drive away customers and create pressure for direct, government regulation. The more responsible firms in such industries therefore had an incentive to rein in irresponsible ones–to bring up the bottom–lest the actions of these bad actors impose costs on the industry as a whole.

The sectors employed codes of conduct to achieve this. They drafted codes that embodied a relatively high standard of data protection–one that more established firms were likely to meet but that less responsible ones might not. They then required, as a condition of association

---

[260]Interviewee 1 (1:50, 40:30) (banking industry); Interviewee 11 (2:23) (same); Interviewee 9 (1:20) (pharmaceutical industry); Interviewee 5 35:00 (trade information bureaus); Interviewee 7 (private investigators); *see also* Interviewee 12 (58:00) (former DPA regulator affirms this). As a representative for the banking industry explained it, "The code was a vehicle to educate the employees. When we completed the code we gave it a lot of publicity and we discussed it within the banks and we made within the banks also instructions for the employees – how to deal with access requests, how to set up direct marketing activities, what is allowed and what is not allowed, the sharing of data among business units." Interviewee 1 40:30.

[261]*See supra* notes ___-___ and accompanying text.

[262]Interviewee 8 1:16:30 (describing "the cowboys who don't care").

membership, that firms commit to comply with the code.[263] Finally, they expelled or otherwise sanctioned member firms that violated the code in a significant way.[264] Companies believed that such measures would preserve the industry's reputation and head off public pressure for direct government regulation.[265] They further thought that they would give customers a way to differentiate good actors from bad–to see the "difference between the black and the white sheep."[266]

---

[263]The private investigator industry took this a step further. In the Netherlands, private investigators must comply with regulatory requirements and obtain a license from the Ministry of Justice in order to operate. In an effort to make its code of conduct binding on all companies in the sector, the industry association successfully lobbied the Ministry of Justice to build the code into the regulatory requirements that firms must meet in order to obtain a license. Interviewee 7 25:00-26:00; Ministry regulations, section 23(a). This turned the code into a legally binding requirement for all private investigation firms, even those that did not belong to the industry association.

[264]Interviewee 12 (1:04) (former regulator describes); Interviewee 8 (1:17-1:19) (direct marketing industry expels); Interviewee 7 (1:01) (private investigator industry imposes fines). For example, the Direct Marketing Association learned that one of its members had shared personal information with a third party in violation of the industry code. The Association forced out the member and then issued a press release explaining why it had done so. Interviewee 8 (1:17-1:19). In another particularly interesting example of this the DPA found a particular trade information bureau to be in violation of the Personal Data Protection Act but, seeking to reward the firm for its cooperation with authorities, refused to release its name. The industry trade association, in an effort to preserve the sector's reputation, sought the name of the violator so that it could publicly expel it from the association, but the DPA refused to provide it. The association ultimately sued the DPA in an unsuccessful attempt to get this information. Interviewee 12 (2:11-2:12:30); Interviewee 5 (23:00-28:00). The association ultimately figured out on its own the identity of the offending firm and pressured it into leaving the organization. Interviewee 5 (29:00-30:00).

[265]As a representative of the trade information bureaus explained: "[t]he industry as a whole has an interest in getting companies to sign up for the code so as to protect the name of the industry. With all the free riders around, you can expect the legislature will draw his own rules to prevent them from doing things. The more organized we are, the less the legislature will need to create rules for us that would be more restrictive"; Interviewee 5 (1:11?), 1:29:30. As a representative of the direct marketing industry put it, the code provided a way to "protect our own business from others in our industry. Our mantra is: 'united we stand, divided we fall.'" Interviewee 8 (1:59). *See also* Interviewee 12 (1:25); Interviewee 12 1:48 (where industry has a code of conduct regulators "step back"); A representative of the banking industry explained that the sector developed its code in order to "demonstrate to the public and regulators that the industry is serious about protecting personal information," Interviewee 1 (4:00), and representatives for the trade information bureaus said they developed theirs "to show the outer world how we are handling the data." Interviewee 5 (28:00).

[266]Interviewee 5 (9:00); *See* Interviewee 12 (4:30) (code of conduct builds trust among customers. That can be a competitive advantage within an industry).

5. *Self-policing: monitoring peers*

While trade associations seemed eager engage in policing of smaller companies that they perceived to be irresponsible, they seemed far less inclined to monitor the compliance of their core members, the more established firms. Instead, with one exception that I will discuss below,[267] the associations eschewed monitoring and focused instead on responding to consumer complaints or DPA enforcement actions.[268] Typically, industries used an independent supervisory board for this purpose.[269] The industry code would authorize the board to hear individual complaints and to expel those companies it found to be in violation of the code. However, neither the board, or any other arm of the trade association, would monitor compliance or otherwise seek to uncover violations.[270]

Such a reactive system almost ensures that many violations will go unnoticed. Most individuals know very little about how their personal data is collected and used and so will fail to spot many more violations than they detect.[271] Any system that relies on individual complaints to

---

[267] *See infra* notes ___-___ and accompanying text.

