GOING DUTCH? COLLABORATIVE DUTCH PRIVACY REGULATION AND THE LESSONS IT HOLDS FOR U.S. PRIVACY LAW

Dennis D. Hirsch[*]

2013 MICH. ST. L. REV. 83

TABLE OF CONTENTS

---

* Geraldine W. Howell Professor of Law, Capital University Law School. Fulbright Senior Professor (2010), Institute for Information Law, University of Amsterdam, Faculty of Law, Amsterdam, the Netherlands. This Article would not have been possible without the assistance and support of others. The author conveys his deepest thanks to: the Fulbright Program, sponsored by the U.S. Department of State, which funded the author's semester in the Netherlands; the Institute for Information Law (IViR) of the University of Amsterdam, Faculty of Law, particularly Professor Bernt Hugenholtz, Professor Nico van Eijk, and Anja Dobbelsteen, who made the author feel welcome and facilitated his research; Capital University Law School, which provided the sabbatical and summer research grant required for the research and writing; the interviewees, who gave generously of their time and knowledge; Professors Peter Swire and Dan Solove, who offered early encouragement and support; Professors Bert-Jaap Koops, Ira Rubinstein and Dan Fiorino, who commented on early drafts; Kim de Beer, Bob de Jong, Jennifer Lause, and Abi Zimmerman, who provided highly effective research assistance; and, most especially, the author's wife Suzanne and children Clara and Zander, who embarked with him on an adventure to the Netherlands and were the best traveling companions anyone could ever hope for. The author claims sole responsibility for the any errors or omissions in this Article.

INTRODUCTION

Privacy law 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 locations,[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 communication technology and that regulation will therefore impede growth in this increasingly important economic sector.[4] They insist that only industry, which knows the emerging technologies and business models far better than government, is in a position to establish workable

1. *See generally*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998) (providing a clear and informative overview of this phenomenon).

2. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS iii (1998) (stating that Federal Trade Commission research "shows that the vast majority of websites—upward of 85%—collect personal information from consumers"); *accord* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1629-31 (1999) (describing how and why websites collect personal information).

3. Jared Strauss & Kenneth S. Rogerson, *Policies for Online Privacy in the United States and the European Union*, 19 TELEMATICS & 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.*, Orson G. Swindle, Comm'r, Fed. Trade Comm'n, Address to the Reston Chamber of Commerce (Apr. 8, 1999), *available at* http://www.ftc.gov/speeches/swindle/reston.shtm ("[G]overnment regulation of privacy . . . will inevitably be inflexible and outdated and will stifle the growth and innovation of electronic commerce.").

rules.[5] They believe that industry self-regulation should provide the framework for protecting individual privacy interests.[6]

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.[7] At the same time industries have tried self-regulation, but nongovernmental organization (NGO) and government evaluations of these efforts have repeatedly found them to be lacking.[8] 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. Three bills currently before Congress[9] and a long-awaited 2012 White House policy paper on privacy regulation (the White Paper)[10] contain a kernel of something new. Each calls for government and regulated industries to work *together* to produce commercial privacy rules. Under these proposals, Congress would pass broadly-worded privacy requirements for business.[11] The regulated companies themselves,

---

5. *Id.* (calling for "an Internet privacy initiative under which industry takes the lead to address citizens' concern[s] about privacy through self-regulation devoid of government intrusion").

6. *Id.*; *see also* Robert E. Litan, *Law and Policy in the Age of the Internet*, 50 DUKE L.J. 1045, 1045 (2001) (explaining that 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 3, at 181 (discussing those who hold this view).

7. *See* MARCIA S. SMITH, CONG. RESEARCH SERV. RL 31408 INTERNET PRIVACY: OVERVIEW AND LEGISLATION IN THE 109TH CONGRESS, 1ST SESSION 18 (2006) (describing Internet privacy bills proposed in the 109th Congress and concluding that while some such bills were introduced in the House and Senate, none have passed).

8. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS iii (2010) (stating that 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 U. L. REV. 439, 455-64 (2011) (describing industry efforts at self-regulation and explaining how they have come up short).

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

10. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012) [hereinafter WHITE PAPER]. Prior to the issuance of the White Paper, the Department of Commerce released a preliminary version of the document known as the Green Paper. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010) [hereinafter GREEN PAPER]. Together, the White and Green Papers set out the Administration's position.

11. Kerry-McCain Bill, *supra* note 9, Titles I-III; WHITE PAPER, *supra* note 10, at 35; GREEN PAPER, *supra* note 10, at 23-30 (calling for adoption of a set of a baseline com-

possibly joined by other interested parties,[12] would then draft the detailed rules that spell out how the statute applies to specific industry sectors and situations and would submit these industry "codes of conduct" to regulators for approval.[13] Companies that followed an approved code of conduct would be deemed to be in compliance with the statute and would inhabit a legal safe harbor.[14] Firms that voluntarily committed to adhere to a code, and then failed to do so, would be subject to government enforcement.[15] The congressional bills call this method a "safe harbor" approach.[16] The White Paper calls it "enforceable codes of conduct."[17] Despite this different terminology, the basic concept is the same, and this Article uses the terms "safe harbor programs" and "code of conduct programs" interchangeably.

Safe harbor programs do not constitute direct government regulation since industry representatives draft the rules that spell out how the statute applies to particular firms. But neither do they represent pure industry self-regulation since Congress sets the baseline requirements and a regulatory agency must agree that the industry code fulfills the terms of the statute. Safe harbor programs are, instead, 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

---

mercial data privacy framework and noting that many commentators favored doing this through legislation).

12. The three bills and the White Paper differ somewhat on this point. The White Paper clearly calls for codes to be developed by "multistakeholder" 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 10, 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." H.R. 611, 112th Cong. § 401 (2011) [hereinafter Rush Bill]; H.R. 1528, 112th Cong. § 9 (2011) [hereinafter Stearns Bill]. 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, *supra* note 9, § 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.

13. WHITE PAPER, *supra* note 10, at 37; GREEN PAPER, *supra* note 10, at 42; Kerry-McCain Bill, *supra* note 9, § 501 (referring to these industry-drafted rules as "safe harbor programs" and allowing any NGO, including but not limited to industry associations, to develop such a program).

14. WHITE PAPER, *supra* note 10, at 37; GREEN PAPER, *supra* note 10, at 43-44; Kerry-McCain Bill, *supra* note 9, § 502(a).

15. WHITE PAPER, *supra* note 10, at 27; Rush Bill, *supra* note 12, § 403(2)(C).

16. Kerry-McCain Bill, *supra* note 9, Title V.

17. WHITE PAPER, *supra* note 10, at 23; GREEN PAPER, *supra* note 10, at 41.

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.[18] 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.[19] 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.[20]

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 inoculate the rules against industry bias? The safe harbor bills, and the momentum that they are gathering, require 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 II explains, scholars have analyzed the questions just posed. Proponents, such as Professors Jody Freeman of Harvard Law School and Philip Harter of the University of Missouri School of Law, maintain that collaborative methods can fundamentally change the relationship between traditional adversaries in the regulatory process.[21] 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.[22] Yet the collaborative approach also raises important concerns. Industry may seek to manipulate the rules to serve its own interests, and the government approval process may not be able to check this behavior.[23] As a result, collaborative methods may produce rules that favor industry over the public.[24]

---

18. *See generally* Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1 (1997). Others use the term "co-regulation" to describe the middle ground between direct government and pure self-regulation. *See, e.g.*, Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, J. L. & POL'Y FOR THE INFO. SOC'Y 355, 357, 371 (2010).

19. NEIL GUNNINGHAM & DARREN SINCLAIR, LEADERS & LAGGARDS: NEXT-GENERATION ENVIRONMENTAL REGULATION 154-55 (2002).

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

21. *See, e.g.*, Freeman, *supra* note 18, at 2; Philip J. Harter, *Collaboration: The Future of Governance*, 2009 J. DISP. RESOL. 411, 412.

22. *See* Freeman, *supra* note 18, at 26-28.

23. *See* GUNNINGHAM & SINCLAIR, *supra* note 19, at 105 (stating that industry "is likely to negotiate hard to minimise its commitments").

24. Daniel J. Fiorino, *Toward a New System of Environmental Regulation: The Case for an Industry Sector Approach*, 26 ENVTL. L. 457, 485 (1996) (explaining that collaborative

Riven by these conflicting views, the literature alone cannot settle the question of 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 to draw? Has anyone actually 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.[25] It involves a privacy statute with broad requirements; sectoral industry-drafted "codes of conduct"; government evaluation and approval of these codes; and a legal safe harbor for those firms that follow the approved code for their sector.[26] 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 codes for twenty sectors including banks, insurance companies, direct marketers, pharmaceutical companies, private investigators, commercial information bureaus, personnel recruitment agencies, medical researchers, and many other industry sectors.[27] 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

---

processes "could increase the chance that the regulatory process would be co-opted by industry").

25. *See infra* Part III (describing this Dutch regulatory program).

26. Wet persoonsregistraties, Stb. 1988, p. 665 (Neth.), *amended by* Stb. 1989, p. 480, ch. 4, art. 15 (Neth.) [hereinafter Law on Personal Data Files] (establishing a process for agency approval of industry codes of conduct); Wet bescherming persoonsgegevens, Stb. 2000, p. 302, ch. 3, art. 25 (Neth.) [hereinafter Personal Data Protection Act] (further explaining the process for agency approval of industry codes of conduct). Professors Bennett and Raab have identified five types of privacy codes of practice: organizational codes, sectoral codes, functional codes, technological codes, and professional codes. COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 155 (2006). They define sectoral codes as those "developed by industry associations for adoption by their member organizations," and functional codes as those "defined less by the economic sector and more by the practice in which the organization is engaged." *Id.* at 157. The Dutch codes, which are to be drawn up by industry "organisations" and interpret the statute in light of the "particular features of the sector or sectors of society in which these organisations are operating," Personal Data Protection Act, *supra*, art. 25(1), would qualify as sectoral or functional codes in the Bennett and Raab typology.

27. *See* Appendix: Dutch Data Protection Codes of Conduct (listing all twenty codes).

and how to implement such a program and on potential stumbling blocks and pitfalls that it might encounter.[28]

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. 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 United States should employ a collaborative approach to commercial privacy regulation and, if so, how it should go about this.

In conducting my research, I reviewed primary source documents (e.g. the codes of conduct and Data Protection Authority (DPA) publications) and the secondary literature on codes of conduct and Dutch privacy regulation more generally. However, I focused my research effort on face-to-face interviews with those who have been centrally involved in the Dutch data protection codes of conduct. I conducted twenty-six interviews with government officials,[29] industry representatives,[30] privacy advocates[31] and academics with expertise in data protection law (including two who had

28. For other relevant and informative literature on privacy and data protection codes of conduct, see generally Colin J. Bennett & Deirdre K. Mulligan, *The Governance of Privacy Through Codes for Codes of Conduct: International Lessons for U.S. Privacy Policy* (2012) (copy on file with author); BENNETT & RAAB, *supra* note 26, at 151-75; Peter J. Hustinx, *Co-Regulation or Self-Regulation by Public and Private Bodies – the Case of Data Protection,* Freundesgabe Büllesbach 283, 283 (2002), *available at* http://www.cbpweb.nl/downloads_artikelen/art_phu_2002_coregulation.pdf; Rubinstein, *supra* note 18.

29. The Data Protection Authority (the College bescherming persoonsgegevens) allowed me only a single interview with Commissioner Madeleine McLaggan-van Roon. I was not permitted to meet with other, current CBP employees. However, I was able to identify and meet with five former CBP employees (Ulco van de Pol, John Borking, Peter Hustinx, Richard Wishaw, and Jacqueline Wierdak) with long experience at the agency and with the codes of conduct.

30. I met with ten industry representatives who, among them, represented the following industries: banking (Jan Berkvens, Bruno van der Burgh), pharmaceuticals (Matthijs van Blokland), private investigators (Felix Olijslager, Pieter Ijfs, Carlo Cahn), trade information bureaus (A. van Herk, E. Rhein, and G.J. Nobel), and direct marketing (Alexander Singewald, Alistair Tempest). I also interviewed a leading consultant (Jeroen Terstegge) and a leading attorney (Lokke Moerel).

31. I met with two privacy advocates, including the Executive Director of the leading Dutch privacy organization Bits of Freedom (Ot van Daalen), a highly influential and experienced privacy advocate who had been involved in some of the very first code negotiations (Jan Holvast), and a significant journalist with a long-standing interest in privacy issues (Frank Kuitenbrouwer).

worked at the DPA and two who had authored formal evaluations of the Data Protection Act).[32] I studied in depth five of the twenty Dutch data protection codes of conduct (banking, pharmaceuticals, private investigators, trade information bureaus, and direct marketing). I chose these because they were among the most developed and detailed codes and because, taken together, they reflected a variety of industries. However, my research results must be viewed as a partial study of the Dutch codes, not a comprehensive one.

In preparing for the interviews, I surveyed the literature on collaborative governance and found that scholarly disagreements over this approach focused on four areas: the *process* of negotiating a code of conduct; the *substance* of the code itself; *compliance* under a code system; and the *reasons for adopting* a code-based system in the first place.[33] I used these four major topic areas to structure my interview questions, although I did not require strict adherence to the "script" when the interviewee ventured onto a different topic. The interviews were, accordingly, semi-structured.

This Article presents the results of those interviews and of my research as a whole. It proceeds as follows. Part I describes the recent congressional bills and the White Paper each of which proposes using a collaborative, safe harbor approach to regulate commercial privacy. Part II synthesizes the literature on collaborative governance. It describes both the proponents' optimistic vision of this method and the skeptics' concerns. As suggested above, it concludes that the literature raises more questions than it answers. It therefore makes sense to look not just to theory, but also to actual experience with the safe harbor approach to privacy regulation. Part III describes the Dutch safe harbor program. It sets out the program's legal foundations and describes its central components. It shows that the Dutch program resembles the American proposals and that, like them, it constitutes a form of collaborative governance. Drawing on interviews, Part IV explores whether the Dutch experience provides reason to be optimistic, or pessimistic, about using collaborative governance for privacy regulation. Part V draws 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.

---

32. I met with Professors Bert-Jaap Koops, Corien Prins, Pieter Ippel, Pieter Glasbergen, Ivo Giesen, Jan Kabel, Gerrit-Jan Zwenne, Heinrich Winter, Marguerite Overkleeft-Verburg, and with Vice-Chancellor Philip Eijlander.

33. *See infra* Part II (describing how the literature treats these four areas).

I. 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[34] and the recently-issued White Paper[35] that expresses the Obama Administration's views on the topic. While the bills and the White Paper differ from each other in some respects, they have much 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.[36] Collectively, the bills and the White Paper represent a rather remarkable and bipartisan[37] embrace of the safe harbor approach to privacy regulation by both the legislative and executive branches.[38] They suggest that the relatively untested safe harbor approach is fast becoming the dominant model for future commercial privacy law.[39] Due to their similarities, it makes sense to describe the bills and the White Paper as a unified approach and then note the differences between them.[40]

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.[41] Like the original Fair Information Practice Principles (FIPPs),[42] the bills and the White Paper begin with notice and choice.[43] Each would require regulated companies to notify individuals that they are col-

---

34. *See generally* Kerry-McCain Bill, *supra* note 9; Rush Bill, *supra* note 12; Stearns Bill, *supra* note 12.

35. *See generally* WHITE PAPER, *supra* note 10.

36. *Id.* at 23. The Administration encourages multistakeholder groups to develop codes of conduct to implement broad statutory principles. *Id.*

37. The bills have sponsors from both parties.

38. Kerry-McCain Bill, *supra* note 9; Rush Bill, *supra* note 12; Stearns Bill, *supra* note 12; WHITE PAPER, *supra* note 10.

39. Kerry-McCain Bill, *supra* note 9; Rush Bill, *supra* note 12; Stearns Bill, *supra* note 12; WHITE PAPER, *supra* note 10.

40. Kerry-McCain Bill, *supra* note 9; Rush Bill, *supra* note 12; Stearns Bill, *supra* note 12; WHITE PAPER, *supra* note 10.

41. WHITE PAPER, *supra* note 10, at 9-22 (setting forth these rights).

42. U.S. DEP'T OF HEALTH, EDU., & WELFARE, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS: RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, at XXV-XXVI (DHEW Publ'n 1973).

43. *See infra* note 44 and accompanying text.

lecting, using, and/or disclosing their personal information,[44] and to do so in a way that is "clear, concise, and timely."[45] Each would further require these entities to provide individuals with either opt-out[46] or opt-in[47] choices as to the collection, use, sale, and disclosure of their information.[48] Having stated these requirements, the bills and the 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[49] and to provide individuals with access to their personal information and the opportunity to correct it.[50] They require regulated entities that collect personal information to articulate the purpose for which they intend to use it[51] and to employ it only for that intended purpose.[52] They

---

44. Stearns Bill, *supra* note 12, § 4(a); Rush Bill, *supra* note 12, §§ 101-02; Kerry-McCain Bill, *supra* note 9, § 201; WHITE PAPER, *supra* note 10, 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 Bill, *supra* note 12, § 4(a)(2); Kerry-McCain Bill, *supra* note 9, § 201(a)(2).

45. Stearns Bill, *supra* note 12, § 4(b) ("clear and conspicuous" notice); Rush Bill, *supra* note 12, § 102(a) (notice that is "concise, meaningful, timely, prominent, and easy-to-understand"); Kerry-McCain Bill, *supra* note 9, § 201(a) (notice that is "clear, concise, and timely"). 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 information." Stearns Bill, *supra* note 12, § 5.

46. Rush Bill, *supra* note 12, § 103(a) (opt-out of collection and use of personal information); Stearns Bill, *supra* note 12, § 6(a) (opt-out of the sale or disclosure of personally identifiable information to a non-affiliate); Kerry-McCain Bill, *supra* note 9, § 202(a)(1)-(2) (opt-out of unauthorized use of personal information and opt-out of use by third parties for behavioral advertising or marketing).

47. Rush Bill, *supra* note 12, § 104(a)(1) (opt-in required for disclosure of personal information to third-party); Kerry-McCain Bill, *supra* note 9, § 202(a)(3) (opt-in required for transfer to third party for unauthorized use where such use carries risk of economic or physical harm).

48. Kerry-McCain Bill, *supra* note 9, § 202(a)(3); Stearns Bill, *supra* note 12, § 6; Rush Bill, *supra* note 12, §§ 103-04; WHITE PAPER, *supra* note 10, at 11-14 (individual control).

49. Rush Bill, *supra* note 12, § 201(a) (stating that regulated entities must establish "reasonable procedures" to ensure the accuracy of the information they collect); Kerry-McCain Bill, *supra* note 9, § 303(a) (stating that regulated entities shall attempt to establish "reasonable procedures" to ensure the accuracy of information the entity collects); WHITE PAPER, *supra* note 10, at 19-20 ("Companies should use reasonable measures to ensure they maintain accurate personal data.").

50. Rush Bill, *supra* note 12, § 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, *supra* note 9, § 202(a)(4) (requiring "reasonable access" to "any individual to whom the personally identifiable information that is covered information pertains, and which the . . . service provider stores").

51. WHITE PAPER, *supra* note 10, at 15-19; Kerry-McCain Bill, *supra* note 9, § 201(a)(1)(B); Rush Bill, *supra* note 12, § 101(3)-(4).

further require companies to retain the personal information only for so long as it takes to accomplish the intended purpose[53] and to notify and obtain consent from individuals before using the data for a purpose other than the one originally specified.[54] In sum, the bills and the 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.[55]

The bills and the White Paper also share another feature. Each states its requirements in broad, ambiguous language.[56] For example, the bills and the 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."[57] Fair enough. But how is a company to tell whether its notice is sufficiently "concise" or "meaningful" or "timely" or "easy-to-understand"?[58] The bills' and the White Paper's other main requirements are similarly open-ended. Companies are to provide the consumer with a choice mechanism that is "easy to access and to use"[59] and that offers "reasonable means to exercise

---

52. WHITE PAPER, *supra* note 10, at 15-19; Rush Bill, *supra* note 12, § 104(d) (explaining that third party recipients of information are limited to the originally specified purpose).

53. Rush Bill, *supra* note 12, § 303 (providing that a 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, *supra* note 9, § 301; *cf.* WHITE PAPER, *supra* note 10, at 21 (giving an example where a party would have to make sure that it does not retain personal data beyond the time that is needed to achieve its stated purpose).

54. WHITE PAPER, *supra* note 10, at 16 (enhanced choice required).

55. *See generally id.*; Stearns Bill, *supra* note 12; Rush Bill, *supra* note 12; Kerry-McCain Bill, *supra* note 9.

56. *See generally* Stearns Bill, *supra* note 12; Rush Bill, *supra* note 12; Kerry-McCain Bill, *supra* note 9; WHITE PAPER, *supra* note 10.