[268] Several codes of conduct do require firms to audit and certify their own compliance. These include the private investigators' code, Art. 12, Interviewee 7 (1:05-1:06:30), the banking code, Code 1Chapter 9, Code 2 Chapter 10, Interviewee 7 (1:10), and the direct marketing code, Interviewee 8. 17:00. The evidence did not show the extent to which trade associations monitored and enforced compliance with this self-certification requirement. However, I did learn that the banking code initially required members to conduct self-audits annually but later changed this to make the process less frequent. Compare Financial Institutions Code 1, Chapter 9 (annual self-audit), with Financial Institutions Code 2 (less frequent); Interviewee 7 1:10.

[269] Interviewee 8 (1:02, 1:18) (direct marketing industry); Interviewee 7 (59:00) (private investigators); Interviewee 5 (13:30-15:00) (trade information bureaus); Interviewee 11 (1:26-1:28) (banking industry).

[270] Interviewee 9 (1:17:30) (pharmaceutical industry); Interviewee 11 1:24-1:25 (banking industry); Interviewee 5 1:08 (trade information bureaus).

[271] The industry representatives that I interviewed reported that a very low number of individuals had availed themselves of the trade associations' complaint process. *See* Interviewee 11 (1:29:45) ("very few" complaints in banking sector); Interviewee 5 (1:05) (only six complaints against trade information bureaus since 2003).

identify violations is therefore bound to miss many of them. Indeed, the lead data protection attorney for one industry association candidly told me that, due to the lack of monitoring, "we don't know" whether firms in the sector are abiding by the Code, or not.[272]

There have, as yet, been no comprehensive studies of industry compliance with the Dutch codes of conduct. Yet the evidence that does exist suggests that industry's reactive system, even when combined with the DPA's rather limited enforcement efforts,[273] is not terribly effective. In 2004 the Ministry of Justice, acting in response to a series of complaints, commissioned the only in-depth evaluation of compliance with a sectoral code of conduct–the private investigators' code.[274] The resulting report offered a discouraging picture of industry compliance. It found that while firms complied regularly with some code requirements, they violated others more than half the time.[275] Compliance with the requirement to notify employees who had been investigated but then found innocent–the very requirement that industry had fought over in the code negotiation process[276]–was particularly poor.[277] The study's "main conclusion . . . [was] that there is an incomplete compliance with the Privacy Code."[278] It attributed this, in part, to the industry

---

[272]Interviewee 11 1:23:30.

[273]*See supra* notes ___-___ and accompanying text.

[274]Regioplan Policy Research, *Evaluation of the Privacy Code for Private Detective Agencies* (Oct. 2007).

[275]Investigation firms complied with the requirement to notify data subjects of the investigation 91 percent of the time. However, they violated the requirement to use the least intrusive method only 56 percent of the time, violated the requirement to have two investigators present at interviews and the requirements for use of cameras nearly 66 percent of the time. *Id.* at IV.

[276]*See supra* notes ___-___ and accompanying text.

[277]Regionplan, *Evaluation*, *supra* note ___, at IV.

[278]Regioplan, *Evaluation*, *supra* note ___, Summary at V.

perception that the probability of detection of non-compliance was low and that this led some firms to take a more "free" approach to compliance with the code.[279] While one must be careful not to read too much into a one study of a single industry, the report does raise important questions about the effectiveness of industry self-policing and about compliance more generally under the Dutch code of conduct system. Increased industry ownership and acceptance of the rules may not be sufficient to ensure compliance with them.

6. *Third-party certification*

If agencies lack sufficient resources adequately to monitor and enforce data protection law,[280] and industry trade associations lack the incentive to do so,[281] then who can assure compliance with privacy codes of conduct? The Dutch experience suggests an intriguing answer to this question. In the aftermath of the Ministry of Justice report, the Private Investigators Association, seeking to improve the industry's damaged reputation, adopted a new program of required, annual, *third-party* compliance audits. The Association trained a group of independent "certifying professionals" on how to assess compliance with the industry code of conduct. It then required every member to hire an independent auditor every three years to examine both its current compliance with the code and its management system for achieving compliance in the future. Firms that received passing marks could display a Quality Mark logo as a sign of their sound data protection practices. Those that did not would face the loss of their Association membership.

---

[279]Regioplan, *Evaluation*, *supra* note ___, Summary at VI.

[280]*See supra* notes ___-___ and accompanying text.

[281]*See supra* notes ___-___ and accompanying text.

The private investigator industry's Quality Mark program appears to address a number of the problems identified above. It reduces the trade association's conflict of interest by taking the monitoring and auditing function out of the association's hands and placing it in those of an independent certifying organization (albeit one that the association has trained). It avoids the problem of limited agency resources by requiring the regulated party itself to pay for the audit. Finally, by granting a Quality Mark to those firms that successfully pass muster, the program creates incentives for more responsible behavior. It is too early to tell how the Quality Mark program will affect compliance in the private investigator industry. A follow-up study that compared compliance under the Quality Mark, third-party certification program with that which the Ministry of Justice found in its 2004 report, would be very useful.