57. *See* Rush Bill, *supra* note 12, § 102(a); *see also* WHITE PAPER, *supra* note 10, at 14 (stating that notice must be "easily understandable and accessible"); Stearns Bill, *supra* note 12, § 4(b) (stating that notice "shall be provided in a clear and conspicuous manner"); Kerry-McCain Bill, *supra* note 9, § 201(a)(1) (notice that is "clear, concise, and timely").

58. Must a company provide a shorter notice to those who access its website 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 website, 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?

59. *See* Stearns Bill, *supra* note 12, § 7(2); *see also* Kerry-McCain Bill, *supra* note 9, § 202(a)(1) (requiring "clear and conspicuous mechanism for opt-out consent").

an opt-out right and decline consent for such collection and use."[60] 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.[61] Companies must institute "reasonable procedures to assure the accuracy of the covered information or sensitive information it collects, assembles, or maintains."[62] And they must provide individuals with "appropriate and reasonable" access to their personal information and mechanisms to correct it.[63] 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 Obama Administration and Congress use such open-ended language? The Administration's White Paper explains that "[i]n 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 practices that exist at the time."[64] While that makes sense, it does not answer the question of how regulated parties, faced with such broad, flexible standards, are to figure out what they need to do to comply with them, or how individuals and stakeholders are to track such compliance.[65]

---

60. Rush Bill, *supra* note 12, §103(a)(2). Is it sufficient for a company to post an opt-out notice on its website? 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. The bills create further ambiguities with respect to the "opt-in" consent requirements. For example, the Kerry-McCain Bill requires opt-in consent if a covered party changes its stated data practices in a material way and, as a result, the use or transfer of an individual's personal data would cause "risk of economic or physical harm to [the] individual." Kerry-McCain Bill, *supra* note 9, § 202(a)(3)(B)(ii). What is the threshold of economic harm? $1? $1,000? $5,000? How much of a risk of physical harm is required? Significant risk? Or will any small risk do?

61. Rush Bill, *supra* note 12, § 103(f).

62. *See id.* § 201(a); *see also* Kerry-McCain Bill, *supra* note 9, § 303(a) (requiring "reasonable procedures to ensure that personally identifiable information that is covered information and maintained by the covered entity is accurate").

63. *See* Kerry-McCain Bill, *supra* note 9, § 202(a)(4); *see also* Rush Bill, *supra* note 12, § 202(a) (requiring "reasonable access to, and the ability to dispute the accuracy or completeness of, covered information").

64. *See, e.g.*, WHITE PAPER, *supra* note 10, at 36.

65. The Department of Commerce acknowledged this point in its Green Paper. *See* GREEN PAPER, *supra* note 10, at 41 ("FIPPs are designed to be comprehensive and general . . . . [A]dopting 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.").

B. Privacy Safe Harbors

The bills and the White Paper provide two mechanisms for clarifying the broad statutory provisions. First, each would authorize the Federal Trade Commission (FTC) to promulgate rules that flesh out and interpret the statutory requirements.[66] This is traditional agency rulemaking of the type that can be found in many regulatory statutes. Second, the bills and the White Paper would authorize the safe harbor approach. That is, each would allow a nongovernmental organization—referred to as a "safe harbor program"[67] or a "multistakeholder process"[68]—to draft a set of rules that interprets the statute and spells out how it will apply to a particular sector or group of firms.[69] The bills and the White Paper then instruct the FTC[70] to evaluate the safe harbor rules to determine whether they are "substantially equivalent to or superior to the protection otherwise provided under" the statute.[71] 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.[72] 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 general statutory obligations as interpreted through default FTC rules.[73] Those firms that voluntarily committed to follow a given safe harbor program's rules,

66. Stearns Bill, *supra* note 12, § 10(b); Rush Bill, *supra* note 12, §§ 102(b), 201(a), 202(k), 301(b); Kerry-McCain Bill, *supra* note 9, §§ 101(a), 201(a), 202(a), 501(a).

67. This is the term that the Kerry-McCain Bill uses. Kerry-McCain Bill, *supra* note 9, § 501. The Stearns Bill refers to "self-regulatory programs." Stearns Bill, *supra* note 12, § 9. The Rush Bill refers to "Choice Programs." Rush Bill, *supra* note 12, § 401. The White Paper refers to "multistakeholder processes." WHITE PAPER, *supra* note 10, at 23. For the sake of simplicity, we will refer to all of these as "safe harbor programs."

68. WHITE PAPER, *supra* note 10, at 23.

69. Kerry-McCain Bill, *supra* note 9, § 501(a)(1); Stearns Bill, *supra* note 12, § 9(c)(1); Rush Bill, *supra* note 12, § 403(2)(A)-(B). The rules are sometimes referred to as a "codes of conduct." *See* WHITE PAPER, *supra* note 10, at 2.

70. Kerry-McCain Bill, *supra* note 9, § 501(b)(3); Stearns Bill, *supra* note 12, § 9(b); Rush Bill, *supra* note 12, § 402(b); WHITE PAPER, *supra* note 10, at 37.

71. *See* Kerry-McCain Bill, *supra* note 9, § 501(b)(3); *see also id.* § 502(a) (requiring that safe harbor rules must be "substantially the same as or more protective of privacy of individuals"); Stearns Bill *supra* note 12, § 9(c)(1) (requiring that self-regulatory programs must contain guidelines and procedures that are "substantially equivalent" to or "greater" than protections that statute itself sets out); Rush Bill, *supra* note 12, § 403(2)(D) (requiring that the programs 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"); WHITE PAPER, *supra* note 10, at 37 (FTC should "review codes of conduct against the Consumer Bill of Rights").

72. Kerry-McCain Bill, *supra* note 9, § 502(a); Stearns Bill, *supra* note 12, § 9(a); Rush Bill, *supra* note 12, § 401; WHITE PAPER, *supra* note 10, at 37 (giving the FTC the "authority to grant a 'safe harbor'").

73. WHITE PAPER, *supra* note 10, at 36-37.

and then failed to do so, would be subject to FTC Section 5 enforcement for engaging in an "unfair" or "deceptive" business practice[74] or, potentially, for violating the underlying terms of the Act itself.[75] Safe harbor programs would accordingly be both "voluntary" and "enforceable."

The bills and the 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.[76] The Senate bill calls them "nongovernmental organization[s]."[77] 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."[78]

The bills and the 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, and more.[79] The Rush Bill would extend the approach to notice, choice, and access, but not to data security or data minimization.[80] The Kerry-McCain Bill would narrow the safe harbor still further. It expressly extends it only to the opt-out choice that companies must provide before transferring personal data to a third party[81] and not to the bill's other substantive requirements,

---

74. The White Paper affirms the FTC's ability to use its Section 5 enforcement authority in this way. *See id.* at 29; Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2006).

75. *See* Kerry-McCain Bill, *supra* note 9, § 402 (stating that the FTC can bring enforcement actions against regulated entities that engage in "knowing or repetitive" violations of the Act); Stearns Bill, *supra* note 12, § 10 (stating that the FTC can bring enforcement actions against regulated entities that violate the Act); Rush Bill, *supra* note 12, § 602(a)-(b) (stating that the FTC can bring enforcement actions against regulated entities that violate the Act); WHITE PAPER, *supra* note 10, at 36 (arguing that Congress should authorize the FTC to enforce the Privacy Bill of Rights).

76. Rush Bill, *supra* note 12, § 401; Stearns Bill, *supra* note 12, § 9.

77. Kerry-McCain Bill, *supra* note 9, § 501.

78. WHITE PAPER, *supra* note 10, at 23.

79. Stearns Bill, *supra* note 12, § 9(a)(1).

80. Rush Bill, *supra* note 12, § 404(6).

81. Kerry-McCain Bill, *supra* note 9, § 501(a)(1)-(2).

such as notice, access, correction, and data minimization, although the text is somewhat ambiguous on this point.[82]

The bills and the 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.[83] The House bills would also require the safe harbor program itself periodically to review whether its participants were in compliance with its rules[84] and to impose consequences on them if they were not.[85] The Stearns Bill would go even further and require the program participants annually to self-certify their compliance with the program requirements.[86]

Finally, the White Paper diverges from the bills by calling for multistakeholder processes to develop codes of conduct even in the absence of privacy legislation.[87] In such a situation, the 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.[88]

These differences aside, the bills and the 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 Obama Administration Green Paper (the preliminary version of the document that later became the White Paper) provides a rationale. It explains that the technologies and business models in the information economy are evolving at an unusually rapid pace.[89] 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.[90] Moreover, the regulators themselves will not be able to learn enough

---

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

83. *See supra* notes 62-63 and accompanying text.

84. Stearns Bill, *supra* note 12, § 9(c)(2)(E).

85. Rush Bill, *supra* note 12, § 403(2)(D). The White Paper also envisions that self-regulatory bodies will provide the first line of enforcement. WHITE PAPER, *supra* note 10, at 29.

86. Stearns Bill, *supra* note 12, § 9(c)(2)(B), (C), (E).

87. WHITE PAPER, *supra* note 10, at 24.

88. *Id.* at 27.

89. GREEN PAPER, *supra* note 10, at 47.

90. *Id.* ("[T]he 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.").

about quickly evolving industries to design intelligent rules for them.[91] The Administration papers see codes of conduct as a way to address these problems.[92] 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.[93] In addition, codes will bring industry members and consumer advocates to the rule-drafting table and so will enable the regulatory process to tap into these parties' superior knowledge about evolving business, technological, and consumer realities.[94] The result should be more responsive and intelligent rules that do a better job of keeping up with rapidly changing conditions.[95]

II. 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.[96] 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.[97] Privacy safe harbor programs are a form of collabora-

---

91. *Cf. id.* at 49-50 (explaining that the government should "leverage" corporate privacy officers' superior knowledge).

92. *Id.* at 47 (showing codes that stakeholders develop will be "more responsive" than traditional rulemaking).

93. WHITE PAPER, *supra* note 10, at 27 (stating that 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 data privacy"); GREEN PAPER, *supra* note 10, at 20 ("The premise behind this approach was that industry codes would develop faster and provide more flexibility than legislation or regulations.").

94. GREEN PAPER, *supra* note 10, at 5.

95. *Id.* at 47 ("A dynamic system in which both private and public stakeholders participate would yield privacy practices that are more responsive to evolving consumer privacy expectations than would a traditional rulemaking system.").

96. *See generally* Freeman, *supra* note 18; Harter, *supra* note 21; GUNNINGHAM & SINCLAIR, *supra* note 19, at 134-56; 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).

97. Freeman, *supra* note 18, at 6, 30 (arguing that there should be shared responsibility at all stages in the rulemaking process and suggesting 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

tive 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, if properly implemented, can perform better than traditional administrative rulemaking.[98] Yet other writers are far more cautious about reaching such a conclusion.[99] The debate in the literature 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 sets out the differing views on these topics in order to assess what the literature can tell us about this regulatory approach.

A. The Case for 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 adversarial in nature.[100] Interested parties in notice-and-comment rulemaking occupy a position similar to litigants in a court proceeding. They stand at arm's length from the neutral arbiter (here, the agency) and submit written briefs (comments) that they hope will convince it to adopt their position.[101] Each group seeks to push the agency as hard as it can

---

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 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. 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 purely government-driven prescriptions.

98. *See id.* at 3-4; *see generally* Harter, *supra* note 21; REES, *supra* note 96; GUNNINGHAM & SINCLAIR, *supra* note 19; SCRUGGS, *supra* note 96.

99. *See, e.g.*, David A. Dana, *The New "Contractarian" Paradigm in Environmental Regulation*, 2000 U. ILL. L. REV. 35, 51-59 (expressing concerns about, and identifying the costs of, the shift to a "contractarian" model of regulation).

100. Freeman, *supra* note 18, at 19 (stating that traditional regulation assumes relationships are adversarial).

101. Freeman, *supra* note 18, at 11-12, 19 (citing Philip J. Harter, *Negotiating Regulations: A Cure for Malaise*, 71 GEO. L.J. 1, 19-23 (1982)).

in its own direction, believing that it must do so in order to offset its opponents' equally vigorous advocacy.[102] 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.[103] 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.[104] Thus, for example, even where companies know of a more 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 resulting in further delays and the "ossification" of the rulemaking process.[105]

As the proponents see it, collaborative processes are far less adversarial.[106] 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.[107] They thereby "[reorient] the regulatory enterprise around joint problem solving."[108] In this sense the process is 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 other's arguments and to offer positions of their own that the other parties might actually find to be convincing.[109] This deters the posturing and extreme posi-

---

102. *See* Harter, *supra* note 101, at 19-23 (explaining that both agencies and parties take extreme positions in traditional regulation).

103. Freeman, *supra* note 18, at 11-12 (stating that interest groups "often take extreme positions in notice and comment, preferring to posture in anticipation of litigation rather than focus on the regulatory problem posed by the agency"); Harter, *supra* note 101, at 19 (explaining that parties do not express their true concerns).

104. Freeman, *supra* note 18, at 15-16 (explaining that 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, *supra* note 101, at 19 (arguing parties do not want to share information that may reveal weaknesses). If 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, *supra* note 18, at 12-13. The rulemaking process itself also works against timely sharing of information. By the time that the agency has published its Notice of Proposed Rulemaking, and the public gets a chance to comment on it, the agency has already reviewed and approved the proposal and is heavily committed to it. Commenters face an uphill battle in trying to convince the agency to make major changes to the proposal. *Id.* at 12.

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

106. Freeman, *supra* note 18, at 24; Harter, *supra* note 21, at 420.

107. GUNNINGHAM & SINCLAIR, *supra* note 19, at 109 (stating that collaborative processes lead to "consensus building").

108. Freeman, *supra* note 18, at 22; *see* GUNNINGHAM & SINCLAIR, *supra* note 19, at 109.

109. Freeman, *supra* note 18, at 23.

tions that are so characteristic of adversarial rulemaking.[110] The frequent interactions can have another salutary effect. They can build an atmosphere of familiarity and trust among the participants.[111] This can make them more willing to share important information.[112] 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 needs.[113]

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.[114] 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.[115] These two factors should make collaborative methods more nimble and adaptive than traditional rulemaking processes.[116] This is particularly important in areas where technologies, business realities, and consumer expectations change rapidly.[117] In sum, the proponents claim that collaborative *processes* will generate a problem-solving

---

110. *See id.*; SCRUGGS, *supra* note 96, at 143 (explaining that when trying to build consensus, they must acknowledge some information that is contrary to their own original positions).

111. Freeman, *supra* note 18, at 24 (arguing that the process of working together itself forges trust, good faith, civility, and improved relationships); SCRUGGS, *supra* note 96, at 143 (stating that frequent interactions reduce "ill will").

112. Freeman, *supra* note 18, at 22-24; SCRUGGS, *supra* note 96, at 145; *see* GUNNINGHAM & SINCLAIR, *supra* note 19, at 97, 109; Rubinstein, *supra* note 18, at 413. *See generally* Bert-Jaap Koops, et al., *Should Self-Regulation Be the Starting Point?*, *in* STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE-LINERS 109 (Bert-Jaap Koops, et al. eds., 2006).

113. Freeman, *supra* note 18, at 7, 22-23; GUNNINGHAM & SINCLAIR, *supra* note 19, at 109 (inferring that multiple parties working together will learn from each other and so will come up with more creative solutions than any single party working alone); Harter, *supra* note 101, at 29 (stating that parties can find solutions that "accommodate fully the competing interests").

114. Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 CAP. U. L. REV. 21, 91 (2001).

115. Freeman, *supra* note 18, at 14, 22, 28. They further recommend that such initiatives build in feedback mechanisms for evaluating and reassessing the existing rules on an ongoing basis.

116. *Id.* at 9 n.19 ("There appears to be consensus that the rule-making process is excessively costly, rigid, and cumbersome."); Fiorino, *supra* note 24, at 485; IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 112-13 (1992). *See generally* Koops, et al., *supra* note 112.

117. *Cf.* Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 408 (2004) (arguing that new governance models are needed in a competitive global market where "constant change and adaptation" are key to remaining competitive); Daniel J. Fiorino, *Voluntary Initiatives, Regulation, and Nanotechnology Oversight: Charting a Path*, Woodrow Wilson International Center for Scholars Project on Emerging Nanotechnologies 7 (Nov. 2010) *available at* http://www.nanotechproject.org/process/assets/files/8347/pen-19.pdf (arguing that voluntary agreements are particularly useful in sectors that are rapidly and constantly evolving).

rather than an adversarial mentality, promote trust, information sharing, and consensus-building, and respond quickly to changing technologies and circumstances.[118]

2. *Substance*

The proponents maintain that such collaborative methods will generate better rules.[119] To 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.[120] They can then use this information to produce more tailored, workable, and cost-effective rules than those that traditional rulemaking would generate.[121] 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.[122] 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.[123]

---

118. Freeman, *supra* note 18, at 26 (arguing that collaborative methods will be more likely to produce "creative, implementable regulatory solutions capable of adaptation and revision than [will] informal notice and comment").

119. Some go the next step and argue that collaborative methods will produce better social results. SCRUGGS, *supra* note 96 at 15, 123, 146 (environmental results); REES, *supra* note 96, at 2, 224, 233 (workplace safety).

120. Harter, *supra* note 21, at 420, 422.

121. Freeman, *supra* note 18, at 22, 26-27; GUNNINGHAM & SINCLAIR, *supra* note 19, at 104; SCRUGGS, *supra* note 96, at 146, 152; Fiorino, *supra* note 24, at 485 (stating that a negotiated, sector-based approach can allow "companies to tailor rules to their own circumstances"); BENNETT & RAAB, *supra* note 26, at 156 ("Sectoral codes permit, therefore, a more refined set of rules tailored to the issues within each industry."); AYRES & BRAITHWAITE, *supra* note 116, at 116-19. Some proponents further argue that such combined efforts comport better with democratic principles than traditional rulemaking which seeks to insulate government decision-makers from direct interaction with the public. Freeman, *supra* note 18, at 22. Others maintain that collaborative agreements can serve a useful role when regulators identify a problem but do not yet know enough about it to regulate it directly. They can use collaborative processes to learn more about the nature of the issue and possible solutions to it. In this way, collaborative governance can serve a transitional role that can lead to more effective direct regulation. GUNNINGHAM & SINCLAIR, *supra* note 19, at 107.

122. *See* Freeman, *supra* note 18, at 11 n.26, 12 n.29, 19. Some 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 stricter standards than traditional regulation otherwise would. SCRUGGS, *supra* note 96, at 146-47.

123. Freeman, *supra* note 18, at 28; STEPHEN JOHNSON, ECONOMICS, EQUITY, AND THE ENVIRONMENT 236, 240 (2004); Stewart, *supra* note 114, at 82-83.

3. *Compliance*

The proponents claim that collaborative governance also improves compliance and enforcement.[124] 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.[125] 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.[126] Imposing rules from the outside tends to breed resistance.[127] Bringing regulated parties into the drafting process, by contrast, gives them a sense of ownership over the requirements[128] and tends to generate rules that they find legitimate and workable.[129] Businesses should comply more readily with such rules than with those that regulators impose on them.[130] 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 free-riders up to this standard,[131] or because they feel a sense of mutual accountability with the other parties engaged in the process and want to make good on this.[132]

4. *Reasons for Choosing a Collaborative Approach*

The move from traditional to collaborative regulation is not an easy one. As the proponents see it, governments are starting to make this change because they have a strong need for the virtues of the collaborative ap-

---

124. SCRUGGS, *supra* note 96, at 146.

125. REES, *supra* note 96, at 235 (arguing that inspectors cannot monitor every compliance point); *cf.* Freeman, *supra* note 18, at 16 (discussing EPA's difficulty in monitoring hundreds of thousands of permitted facilities).

126. Freeman, *supra* note 18, at 23.

127. Harter, *supra* note 101, at 22.

128. Freeman, *supra* note 18, at 12, 23-24.

129. GUNNINGHAM & SINCLAIR, *supra* note 19, at 109 (inferring that lower cost regulation is generally more politically acceptable); SCRUGGS, *supra* note 96, at 146 (increasing flexibility and efficiency of standards makes the rules easier to accept); Harter, *supra* note 101, at 31 (arguing that regulated parties generally believe negotiated rules are more legitimate).

130. Freeman, *supra* note 18, at 12, 23; Koops, et al., *supra* note 112, at 124; Rubinstein, *supra* note 18, at 371.

131. SCRUGGS, *supra* note 96, at 14, 143-44, 147-48, 151. 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, *supra* note 18, at 22.

132. Freeman, *supra* note 18, at 30.

proach, as just described.[133] 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.[134] 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.[135] This claim resonates strongly with the Obama Administration's rationale[136] for utilizing this alternative form of regulation.

B. Concerns about Collaborative Governance

The proponents' claims are subject to question on all four levels—process, substance, compliance, and the reasons for the recent interest in this approach.

1. *Process*

Some scholars suggest that industry may use its place at the drafting table to push for rules that serve its own interests, rather than the public interest.[137] They wonder whether regulators will be able to check this tendency sufficiently, especially in light of industry's informational superiority and political clout.[138] This can make the collaborative process seem more analogous to the proverbial "fox guarding the hen house" than to dispute resolution.