7. *Enforcement mind-set*

Critics predict that collaborative methods will lead to a weakened enforcement mind-set. While the interviews did not provide specific evidence of this the Data Protection Authority has, in recent years, expressly decided to focus less on advice, compliance assistance and codes of conduct, and more on enforcement.[282] The DPA is still negotiating and approving codes of conduct. But it is doing so in a streamlined fashion that relies more on written submissions than in-person discussions. It is putting more resources into enforcement.

I heard various explanations for this shift. Some attributed it to the 2004 replacement of the initial DPA Chair, who was oriented towards the advice and interpretation function, with a new Chair who had more of an enforcement mentality. Others saw it as a way for the DPA to

[282] *See* DPA annual reports announcing shift to more enforcement.

bolster its image in the eyes of the public and questioned whether the small agency could achieve meaningful enforcement, even with a greater allocation of resources.[283] Yet others, including a current DPA official explained that the advice-giving function, including the negotiation of codes, had been sapping too many agency resources and that this had detracted from the DPA's enforcement efforts.[284] As a result, regulated companies came to believe that enforcement was not a real threat and so made less effort to comply. While this last explanation does not precisely track the critics' concern–it focuses more on agency resources than on agency mind-set–it does connect the code of conduct approach with a lessening in agency enforcement efforts. The evidence for such a connection is incomplete and, as just mentioned, open to various interpretations. But it does suggest the need for further research into this point and, in particular, into the Dutch DPA's recent decision to emphasize enforcement and devote fewer resources to code formation and compliance assistance.

E. Unanticipated Functions of the Dutch Codes of Conduct

Thus far, this Part has looked at what the Dutch experience can tell us about the theorists' views on codes of conduct. Once in existence, however, codes of conduct take on a life of their own. They function in ways that policymakers and scholars may not have predicted. The interviews revealed some of these unanticipated and emergent functions of the Dutch codes of conduct.

[283]Interviewee 10 30:00-31:00 (new emphasis on enforcement will not make difference because "[y]ou have to monitor the whole society, to inspect, and that is impossible.")

[284]Interviewee 4 I 6:00-7:30.

1. *Cycle of interpretation*

As originally designed, the Dutch code of conduct program assumed that Data Protection Authority would approve the codes and would itself be bound by them. The courts, however, would remain free to interpret the Data Protection Act on their own. But this is not the way it has turned out in practice. Instead courts, faced with the task of interpreting the Act, have in a number of cases turned to the relevant code of conduct and simply adopted its interpretation.

For example, a private investigator's walk-by observance of an insured in his home revealed that the insured was not, in fact, injured in the way that he had claimed that he was.[285] When the company refused to pay on the claim, the insured brought suit on the grounds that the investigator's surveillance of him in his home violated the Data Protection Act. In its ruling, the court looked to the provisions of the private investigator's code of conduct that govern walk-by surveillance of a person's home, found that investigator had acted in accordance with these rules, and so held that the investigator's behavior did not violate the Act.[286] In short, the court adopted *the code's* interpretation of the Act.

Given that the DPA had reviewed and approved the code, the court's reliance on the document is understandable and, perhaps, unremarkable. But the process did not stop there. In its opinion, the court added its own gloss to the conditions under which walk-by observation would be permissible.[287] The private investigator association, wanting to make sure that its guidelines were in accordance with the latest law, then revised its code of conduct to incorporate the judicial

[285]*See* Interviewee 7 (2:15-2:16).

[286]Interviewee 7 1:30-1:33; 2:15-2:16.

[287]Interviewee 7 2:15-2:16.

views on walk-by observation.[288] Thus the code shaped the law which, in turn, shaped the code. According to a representative of the private investigator industry, such a cycle would continue. Additional court decisions would adopt the revised code and, again, would add some judicial gloss to it. The association would then revise the code to reflect the new jurisprudence. Over time, this would produce an unending cycle of statutory interpretation of elaboration. "[I]t goes on and on and on. It is a dynamic circle. The code leads to the court decisions, the court decisions lead to the code. It all gets more elaborated over time. And from that the private investigators get a better idea of what they can and cannot do better than just from the broad terms of the statute. Yes. That's what happened."[289]

2. *Migrating codes*

The courts' adoption of code provisions also has another fascinating effect. It expands the a code's reach far beyond the companies that formally sign up to comply with it. The expansion happens in two directions. First, judicial decisions bind all companies in a given industry. When a court adopts a code's interpretation of the Data Protection Act, the resulting judicial decision accordingly makes the interpretation binding on all similarly situated companies including those that never agreed to follow the terms of the code.[290] In this way, court decisions can expand a code's reach to cover, not just those firms that have signed up to comply with it, but also those companies in the sector that have not done so.