These writers express particular concern about those collaborative processes—such as the Dutch code of conduct program and, potentially, the

133. *See, e.g.*, MANDELKERN GRP. ON BETTER REGULATION, FINAL REPORT (2001) (explaining the European Union's interest in alternative regulatory methods).

134. Lobel, *supra* note 117, at 408; *See generally* JAN MAZUREK, MAKING MICROCHIPS: POLICY, GLOBALIZATION, AND ECONOMIC RESTRUCTURING IN THE SEMICONDUCTOR INDUSTRY (1999).

135. Lobel, *supra* note 117, at 408; Dennis D. Hirsch, *Lean and Green? Environmental Law and Policy and the Flexible Production Economy*, 79 IND. L.J. 611, 639-43 (2004).

136. *See supra* notes 89-95 and accompanying text.

137. *See* GUNNINGHAM & SINCLAIR, *supra* note 19, at 105 (stating that industry will push hard to "minimise its commitments"). *See generally* William Funk, *When Smoke Gets in Your Eyes: Regulatory Negotiation and the Public Interest—EPA's Woodstove Standards*, 18 ENVTL. L. 55 (1987); Harter, *supra* note 21, at 439-40 (describing those who believe that negotiated approaches will disserve the public interest).

138. Fiorino, *supra* note 24, at 485 (stating that collaborative processes "could increase the chance that the regulatory process would be co-opted by industry"); GUNNINGHAM & SINCLAIR, *supra* note 19, at 105 (discussing "asymmetry of information" between government and industry participants).

recent congressional proposals for privacy safe harbors[139]—that allow industry members alone to draft the rules and negotiate them with the regulators before bringing public interest stakeholders into the process.[140] 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.[141] Some take this argument a step further and assert that the road of collaborative governance can lead, ultimately, to "agency capture"—the scenario in which the regulators come to serve industry's interests rather those of the broader society.[142] They note that the conditions that lend themselves to industry-government 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 to agency capture.[143]

Even where backroom deals and agency capture do not emerge, there remains reason to question whether collaborative governance will, in fact, produce the new dynamics that the proponents claim. Will industry be as forthcoming as the proponents predict, or will it share information only where doing so suits its purposes? Will business, driven by the need to increase shareholder value, drop its adversarial stance and truly engage in good faith problem-solving?

---

139. While the Obama Administration policy papers expressly call for a *multi*-stakeholder 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.

140. Dana, *supra* note 99, at 52 (criticizing the bilateral nature of contractarian regulation which can limit the influence of other interested parties such as public interest groups).

141. *Cf.* Koops, et al., *supra* note 112, at 124-25 (identifying a lack of transparency and accountability); JOHNSON, *supra* note 123, at 243 (stating that regulatory contracting and similar programs have been criticized for lack of accountability and allowing back room deal making); Stewart, *supra* note 114, at 83 ("The 'closed-door' nature of the negotiations raises serious concerns about transparency and democratic accountability.").

142. GUNNINGHAM & SINCLAIR, *supra* note 19, at 105 (stating that collaborative negotiations "generate risks of a phenomenon tantamount to regulatory capture"); JOHNSON, *supra* note 123, at 243 (describing the significant opportunities for agency capture); SCRUGGS, *supra* note 96, at 128 (describing those who hold this view); REES, *supra* note 96, at 12, 236 (describing those who hold this view). Agency capture is the control or domination of administrative agencies by private parties who are subject to the regulatory authority of the agency. It occurs when a regulated entity, for example a group of corporations, replaces the public-policy agenda of the agency with its own private and self-serving agenda through lobbying or other influential methods. *See* Mark C. Niles, *On the Hijacking of Agencies (and Airplanes): The Federal Aviation Administration, "Agency Capture," and Airline Security*, 10 AM. U. J. GENDER SOC. POL'Y & L. 381, 401 (2002); Bradford C. Mank, *Superfund Contractors and Agency Capture*, 2 N.Y.U. ENVTL. L.J. 34, 35 (1993); Eric R. Pogue, *The Catastrophe Model of Risk Regulation and the Regulatory Legacy of Three Mile Island and Love Canal*, 15 PENN ST. ENVTL. L. REV. 463, 480 (2007).

143. GUNNINGHAM & SINCLAIR, *supra* note 19, at 105 (quoting AYRES & BRAITHWAITE, *supra* note 116, at 55).

These questions and others have led some commentators to express a preference for the traditional notice-and-comment rulemaking process, which requires all parties to work through formal, written channels, reduces the ability to bring pressure on regulators, and levels the playing field.[144]

2. *Substance*

The procedural flaws just described could conceivably undermine the substance of the rules that collaborative mechanisms produce. Some commentators worry that collaborative processes, stacked in industry's favor, will tend to generate overly lenient rules that place business interests over those of the public.[145] They further point out that industry representatives, who by definition come from existing firms, will have an incentive to promote rules that increase the barriers to entry and secure their own competitive position.[146] This could be particularly damaging for the fast-changing information economy that relies so heavily on innovation and entrepreneurial energy.

3. *Compliance*

Some scholars have questioned whether regulators, or the industry associations with whom they negotiate, will monitor and enforce collaborative arrangements to the degree necessary to make them effective.[147] Industry trade associations, which must look to their membership for support and funding, lack an incentive to police vigorously these very same members. In addition, collaborative governance, by encouraging regulators to establish a more cooperative relationship with industry, may make it more difficult for them to take hard-nosed enforcement positions that could damage these relationships. Industry members could perceive this decreased enthusiasm for enforcement and, acting rationally, put less effort into compliance. The result could be a decrease in compliance, not the increase that the proponents predict.

Free riding is also a concern. When a sector negotiates a collaborative agreement with the government—a code of conduct, for example—this improves the reputation of the sector as a whole. Yet participation in the col-

144. *Cf.* Dana, *supra* note 99, at 53, 57.

145. *Id.* at 52 (suggesting that the content of contractarian regulation may favor the cost-saving agenda of the regulated entities over the interests of public interest groups).

146. Koops, et al., *supra* note 112, at 124-25 (stating that the process of negotiating rules will increase the power of strongest or best-organized participating parties).

147. Stewart, *supra* note 114, at 85 (citing those who hold this view); BENNETT & RAAB, *supra* note 26, at 171 (stating that critics remain skeptical about compliance with and enforcement of industry codes of conduct); Susan Ridgley, *Environmental Protection Agreements in Japan and the United States*, 5 PAC. RIM L. & POL'Y J. 639, 642 (1996).

laborative arrangement is often voluntary. Individual firms are not required to participate; they must voluntarily commit to do so. This raises the possibility that some firms will decide not to participate and will, instead, free ride on the reputational benefits that their competitors' voluntary commitments bring to the industry as a whole.

4. *Reasons for Choosing a Collaborative Approach*

In short, some writers express concerns that the proponent's dream of collaborative governance could turn into 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.

III. DUTCH DATA PROTECTION CODES OF CONDUCT: AN EXPERIMENT IN COLLABORATIVE GOVERNANCE

Collaborative governance theory crystallizes 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 provides an excellent opportunity to do so. It represents more than twenty years of regulatory experience with the very instrument—industry codes of conduct and safe harbor agreements—that U.S. legislators and policymakers are getting ready to use to protect consumer privacy. While the Netherlands and the United States are very different countries, the Dutch experience should shed at least some light on the merits of collaborative governance in the privacy area. This Part introduces the Dutch code of conduct program. It outlines the initiative's legal and programmatic foundations and explains why the Dutch decided to use this form of regulation in the first place. It shows 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 IV draws 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 V makes 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 re-

search findings and policy recommendations, may want to skip directly to Part IV.

A. Legal Foundations

Just as the proposed U.S. privacy bills would establish a safe harbor initiative, so the Dutch Data Protection Acts authorize and establish the Dutch code of conduct program.[148] 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.[149] 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.[150] 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.[151] Like other directives at the time, this one would be a legislative act of the European Community (one of the three pillars of the European Union until it was abolished, and succeeded by the European Union, in 2009).[152] It would set

148. Personal Data Protection Act, *supra* note 26, art. 25.

149. DOUWE KORFF, DATA PROTECTION LAWS IN THE EUROPEAN UNION 13 (2005); Bert-Jaap Koops, *The Evolution of Privacy Law and Policy in the Netherlands*, 13 J. COMP. POL'Y ANALYSIS 165, 168 (2011).

150. Koops, *supra* note 149, at 168.

151. The Commission hoped that the new directive would facilitate the free flow of information within the European Union, and it hoped to ensure protection of the right to privacy that the European Convention on Human Rights had recognized as fundamental. Council Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Preamble, 1995 O.J. (L 281) 31, 31-32 [hereinafter Council Directive 95/46/EC].

152. *Pillars of the European Union*, EUROPA.EU, http://europa.eu/legislation_summaries/glossary/eu_pillars_en.htm (last visited May 23, 2013).

out broad standards and require the E.U. member nations to pass implementing statutes to incorporate these standards into national law.[153]

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 (1995 Data Protection Directive).[154] The 1995 Data Protection Directive required each member state to pass implementing legislation and to establish a DPA to administer these laws.[155] Unlike the first generation statutes, the 1995 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.[156] 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."[157] 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.[158] To implement the 1995 Data Protection Directive, European Member states passed a second generation of data protection statutes.[159] These second generation laws adopt the Directive's basic concepts and structure.[160] They focus on data processing, regulate data controllers, and seek to protect data subjects.[161]

---

153. *See Application of EU Law: What Are EU Directives?*, EUROPEAN COMMISSION, http://ec.europa.eu/eu_law/introduction/what_directive_en.htm (last updated June 25, 2012) (describing the role and function of directives); KORFF, *supra* note 149, at 2.

154. Council Directive 95/46/EC, *supra* note 151.

155. *Id.* art. 28.

156. KORFF, *supra* note 149, at 13; Hustinx, *supra* note 28, at 286 (explaining that the post-Directive Dutch data protection law "[replaced] . . . the concept of 'personal data file' [with] the 'processing of personal data'"). 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." Council Directive 95/46/EC, *supra* note 151, art. 2(b).

157. *Id.* art. 2(d); KORFF, *supra* note 149, at 13.

158. Council Directive 95/46/EC, *supra* note 151, art. 2(a).

159. Examples would include Data Protection Act, 1998, c. 29 (U.K.); Protection of Personal Data Law (B.O.E. 1999, 298) (Spain); Lei da Protecção de Dados Pessoais [Law to Protect Personal Data], Oct. 26, 1998, Diário da República at 5536, (Port.); and Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], May 22, 2001, BUNDESGESETZBLATT I [BGBL I] (Ger.).