---

[288]Interviewee 7 2:15-2:16.

[289]Interviewee 7 2:16.

[290]*Cf.* Interviewee 12 50:00 (DPA will apply interpretations contained in code to companies in that industry that have not signed up to comply with the code).

They can also cause codes to spread in another, even more far-reaching way. The Data Protection Act, and judicial decisions interpreting it, bind all industries. Where a court adopts a code's interpretation of the Act then that interpretation indirectly becomes part of the law binding on all industries.[291] In this way a code from one industry can, through judicial incorporation, "migrate" to other industries and influence how the Act applies to them. The Dutch experience provides a clear example of this. The private investigator industry code does not bind insurance company investigators since they belong to a different sector.[292] But the Data Protection Act, and judicial decisions interpreting the Act, do apply to them. This has led some insurance companies voluntarily to adopt the private investigators' code of conduct as a guideline for their own investigators in their efforts to verify claims. The insurance companies believe that this will make it more likely that courts will uphold their employees' investigatory practices.[293] As one seasoned practitioner who has assisted both industries with data protection compliance observed: "What is interesting is that it started as an initiative from a specific industry [i.e. the private investigators], which was heavily under fire, and now this code evolves into the code of the insurers . . . It goes beyond the scope of [the original] industry."[294]

3. *Codes to integrate statutes*

Industry also used the Dutch codes of conduct to bring together a wide variety of legal requirements relating to personal information–arising not just from the Data Protection Act, but

[291]Interviewee 7 (2:17).

[292]Interviewee 7 (2:17-2:18).

[293]Interviewee 7 (2:19).

[294]Interviewee 7 (2:20).

from other statutes as well–and integrate them into a single document, the code. This allowed companies to look to one document for all legal requirements related to personal information and so made it easier for them to comply with these various provisions. For example, both data protection law and telecommunications law govern how the direct marketing industry can use personal information that it collects. The industry accordingly integrated both sets of requirements into its data protection code of conduct, thereby providing itself with a single, unified statement of its legal obligations. A representative for this industry remarked that "something that is very powerful about [a code of conduct] is that you bring out all the bits and pieces relevant for your industry from all different kind of directives together in one document."[295]

4. *Codes to resolve conflicts between statutes*

The Dutch sectors did not only use codes to bring various statutes together; they also employed them to resolve the conflicts between statutes. The pharmaceutical industry code provides an example of this.

When a pharmaceutical company wants to test a new drug it hires independent medical professionals to run the trials. These professionals collect large amounts of personal data from the trial participants. A health care regulation requires the pharmaceutical companies to notify, or verify that the medical professional has notified, trial participants where the company learns that

[295]Interviewee 8 (42:50); *see also id.* (49:00) (prevents you from having to go through a whole pile of laws); Interviewee 7 (1:15) (private investigator industry uses code to integrate two statutes governing the use of hidden cameras); Interviewee 12 (14:40) (former regulator recounts that sectors used codes to integrate requirements from various laws and statutes into single document).

the drug being tested could be harmful.[296] The medical professionals accordingly made a practice of providing participants' initials, country of origin, birth date, birth year, and gender[297] to the sponsoring pharmaceutical companies. This allowed the companies separately to identify each trial participant and so to verify that each had received the required notification.

The Data Protection Act limits the extent to which medical professionals can share "personal data" with a third party such as the sponsoring pharmaceutical company. Prior to 2007, the companies had assumed that since the information they were receiving did not enable them to identify the specific participant, it did not qualify as "personal data."[298] But a 2007 opinion of the Article 29 Working Party[299] made it impossible to hold this view. Concerned about entities' increasing ability to use "anonymous" personal information to identify the individuals concerned, the Working Party broadened its definition of the types of personal information that, when used in combination, could be employed to identify an individual.[300] Under the revised definition it became clear that the medical professionals *were* providing "personal data"[301] and that their sharing accordingly violated the Act.[302] This put the Data Protection Act squarely in conflict with

---

[296]Interviewee 9 (23:00).

[297]Interviewee 9 (28:00?)

[298]2000 Data Protection Act Art. 1(a) (defining "personal data" as "any information relating to an identified or identifiable natural person.")

[299]The Article 29 Working Party is an E.U.-level entity that provides expert opinions on data protection law. *See* <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/tasks-art-29_en.pdf> (last visited April 25, 2012).

[300] Interviewee 9 (22:00, 30:00).

[301]Interviewee 9 (31:00).

[302]Interviewee 9 (24:30).

the health care regulation which implicitly *required* such sharing of data.[303]

The pharmaceutical industry trade association and the DPA used the code to resolve the conflict. First, industry members met and determined that, at an "absolute minimum," they needed participants' date of birth and year of birth in order to separate out the participants and comply with the health care regulation.[304] After some negotiation the DPA agreed that the industry could have these two pieces of information, but no more.[305] The parties implemented the agreement in Section 2.7 of the pharmaceutical industry code which provides that "date of birth and year of birth are not usually traceable to the individual" and so do not constitute information that renders a person identifiable.[306] This short phrase allowed the pharmaceutical companies to resolve the tension between two, conflicting statutes.[307]

VI. Recommendations for U.S. Privacy Law and Policy

The Dutch experience shows that the code of conduct approach has important virtues. It can promote information sharing and problem solving; lead to more tailored, workable and cost-effective rules; increase industry awareness of its privacy impacts and give it a sense of ownership over the rules needed to mitigate them; initiate an iterative process by which broad statutory requirements get interpreted and clarified; and provide a means to resolve conflicts

---

[303]Interviewee 9 (23:15).

[304]Interviewee 9 (42:30). The location of the trial would also give them country of origin. With these three pieces of information they could separate out the various trial participants.

[305]Interviewee 9 (24:30)?

[306]NEFARMA, *Code of Conduct Concerning the Processing of Personal Data* § 2.7; Interviewee 9 (52:00-55:00).

[307]*See also* Interviewee 8 (49:15-51:00) (direct marketing industry uses code to resolve conflicting statutory requirements).

between statutes. Yet the Dutch codes also reveal significant weaknesses in this regulatory method. The Dutch codes are slow-moving and static, not nimble and adaptive. In some situations at least, industry can exert too much leverage in the drafting process, resulting in overly lenient rules. Sectors do not routinely monitor their members' observance of the rules and, in one industry at least, a study found wide-spread non-compliance. Established players can use the codes to strengthen their own position and discourage new entrants.

What lessons are we to draw from such a mixed picture? On the one hand, the Dutch experience suggests that the strengths of the collaborative, code of conduct approach are not mere figments of the theorists' imaginations. Information sharing, problem solving, tailoring of rules–these things do happen, and the Dutch codes provide concrete examples of them. This suggests that the U.S. move towards safe harbor programs and codes of conduct could be a productive one. At the same time, the Dutch experience suggests that if the U.S. is to utilize this approach, then it must do so in a way that is sensitive to both the strengths, and the very real weaknesses, of this regulatory method. It must design its program in a way that will mitigate and minimize the weaknesses and the same time as it maximizes the strengths. The remainder of this part suggests how policymakers might build on the Dutch experience in order to achieve this.

A. Minimizing Weaknesses

We begin with the ways policymakers could design the U.S. program to mitigate the weaknesses in the code of conduct approach.

1. *Require third-party audits*

The Dutch code of conduct program demonstrated a weakness with respect to monitoring,

enforcement, and compliance. The small, understaffed Dutch DPA does not have the resources to monitor the many companies that use personal data. Industry sectors show little interest in the kind of comprehensive self-policing that would be needed to fill this gap, choosing to rely instead on individual complaints. The Ministry of Justice study of compliance in the private investigator industry, while limited to a single industry, showed wide-spread non-compliance.

How to address this weakness? The private investigator industry's third-party certification program provides a possible strategy. It addresses the agency resource problem by requiring industry to pay for the monitoring, thereby allowing the regulators to focus their resources on evaluating and approving the auditors. It also overcomes the industry trade association's reluctance to monitor its own members by placing the responsibility, instead, in the hands of approved, professional auditors. It is worth noting that the private investigator sector did not fight this requirement. Instead, the more established members embraced it as a way to demonstrate their sound practices and differentiate themselves from less responsible competitors. Neither the U.S. privacy bills, nor the White Paper, include third-party audits of compliance or of management systems. The Dutch experience suggests that they should.

2. *Build in stakeholder input*

The Dutch codes suggest another possible weakness. In some instances, industry may be able to exert disproportionate influence over the shape of the code, resulting in overly lenient code provisions. I found only one, clear example of this – the private investigator industry's ability to convince regulators that employer who hired the investigation company, not the

company itself, should notify an innocent employee that he had been investigated.[308] Still, such instances are a warning sign that industry groups may, in some circumstances, be able to tilt the codes in their favor.

One way to mitigate this would be to open up the code negotiation process on include other stakeholders such as consumer or privacy advocacy groups. The Dutch themselves seemed to be aware of this and, in their 1989 Data Protection Act, required industry to consult with consumer representatives during the code drafting process. However, the small number of such groups made it impossible for industry associations to comply with the requirement and the 2000 Act accordingly dropped it.[309]

The U.S. faces no such shortage of sophisticated and well-resourced consumer and privacy groups and the idea should be revisited here. The presence of stakeholder groups in the code or safe harbor negotiation process would have at least three beneficial effects. It would provide a counter-weight to industry influence and so promote more balanced rules. It would increase the transparency of the negotiation process and create more accountability for those involved in it. And it would bring another set of well-informed minds to bear on the issues. The U.S. proposals appear to understand the importance of stakeholder involvement. The White

---

[308] *See supra* notes ___-___ and accompanying text.