160. KORFF, *supra* note 149, at 2.

161. *Id.* at 2, 10-12 (describing these aspects of the Directive and explaining that national laws have adopted them).

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 persoonsregistraties,[162] and the 2000 Personal Data Protection Act, or Wet bescherming persoonsgegevens.[163] This Subsection treats these two statutes separately. Later Sections refers to them collectively as the "Data Protection Act" when discussing Dutch data protection law more generally.

The 1989 Law on Personal Data Files was in many respects a typical first generation European statute.[164] As its name suggests, it sought to protect the "personal data files" contained in large, stand-alone databases.[165] To this end, it established regulatory requirements for "data users," which it defined as the parties "with control over . . . personal data file[s]."[166] It also set up a regulatory agency, the Registration Chamber (Registratiekamer), to oversee the implementation of the Act.[167]

The Law on Personal Data Files established many requirements for data users. For example, it required data users, each time they opened a new

---

162. Law on Personal Data Files, *supra* note 26.

163. Personal Data Protection Act, *supra* note 26. The Dutch first became seriously concerned with information privacy in the 1960s. The expansion of the welfare state had increased the government's need for accurate and comprehensive records about its citizens. It accordingly proposed the creation of a computerized national registry that would assign to each individual a registration number. MARGRIET G. OVERKLEEFT-VERBURG, DE WET PERSOONSREGISTRATIES: NORM, TOEPASSING EN EVALUATIE 699 (1995). This provoked protest in a country whose non-computerized registration records, only a couple of decades before, had been utilized as a tool of repression and persecution by the occupying German army. In 1971, when the government attempted to implement the first national census to make use of computer-ready forms, it met wide-spread protest and non-compliance. Koops, *supra* note 149, at 167; OVERKLEEFT-VERBURG, *supra*, at 699; A.C.M. NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC 146 n.4 (1990). The battle over information privacy was on. Partially as a result of this controversy, the Dutch, in 1983, amended their Constitution to add a general right to privacy. 1983 GW. art. 10 (Neth.); OVERKLEEFT-VERBURG, *supra*, at 699; NUGTER, *supra*, at 146 n.4 (providing unofficial translation). The provision called upon Parliament to pass legislation for the protection of personal data by 1988, the effective date of the 1983 amendments. Koops, *supra* note 149, at 168; OVERKLEEFT-VERBURG, *supra*, at 700; 1983 GW. art. 10(2)-(3) (Neth.). In 1989, the Dutch Parliament responded to this mandate by passing the Law on Personal Data Files (Wet Persoonsregistraties), the first major information privacy statute in the Netherlands. *See* Koops, *supra* note 149, at 168 (describing this history); DOUWE KORFF, DATA PROTECTION LAWS IN THE EUROPEAN UNION (2005), attached cd-rom, vol. 2, The DUTCH DATA PROTECTION LAW § 1; NUGTER, *supra*, at 147.

164. KORFF, *supra* note 163, § 1.

165. Law on Personal Data Files, *supra* note 26, art. 1; NUGTER, *supra* note 163, at 148.

166. Law on Personal Data Files, *supra* note 26, art. 1; NUGTER, *supra* note 163, at 149.

167. Law on Personal Data Files, *supra* note 26, art. 37; NUGTER, *supra* note 163, at 173.

personal data file, to "register" that file with the Registration Chamber.[168] 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.[169] 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.[170] The Law also regulated the relationship between the data user and the data subject. It required a data user to notify each data subject individually the first time that it recorded information about that person in a data file.[171] When 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;[172] to let that person correct or erase inaccurate data;[173] and to tell the data subject whether it had disclosed information about him to a third party.[174] 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.[175] 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.[176] The Personal Data Protection Act implements the 1995 European Data Protection Directive[177] and follows the second generation model. It applies to all "processing" of personal data and does not limit itself to personal data files or stand-alone databases.[178] It targets "responsible part[ies]," which it defines as the persons or organizations

168. Law on Personal Data Files, *supra* note 26, art. 24; NUGTER, *supra* note 163, at 165.

169. Law on Personal Data Files, *supra* note 26, art. 24; NUGTER, *supra* note 163, at 165.

170. Law on Personal Data Files, *supra* note 26, art. 6(1); NUGTER, *supra* note 163, at 168.

171. Law on Personal Data Files, *supra* note 26, art. 28(1); NUGTER, *supra* note 163, at 160-62.

172. Law on Personal Data Files, *supra* note 26, art. 29(1); NUGTER, *supra* note 163, at 157.

173. Law on Personal Data Files, *supra* note 26, art. 31(1); NUGTER, *supra* note 163, at 158.

174. Law on Personal Data Files, *supra* note 26, art. 32; NUGTER, *supra* note 163, at 159.

175. *See* Koops, *supra* note 149, at 174; KORFF, *supra* note 163, § 1.

176. Personal Data Protection Act, *supra* note 26.

177. KORFF, *supra* note 163, § 1 (stating that the 2000 Law replaces the 1989 Law in order to implement the 1995 Directive).

178. Personal Data Protection Act, *supra* note 26, art. 2 (establishing conditions for the lawful processing of personal data); KORFF, *supra* note 163, § 2.

that "determine[] the purpose of and means for processing personal data"[179] (a term directly analogous to the 1995 Data Protection Directive's term "controller.")[180] It seeks to protect data subjects.[181] It creates a Data Protection Authority known as the College Bescherming Persoonsgegevens (CBP).[182] From this point forward, and for the sake of simplicity, this Article refers 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.[183] 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*.[184] 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";[185] (2) the data were collected for defined purposes, and the processing is "not . . . incompatible" with these purposes;[186] (3) the data is "adequate, relevant and not excessive" in relation to the purposes for which it is being processed;[187] (4) the data is as accurate and current as it needs to be to serve the defined purpose;[188] and (5) the responsible parties retain the data no longer than is necessary for the purpose.[189] Processing operations that do not satisfy each of these principles are illegitimate and can violate the Act.[190]

---

179. Personal Data Protection Act, *supra* note 26, art. 1(d) (defining "responsible party").

180. Council Directive 95/46/EC, *supra* note 151, art. 2(d) (defining "controller" to include those who "determine[] the purposes and means of the processing of personal data").

181. KORFF, *supra* note 163, § 2.

182. The official name for the DPA is the College Bescherming Persoonsgegevens. This Article will refer to it as the Dutch DPA.

183. Personal Data Protection Act, *supra* note 26, arts. 6-11.

184. KORFF, *supra* note 163, § 4 (explaining that the 2000 Law incorporates the principles and criteria laid out in the 1995 Directive).

185. Personal Data Protection Act, *supra* note 26, art. 6; Council Directive 95/46/EC, *supra* note 151, art. 6(1)(a).

186. Personal Data Protection Act, *supra* note 26, arts. 7, 9; Council Directive 95/46/EC, *supra* note 151, art. 6(1)(b).

187. Personal Data Protection Act, *supra* note 26, art. 11(1); Council Directive 95/46/EC, *supra* note 151, art. 6(1)(c).

188. Personal Data Protection Act, *supra* note 26, art. 11(2); Council Directive 95/46/EC, *supra* note 151, art. 6(1)(d).

189. Personal Data Protection Act, *supra* note 26, art. 10; Council Directive 95/46/EC, *supra* note 151, art. 6(1)(e).

190. Personal Data Protection Act, *supra* note 26, arts. 15, 65.

In addition, processing operations must satisfy at least one of the following criteria which focus on data subject consent or exceptions to it.[191] The criteria are: (1) the data subject unambiguously consented to the processing;[192] (2) "the processing is necessary for the performance of a contract" into which the data subject entered;[193] (3) the processing is necessary to "comply with a legal obligation" "to which the [data] controller is subject";[194] (4) the "processing is necessary . . . to protect the vital interests of the data subject";[195] (5) "the processing is necessary for the proper performance of a public law duty" by the appropriate "administrative body";[196] 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.[197]

It is beyond the scope of this Article to describe more fully the provisions of the 2000 Personal Data Protection Act or of the 1989 Law on Personal Data Files. Instead, this Article focuses on two things that the 1989 and 2000 laws have in common. First, as was true with the proposed congressional bills described above,[198] 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.[199] 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 it involves marketing or an incompatible one because the first use involves the banking side of the business and the second the insurance side? The 1989

191. *Id.* art. 8; Council Directive 95/46/EC, *supra* note 151, art. 7(a).

192. Personal Data Protection Act, *supra* note 26, art. 8(a); Council Directive 95/46/EC, *supra* note 151, art. 8(2)(a).

193. Personal Data Protection Act, *supra* note 26, art. 8(b); Council Directive 95/46/EC, *supra* note 151, art. 7(b).

194. Personal Data Protection Act, *supra* note 26, art. 8(c); Council Directive 95/46/EC, *supra* note 151, art. 7(c).

195. Personal Data Protection Act, *supra* note 26, art. 8(d); Council Directive 95/46/EC, *supra* note 151, art. 7(d).

196. Personal Data Protection Act, *supra* note 26, art. 8(e); Council Directive 95/46/EC, *supra* note 151, art. 7(e).

197. Personal Data Protection Act, *supra* note 26, art. 8(f); Council Directive 95/46/EC, *supra* note 151, art. 7(f).

198. *See* text accompanying notes 56-63.

199. Law on Personal Data Files, *supra* note 26, art. 6(1); NUGTER, *supra* note 163, at 168; Personal Data Protection Act, *supra* note 26, arts. 7, 9.

and 2000 laws, with their broad language, do not define "compatible" or spell out how it applies to the banking industry. They leave points such as this one unclear and open to interpretation.[200]

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 to the purposes for which they are being processed?[201] How is it to know whether they are as accurate and current as they need to be to serve the defined purpose[202] or whether it is retaining the data for longer than is necessary for the purpose?[203] How is it to determine whether the processing is required to protect a "vital interest" of the data subject[204] or whether the data user's legitimate purposes override the data subject's "fundamental rights and freedoms"?[205] 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.[206]

The Dutch program does not rely on administrative regulations to flesh out the statute and fill these gaps. The Data Protection Act does not require, or even authorize, the DPA to promulgate legally binding regulations interpreting the statute.[207] Instead—and this is the second main thing

---

200. 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, *supra* note 26, 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.

201. Personal Data Protection Act, *supra* note 26, art. 11; Interview with Jacqueline C. Wierdak, Att'y, IP advocaten, in Amsterdam, Neth. (Apr. 13, 2010) [hereinafter Weirdak Interview] (raising this issue).