[309] The 1989 Act required industry drafters to consult with representatives of data subjects and instructed the Authority to approve a code only if "there has been sufficient consultation with organizations of interested persons, including data subjects." Law on Personal Data Files, § 15. However, due to the lack of organized privacy groups in the Netherlands, business representatives found it hard to find enough qualified privacy advocacy groups to consult with. This made the consultation requirement unworkable. Interviewee 2 46:30, 50:00 (there were no appropriate candidates; Sometimes it was, "who in the hell should I address this to?"; this made the stakeholder input mechanism unworkable.) The 2000 law accordingly dropped this requirement. The upshot is that, today, the industry sector drafts the code and negotiates it with the Authority. Privacy advocates and other stakeholders generally do not get to see a code until it is formally proposed for public comment. This is often too late in the process to have a meaningful impact on the content of the code.

Paper calls upon "multi-stakeholder groups" to develop the codes of conduct.[310] These groups will include "individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups."[311] This is significant departure from the Dutch program in which industry trade associations draft the codes largely on their own.

While the White Paper's proposal is on the right track it may pose a problem of a different sort. Government officials need industry information in order regulate the fast-changing information economy. One of the main reasons for using codes is that they can a encourage industry members to share more of this critical information with regulators. But will they do this with public interest stakeholders sitting at the drafting and negotiating table, as the White Paper envisions? I posed this question to government officials who played key roles in the Dutch code negotiations and their answer was a clear and unequivocal "No." In their experience, the way to get industry to open up was to create a safe environment in which companies knew that the information they shared would not be used against them. As one regulator described it, industry provided information because "[w]e were not there in our role as regulator. Our aim was not to inspect. It was to see whether the code will work for reality. Why did they allow us? We trusted each other. It came down to personal trust."[312] These government officials believed that including public interest stakeholders at the initial drafting stage could undermine this sense of trust and so

---

[310]White Paper at 23.

[311]White Paper at 23.

[312]Interviewee 10 (40:–43:00); *see supra* notes ___-___ and accompanying text (discussing this example at greater length).

either choke off the vital information flow, or drive it underground.[313] One compared it to the legislative process: "In a parliament, you have all the relevant parties in a room. And still, the real deals are being made outside of the room. The public part of a parliament serves the deal-making which happens elsewhere. Bringing third-party stakeholders in the process would be great. But having them in the room all the time would not be helpful. That would probably encourage telephone conversations to prepare the meeting."[314] Thus, according to the Dutch regulators, bringing stakeholders in at the initial drafting stage would be too early. On the other hand, waiting until the public comment stage would be too late. At that stage, the agency has already made a public commitment to the draft code and commentators face an uphill battle in getting the agency to change it.

A Dutch lawyer suggested an alternative solution: divide the drafting and negotiation process into two stages. In the first, industry and government would collaborate on an initial, tentative draft. In the second, public interest stakeholders such as consumer or privacy groups would join the discussion and provide their reactions and ideas. Only later would the agency put the document out for public comment (at which point stakeholders would have another chance to weigh in on it). Stakeholders participating in the second stage would not be able to exercise veto power over the document. However, they would be able to review it and "cry foul" to the policymaking community, or even the media, if they believed it to be one-sided. This could add transparency and accountability to the process without undermining the trust and information-

---

[313]Interviewee 4 II (5:00-8:00) (including stakeholders at an early stage would make the negotiations too difficult).

[314]Interviewee 2 (51:00-53:00). See recent NYT article on (do not track)? Industry wants to meet in private. Otherwise people will sit on their hands.

sharing that can emerge from government-industry interactions.[315] Industry might even benefit from stakeholder involvement since it would give the code a "label of quality" that would increase consumer faith in the resulting document.[316] U.S. policymakers should consider using such a staged approach

3. *Improve adaptability*

The Dutch codes also display a third, important weakness. They are slow-moving, largely static instruments. Some took years to negotiate. Others lapsed at the end of their initial five-year period because industry and regulators could not reach agreement on whether and how to update them. This finding contrasts sharply with both the theoretical literature and with the Administration policy papers, all of which claim that collaborative methods such as codes of conduct will be nimble and adaptable instruments and that this is one of their main advantages over traditional rulemaking.

How to make codes and safe harbor programs more adaptable? In the field of environmental law, regulators have experimented with pre-approval of insignificant permit changes, streamlined administrative approval, and other mechanisms designed to speed up the permit revision process. These experiments might prove instructive. At minimum, policymakers and scholars should be sure to track the time and resources it takes to negotiate and revise U.S. privacy codes of conduct. They should also do more research on the possible ways to streamline these processes without sacrificing accountability.

---

[315]Interviewee 12 (1:54:45) (supporting this idea).

[316]Interviewee 11 (1:58-2:02).

4. *Protect new entrants*

The Dutch experience further suggests that established firms can use industry codes of conduct as a way to deter new entrants. A U.S. code of conduct program should take measures to reduce this tendency. For example, program rules might require that the industry representatives drafting a code must include not only the larger established companies, but smaller, newer ones as well. In addition, the program might invite regulators from the FTC's Bureau of Competition to scrutinize codes for possible anti-competitive effects. Measures such as these could reduce any cartel-like tendencies in the code drafting process.

B. Maximizing Strengths

Policymakers should also design the safe harbor program so that it maximizes the strengths of this regulatory approach. The Dutch experience provides a number of lessons on how to achieve this.

1. *Make the safe harbor programs sectoral*

Privacy regulators face a real problem. They must develop rules for a highly complex array of industries whose technologies and business models are changing at an incredibly rapid pace. Yet the regulators know little about the present state of these industries, and even less about what they will look like in the future. To do their jobs, they need industry members to share their superior knowledge of upcoming technologies and business realities. The Dutch experience shows that codes of conduct can facilitate this exchange of information. Indeed, their key advantage appears to be their capacity to develop relationships through which an industry sector can share information about its business with regulators. This can lead to more tailored, workable and cost-effective rules.

Safe harbor programs that seek to encompass companies from many different sectors will find it far more difficult to tailor their rules to *particular* sectoral realities and so will lose much this benefit.[317] Yet that is precisely what the bills and the White Paper propose. For example, the Kerry-McCain bill provides that any "nongovernmental" organization can initiate a safe harbor program.[318] While such an NGO might design its program on a sectoral level, it need not do so.[319] Indeed, NGO's that want to attract a large number of companies to their program will have an incentive to define the scope broadly. The other bills and the White Paper are similar.

The Dutch experience suggests that this is a mistake. In order to achieve the principal benefit of the safe harbor approach–the sharing of information about industry realities–the programs should be drawn at the sectoral level. Following the Dutch model, the U.S. proposals should establish their safe harbor programs at the sectoral level.

2. *Include all statutory requirements*

If an industry sector can provide information that makes rules more tailored and intelligent, then it should be allowed to do this with respect to all statutory requirements, not just a few of them. Yet two of the three bills strictly limit the scope of their safe harbor programs.[320] The Rush bill extends the safe harbor approach to notice and choice (Title I) and accuracy and

---

[317]Indeed, experience with broad-scope safe harbor programs under the Children's Online Privacy and Protection Act show that the NGOs have achieved little in the way of tailoring and have tended to seek information from government, rather than providing insights to it.

[318]Kerry-McCain Bill § 501(a).

[319]*See supra* notes ___-___ and accompanying text.

[320]Stearns Bill §

access (Title II), but not to data minimization, data security and accountability (Title III).[321] The Kerry-McCain bill narrows the scope still further, defining safe harbor programs so that they set the rules only for the bill's requirements with respect to unauthorized uses of personal information, and not for other statutory requirements.[322] The Dutch Data Protection Act, on the other hand, sets no such limits. It calls on industry sectors to address all aspects of the statute in their codes of conduct. As was illustrated above, Dutch sectors were able to utilize this authority to customize a wide variety of statutory requirements. The U.S. proposals should follow this model and should apply the safe harbor approach to all statutory requirements.

3. *Pass a Baseline Privacy Statute*

The preceding recommendation assumes that the U.S. Congress will pass legislation that sets baseline privacy requirements for all economic sectors. But this is not a given. While the White Paper recommends such legislation, it also calls for using multi-stakeholder codes of conduct in the absence of a statute. The Dutch experience suggests that the Dutch sectors' main motivation for drafting their codes of conduct was that it allowed them to clarify the Data Protection Act and achieve a degree of regulatory certainty.[323] Without a statute, companies may not want to invest the resources needed to draft and negotiate a code. While the White Paper anticipates codes in the absence of legislation, the Dutch experience suggests it may have a hard

---

[321]Rush Bill § 403(2)(d).

[322]Kerry-McCain Bill §§ 501(a)(1), 501(c). In a later provision, the bill suggests that the safe harbor will extend to all requirements contained in Titles II and III. Kerry-McCain § 502(a). It is unclear how this relates to the earlier provisions limiting the scope of the safe harbor programs. Even under the broader reading, the bill still excludes from the safe harbor the statutory requirements in Title I governing security, accountability and privacy by design.

[323]*See supra* notes ___-___ and accompanying text.

time getting companies to answer this call. Congress should pass a baseline privacy statute, not only for the privacy protections it will bring, but also to give companies an incentive to come to the table and negotiate a code of conduct.

4. *Recognize safe harbor participants*

Another interesting lesson from the Dutch experience is that some companies invest in codes of conduct as a way to differentiate themselves from less responsible competitors.[324] The American proposals should build on this useful impulse by providing public recognition to those companies that sign up for a safe harbor program or code of conduct. For example, they could designate such firms to be "privacy leaders" or give them the right to display a special logo. Such measures would strengthen the reasons for participating in a safe harbor program. They could even create a virtuous cycle in which all companies in an industry come to feel the need to sign up for the code in order to remain competitive.