202. Personal Data Protection Act, *supra* note 26, art. 11.

203. *Id.* art. 10.

204. *Id.* art. 8(d).

205. *Id.* art. 8(f).

206. Wierdak Interview, *supra* note 201 ("That's a very vague law . . . and so companies will need to know how long they are to store this data. Two years? Five years? Seven years? Ten years? . . . [T]hose are the gaps that [the codes] are filling.").

207. As the former Chair of the DPA has put it, the DPA sees itself as a "second line institution" that supports and enforces rules that the sectors develop themselves, rather than an institution that promulgates and enforces rules from the top down. Hustinx, *supra* note 28, at 287. "What emerges is co-regulation." *Id.* Still, it should be noted that the DPA can and does conduct investigations, publish studies of industries and other background papers, and

that these statutes have in common—the Dutch laws delegate this task to the industry sectors themselves.[208] As was briefly explained above, each statute allows industry representatives to draft a "code of conduct" that specifies how the statutory requirements apply to their specific sector.[209] 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.[210] Finally, they draft a code that would provide "an interpretation of these questions"[211] and submit it to the DPA for approval.[212]

---

provide advice and guidance. In so doing, it interprets the statute. These interpretations carry some weight, though they are not legally binding on courts in the sense that duly promulgated American regulations are.

208. Personal Data Protection Act, *supra* note 26, art. 25. The 2000 Law does authorize the Ministry of Security and Justice to issue rules for a particular sector where the sector itself fails to develop a code of conduct. *Id.* art. 26. However, the Ministry has seldom used this authority. Thus, in practice, the Dutch authorities do not promulgate sector-based regulations.

209. 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. Interview with Jan Berkvens, Deputy Dir., Legal & Fin. Affairs, Rabobank Nederland, in Eindhoven, Neth. (May 11, 2010) [hereinafter Berkvens Interview]. In some instances, sectors hired "specialists" to handle the drafting. Interview with Richard Wishaw, Courthouse Rotterdam, in Rotterdam, Neth. (Apr. 23, 2010) [hereinafter Wishaw Interview]; Interview with Felix Olijslager, Dir. of the Dutch Info. Ctr. for Sec. & Law, in Amsterdam, Neth. (June 17, 2010) [hereinafter Olijslager Interview]. 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. Olijslager Interview, *supra*. Where specialists were involved, the drafting and negotiation process often went more smoothly. Interview with Peter Hustinx, European Data Prot. Supervisor, in Brussels, Belg. (May 18, 2010) [hereinafter Hustinx Interview].

210. Interview with Ulco van de Pol, Mun. Ombudsman, City of Amsterdam, in Amsterdam, Neth. (June 14, 2010) [hereinafter van de Pol Interview].

211. Berkvens Interview, *supra* note 209.

212. The Personal Data Protection Act states that "[a]n organisation or organisations planning to draw up a code of conduct may request the Data Protection Commssion [sic] 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." Personal Data Protection Act, *supra* note 26, 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, *supra* note 26, art. 15; NUGTER, *supra* note 163, at 175 (providing the unofficial translation just quoted). The phrase "reasonable requirements" appears to have referred to obligations that existed independent of the Act itself, but it is not clear whether they were based in the Constitution, other statutes, or some other authority. The 1995 Directive essentially adopted a very similar model. Article 27 of the Directive requires member states to "encourage the

The Act requires the DPA to reach a preliminary decision within thirteen weeks of submission.[213] It must publish notice of its draft decision in the official Government Gazette (Staatscourant),[214] make the draft decision available for public inspection,[215] give interested parties six weeks to comment on the draft decision,[216] and declare no later than six months after having received the initial application whether the code properly embodies the statute.[217] This declaration has the status of a final agency decision under Dutch administrative law, so it must be published in the Government Gazette,[218] and is subject to judicial review.[219]

In theory, the thirteen-week deadline for the DPA's preliminary decision and the six-month deadline for its final decision following public comment should make for a relatively speedy process. In practice, however, the situation often turns out quite differently.[220] Thirteen weeks is an unrealistically short time for the industry and regulators to negotiate all the issues that they must resolve in order to arrive at an approvable code.[221] As described by a former DPA Official, the negotiation "usually involved [at least] two to three meetings and that was just the standard . . . [a]nd it could

---

drawing up of codes of conduct intended to contribute to the proper implementation of the national [data protection laws and] . . . taking [into] account [] the specific features of the various sectors." Council Directive 95/46/EC, *supra* note 151, art. 27(1). It further instructs the national data protection authorities to review the sectoral codes to determine "whether the drafts submitted to [them] are in accordance with the national [data protection laws]." *Id.* art. 27(2). The 1989 Dutch Law on Personal Data files served as the model on which this aspect of the Directive was based. Hustinx, *supra* note 28, at 285. For a description of Article 27 of the 1995 Directive, and of the national laws that implement it, see generally Hirsch, *supra* note 8.

213. Personal Data Protection Act, *supra* note 26, art. 25(4).

214. The Personal Data Protection Act states that the DPA should follow the procedures laid down by the General Administrative Regulations Act. Personal Data Protection Act, *supra* note 26, art. 25(6). The General Administrative Law Act, in turn, requires administrative authorities to publish notice of draft decisions. Algemene Wet Bestuursrecht [Gen. Admin. Law Act] art. 3:12 (2009). Thus, the Personal Data Protection Act, by way of the General Administrative Law Act, requires the DPA to publish notice of its draft decision. The other requirements mentioned immediately after this footnote derive from the same source.

215. Algemene Wet Bestuursrecht [Gen. Admin. Law Act] art. 3:11 (2009).

216. *Id.* arts. 3:15, 3:16.

217. *Id.* art. 3:18.

218. Personal Data Protection Act, *supra* note 26, art. 25(4), (6); Law on Personal Data Files, *supra* note 26, art. 15(4); KORFF, *supra* note 163, § 8; Wierdak Interview, *supra* note 201.

219. An interested party (a citizen, a competitor) could potentially bring a legal challenge to the DPA's formal approval of a code. Wierdak Interview, *supra* note 201.

220. Wierdak Interview, *supra* note 201.

221. *See id.*

involve ten, twenty meetings during three, four years."[222] In one particularly lengthy example, it took the agency and the banking sector a full five years to reach agreement on a relevant code.[223] Due to the fact that the parties need more than thirteen weeks to negotiate and come to agreement on a code, the deadline has the unintended effect of encouraging the industry and the DPA to negotiate the code informally *before* the sector formally applies for approval.[224] This prevents the thirteen-week clock from beginning to run and so allows the DPA 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 applies for approval.[225] By the time that it does apply, the DPA and the sector have usually worked through all their differences and reached agreement on the key provisions.[226] This, in turn, reduces interested parties' ability to influence the DPA with their comments since, by the time the comment period occurs, the DPA has already been working on the proposed code for many months and is strongly committed to it.[227]

While the industry–government 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 DPA official explained it,

> the discoveries about these problems . . . and the solutions developed for them . . . were quite often a secondary benefit of the negotiations of the code[s] of conduct. It was not generated by complaints; it was not generated typically by a request for information. . . . [It was developed] in the context of codes of conduct . . . what does this mean, in that situation? Oh, I haven't thought about this. Well, come up with texts next time.[228] Through the process of negotiating the code, the [DPA] learned more about the industry it was regulating.[229]

---

222. Hustinx Interview, *supra* note 209; *see also* Wierdak Interview, *supra* note 201 (stating that as a former DPA regulator 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 that it takes a lot of time and effort from the agency as well).

223. Interview with Bruno van der Burgh, Gen. Counsel, Neth. Bankers' Assoc., in Amsterdam, Neth. (June 2, 2010) [hereinafter van der Burgh Interview]. This may have been due to the way that this particular sector, the banking 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 in a public meeting as a "fully fledged, completely developed" code. Hustinx Interview, *supra* note 209. When the DPA raised concerns about the proposal the two sides had to engage in four to five years of discussions and "endless meetings" to arrive at a meeting of the minds. *Id.* The process may have gone more quickly had the sector and the agency met first to discuss preliminary ideas before the sector put pen to paper and publicly presented a 'finished' code.

224. *See* Wierdak Interview, *supra* note 201.

225. *See id.*

226. *See id.*

227. *See id.*

228. Hustinx Interview, *supra* note 209.

229. *See id.*

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."[230] The DPA may also use the pre-submittal period to conduct on-site reviews of data practices and files and "field test" whether a draft code actually addresses the data protection issues that the sector presents.[231] Since the passage of the 1989 Law, the Dutch have approved at least twenty codes for sectors that include banking, pharmaceuticals, information bureaus, direct marketing, medical research, and others.

Once the DPA has approved a code, it considers companies that follow the code to be in compliance with the statute.[232] 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.[233] By contrast, the DPA considers firms that sign up for a code but then fail to follow it to be in violation of the statute.[234] The DPA will subject such firms to written compliance orders and, if the violation is a failure to notify, administrative fines.[235] Interestingly, while the DPA must accept a code of conduct that it 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

---

230. Berkvens Interview, *supra* note 209.

231. van de Pol Interview, *supra* note 210. One former DPA Official described the process this way: "Let's see your files. Let's see, this is the code. When we apply the code to these files, do they cover all the problems? And . . . that was an important way. Real testing. Reality based testing. And we had discussions at the same moment with private investigators." *Id.* If the regulators saw problems in the files that the code did not address, then they went back and revised the code. *Id.*

232. According to one former CBP official, when the CBP does an audit and there is an industry code of conduct in existence, "you have to take the code of conduct into your frame of reference . . . [you have to take it], 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." Wishaw Interview, *supra* note 209.

233. Hustinx Interview, *supra* note 209 ("If you follow the guidance of the code, that [provides] . . . a safe haven, that would be a safe harbor [with respect to the DPA]."); Interview with Madeleine W. McLaggan-van Roon, Comm'r, Dutch Data Prot. Auth., in The Hague, Neth. (Apr. 26, 2010) [hereinafter McLaggan-van Roon Interview]; van der Burgh Interview, *supra* note 223.

234. In such an enforcement action the DPA would assert that the firm was violating the statute, not the code. Hustinx Interview, *supra* note 209; McLaggan-van Roon Interview, *supra* note 233. 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. Berkvens Interview, *supra* note 209.