5. *Use codes to create a global standard*

In the Netherlands, several sectors used their code of conduct as a means to integrate requirements from a number of different statutes, thereby providing themselves with a single, unified set of rules. This practice could suggest a solution to one of the most vexing problems in privacy regulation: how to harmonize conflicting national or regional privacy regimes.

Data flows are global. But the laws that govern them are generally national or, in the case of the E.U., regional. Companies that transmit personal data across national boundaries accordingly have to keep track of various national and regional data protection requirements and

[324] *See supra* notes ___-___ and accompanying text.

make sure that they comply with all of them. This can be a complex and daunting task.

Industry codes of conduct could provide a solution. Just as the Dutch sectors drafted codes that integrated a number of statutes, so American sectors could craft codes of conduct or safe harbor programs that brought together and incorporated the requirements of the various regional laws. These other systems are already set up to accommodate this. The 1995 E.U. Data Protection Directive allows industry sectors to propose, and the Article 29 Working Group to approve, *community-wide* codes of conduct that create a safe harbor with respect to all E.U. member states. Similarly, the Asia-Pacific Economic Cooperation (APEC) organization's Cross-Border Privacy Rules system allows approved "Accountability Agents" to certify a single set of privacy rules as being compliant with all national laws in the region. Were an American sector to succeed in having the FTC, the Article 29 Working Group, and an approved APEC Accountability Agent approve an industry code of conduct or safe harbor program as being compliant with their respective national or regional laws, the resulting code would then constitute a single, globally interoperable, set of privacy rules. The emergence of such codes could facilitate cross-border data flows, reduce costs to business, and provide consumers with more consistent levels of data protection as their personal information travels the globe. The U.S.-E.U. Safe Harbor Agreement takes a step in this direction and the Administration White Paper also expresses an interest in it.[325] To facilitate such a development, the current U.S. proposals should seek to align their safe harbor program as much as possible with the E.U. code of conduct approach. This is another good reason to make the safe harbor programs sector-based, as opposed

[325]White Paper at 31-33. The author and a colleague suggested the idea in comments on the Department of Commerce's Green Paper.

to making them free-form entities that encompass companies from many different industry sectors.

VII. Conclusion: Transferability and the Questions It Raises

The United States and the Netherlands differ in their size, geography, population, culture, history, and many other areas. The Dutch codes have worked in some important respects. But will the approach function as well in the United States as it has in the Netherlands? Are the lessons from the Dutch codes transferable to U.S. soil?

At first blush, it appears that they might not be. As was explained above, Dutch history that has forged a culture based on cooperation and consensus.[326] This may predispose the Dutch to the type of collaboration and problem-solving that lie at the heart of the safe harbor approach. People involved in the Dutch codes of conduct, and scholars writing about them, have referred repeatedly to this history, and to the "polder model" of regulation to which it gave rise, as a reason for the program's success.[327]

As Robert Kagen has shown, U.S. regulatory culture is very different. It is rooted in interest representation and factionalism, not cooperation. This has led to an adversarial regulatory style in which interest groups battle the regulators and each other to get as much of their agenda into law as possible. Insofar as they reach a compromise, they do so as the end product of this battle, not through a process of cooperation and consensus. This raises a real question as to whether American companies, regulatory officials and public interest groups could drop their adversarial postures long enough to engage in they type of cooperative discussions and problem-

[326] *See supra* notes ___-___ and accompanying text.

[327] *See supra* notes ___-___ and accompanying text.

solving that the Dutch seem to have been able to achieve and that is essential to the safe harbor approach.

Yet, in considering the Dutch experience as a whole, one also has to wonder: could the adversarial American regulatory culture prove to be an advantage? As was explained above, the safe harbor approach can allow industry representatives to exert too much leverage. The Dutch themselves recognized this problem and tried to bring consumer groups into the drafting process as a way to mitigate it. But the small number and limited resources of these groups made this impossible.[328] Were the U.S. to implement the safe harbor approach the situation would be very different. Due to its adversarial culture and is greater size the U.S. has an abundance of consumer and privacy advocacy groups with the resources and ability to negotiate a code of conduct. This is a real strength when it comes to implementing the safe harbor approach. If these groups became involved in the negotiation process, in the manner recommended above,[329] they could serve as a counter-weight to industry and so produce a more balanced, transparent and accountable negotiation process.

The U.S. code of conduct program would then confront the real question: can the industry, government and public interest stakeholders temper their adversarial nature sufficiently to cooperate together on crafting intelligent regulation while, at the same time, retaining enough of it to check one another and ensure a balanced outcome? If so, then U.S. privacy codes of conduct could work even better than Dutch ones have. If not, then the process would likely bog down in adversarial wrangling. The only way to find out is to give it a try.

---

[328] *See supra* notes ___-___ and accompanying text.

[329] *See infra* notes ___-___ and accompanying text.