235. KORFF, *supra* note 163, § 7. The controller can challenge such an enforcement action in court.

themselves and to find a firm to be in violation of the statute, even if it is in compliance with its sectoral code.[236]

An approved code of conduct remains in place for five years.[237] After that, the code expires and the sector must seek the DPA's approval of a new code or of a new term for the existing one.[238]

B. Comparing the Dutch and the Proposed American Safe Harbor Programs

The Dutch code of conduct program, just described, shares many features with the safe harbor programs that the U.S. bills and the White Paper propose. 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;[239] and each creates a safe harbor for firms that sign up for and follow the code.[240] 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.[241] 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.[242] By contrast, the American bills do

---

236. NUGTER, *supra* note 163, at 176; *see also* Personal Data Protection Act, *supra* note 26, art. 25(1) (giving the DPA's decision the status of a "declaration" which is not binding on the courts); Korff, *supra* note 163, § 8 (stating that the DPA's decisions are a declaration not binding on the court); BENNETT & RAAB, *supra* note 26, at 142 (stating that Dutch codes are "not formally binding on the courts"). In practice, however, courts are likely to look to an approved code of conduct for guidance on how to interpret the law. Hustinx Interview, *supra* note 209 (stating that the codes in the Netherlands are not binding on the courts, but that the courts may look to them to see what good practices are in the sector); Wishaw Interview, *supra* note 209 (stating also that the codes in the Netherlands are not binding on the courts, but that the courts may look to them to see what good practices are in the sector); BENNETT & RAAB, *supra* note 26, at 142 (stating that courts treat violation of a code as prima facie evidence of liability under the law).

237. Personal Data Protection Act, *supra* note 26, art. 25(5); Law on Personal Data Files, *supra* note 26, art. 15(5).

238. Personal Data Protection Act, *supra* note 26, art. 25(1)-(2).

239. *See supra* notes 67-71 and accompanying text (describing these aspects of the proposed U.S. approach); *supra* notes 208-19 and accompanying text (describing these features of the Dutch code of conduct program).

240. *See supra* notes 72, 232-33 and accompanying text.

241. *See supra* notes 67-72, 208-31 and accompanying text.

242. Dutch law is quite clear on this point. It provides that the sector must be "sufficiently precisely defined." Personal Data Protection Act, *supra* note 26, art. 25(3); *see also* Law on Personal Data Files, *supra* note 26, art. 15. The organization representing a sector and the drafting code must be "sufficiently representative" of that sector. Personal Data Protection Act, *supra* note 26, art. 25(3); Law on Personal Data Files, *supra* note 26, § 15.

not require safe harbor programs to be sector-specific. They allow any non-governmental organization to propose a safe harbor program.[243] Second, in the Netherlands, the industry sector drafts the code and then negotiates it with the agency.[244] Public interest groups and other stakeholders do not weigh in on the document until it is proposed for public comment[245] and, even at that stage, typically do not provide much input.[246] The Obama Administration White Paper, by contrast, calls for wide-ranging, multi-stakeholder groups to draft the codes,[247] and the congressional bills, too, appear to allow for such a process.[248] This is a departure from the Dutch model where industry and government negotiate the codes.[249]

Third, Dutch industry and government negotiate their codes against the background of a comprehensive data protection statute, which the codes are supposed to interpret.[250] While the bills discussed above do propose comprehensive legislation for the United States, 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.[251] This differs from the Dutch approach. Fourth, the Dutch codes of conduct are

---

The DPA will not consider a code that fails to meet both of these threshold criteria. Personal Data Protection Act, *supra* note 26, art. 25(3); *see also* Law on Personal Data Files, *supra* note 26, § 15.

243. Kerry-McCain Bill, *supra* note 9, § 501; Stearns Bill, *supra* note 12, § 9; Rush Bill, *supra* note 12, § 401; WHITE PAPER, *supra* note 10, at 23.

244. *See supra* notes 209-12 and accompanying text.

245. Hustinx Interview, *supra* note 209 (stating that third party stakeholders were never involved in the negotiation). Originally Dutch law, too, created a role for privacy advocates. The 1989 act required industry drafters to consult with representatives of data subjects and instructed the DPA to approve a code only if "there has been sufficient consultation with organizations of interested persons, including data subjects." Law on Personal Data Files, *supra* note 26, § 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. Hustinx Interview, *supra* note 209. This made the consultation requirement unworkable. *Id.* The 2000 Law accordingly dropped this requirement. The upshot is that, today, the industry sector drafts the code and negotiates it with the DPA.

246. Hustinx Interview, *supra* note 209 (stating that CBP has typically received very few comments); Wierdak Interview, *supra* note 201 (stating that CBP has typically received very few comments).

247. WHITE PAPER, *supra* note 10, at 23.

248. The Congressional bills say that "nongovernmental organizations" and "self-regulatory organizations" will draft and sponsor the safe harbor programs. Kerry-McCain Bill, *supra* note 9, § 501; Stearns Bill, *supra* note 12, § 9; Rush Bill, *supra* note 12, § 401. 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.

249. *See supra* notes 209-10 and accompanying text.

250. Personal Data Protection Act, *supra* note 26, art. 26(1).

251. *See* WHITE PAPER, *supra* note 10, at 24.

themselves comprehensive. They implement, and create a safe harbor with respect to, all statutory requirements.[252] 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.[253] Finally, the Dutch have been negotiating and approving codes since 1989, while the American proposals have yet to be implemented.[254] 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. This Article turns now to that assessment.

IV. 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 of my research results follows this same structure. 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.[255]

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 deal of time

252. Personal Data Protection Act, *supra* note 26, art. 25(1).

253. *See supra* notes 79-82 and accompanying text.

254. Law on Personal Data Files, *supra* note 26.

255. *Id.*; Hustinx Interview, *supra* note 209. For example, see the early Swedish data protection law.

and resources to develop sector-specific rules[256] and that this would be beyond the means of the small agency (the Registration Chamber).[257] It accordingly sought to achieve a "division of labor"[258] 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.[259] 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."[260] Second, the Reagan Administration's emphasis on deregulation during the 1980s had an "echo" in Europe at the time that the Ministry was drafting the 1989 Law on Personal Data Files.[261] 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.[262] Third, the Ministry believed that sectors could draft and update codes of conduct more quickly than government officials could draft and update rules.[263] Codes would therefore do a better job of keeping up with the fast-changing information economy.[264] This reason for utilizing codes of conduct corresponds to that which the Obama Administration, and some proponents of collaborative approaches, have articulated.[265]

Finally, history and culture appear to have played a role. 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.[266] In the Netherlands, significant amounts of land lie below sea level. Such land is currently habitable because, over the generations, the inhabitants have built

---

256. Hustinx Interview, *supra* note 209.

257. Wishaw Interview, *supra* note 209 (stating that while the DPA could also have fleshed out the statute, "it takes a lot of energy to do that . . . [w]ith a small [DPA] of 70 people, you cannot do that").

258. Hustinx Interview, *supra* note 209.

259. *Id.*

260. *Id.*

261. *Id.*

262. *Id.*

263. Interview with Jeroen Terstegge, PrivaSense [hereinafter Terstegge Interview] (stating that government regulation cannot keep up with the pace of technological change).

264. Wishaw Interview, *supra* note 209 (explaining that "[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").

265. *See supra* notes 89-95 and accompanying text.

266. van de Pol Interview, *supra* note 210; Hustinx Interview, *supra* note 209; van der Burgh Interview, *supra* note 223.

a system of dikes and pumps to push the sea back and reclaim the land.[267] 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.[268] As a result, negotiation and consensus-building became an integral part of Dutch daily life and culture.[269]

Scholars believe the cooperative, Dutch approach to regulation owes much to this tradition.[270] 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.[271] 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.[272]

These cultural factors appear to be at work in the Dutch approach to data protection regulation. 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:

> I think in Holland it's a very well accepted concept, in various areas not only in data protection . . . . Our polder model . . . is that at meetings you try to get agreement with all the organizations involved, [it is a] consensus-oriented approach. That's a very high standard in Holland . . . . For Holland it is a normal way of thinking tied to each agreement . . . . It's in our culture.[273]

A representative of the banking sector echoed this sentiment, explaining that "Holland is a [small] country that works with consensus. . . . It is what you call the famous 'polder model.' . . . [T]he same goes for this type of problem. We always try to find solutions for things, which are acceptable for

---

267. RUDY B. ANDEWEG & GALEN A. IRWIN, DUTCH GOVERNMENT AND POLITICS 5-7 (1993).

268. *See* CORINA HENDRIKS, THE STORY BEHIND THE DUTCH MODEL: CONSENSUAL POLITICS OF WAGE RESTRAINT 94 (2010).

269. *See id.*

270. *See id.* (stating consensus seeking is part of Dutch national history and culture and influences regulatory style in the Netherlands).

271. *See id.* at 94.

272. 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 environmental goals. *See, e.g.*, Yda Schreuder, *The Polder Model in Dutch Economic and Environmental Planning*, 21 BULL. SCI. TECH. & SOC. 237 (2001).

273. van de Pol Interview, *supra* note 210. 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. Maybe that is also why it made more sense from the point of view of say division of labor. But it is also part of the culture which is very much of [seeking] consensus. Working it out together is . . . a characteristic of Dutch culture." Hustinx Interview, *supra* note 209.

everyone. That's the way we . . . work."[274] This link between codes of conduct, Dutch history, and culture raises questions about whether the model is transferable to the United States. The concluding Part of this Article will return to this question.[275]

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.[276] Industry representatives explained two main reasons for investing in the development and implementation of codes of conduct. First, Dutch industry saw codes of conduct as a valuable mechanism through which to clarify the broad terms of the Data Protection Act.[277] As was explained above, the Data Protection Act speaks in spacious, ambiguous terms.[278] Yet it does not authorize the DPA to promulgate regulations fleshing out these provisions and, in any event, the DPA does not have the staff or resources to do so.[279] Companies accordingly found themselves facing a new, broadly-worded set of legal obligations with few instructions on how to comply.[280] One industry lawyer compared the situation to "feeling our way in the dark."[281] This was an untenable situation for larger, more visible sectors that utilized a great deal of personal information.[282] These sectors put resources into codes so as to gain clearer guidance on what the statutes required of them.[283] In its 2010 Green Paper, the Obama

274. van der Burgh Interview, *supra* note 223.

275. *See infra* p. 161.

276. *See* GREEN PAPER, *supra* note 10, at 51. The Department of Commerce recognized the importance of this question. In its 2010 Green Paper, in which it proposed that the United States 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. *Id.*

277. Berkvens Interview, *supra* note 209.

278. *See supra* notes 198-206 and accompanying text.

279. Hustinx Interview, *supra* note 209. The DPA 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 DPA's views on those topics. Wishaw Interview, *supra* note 209.

280. Wierdak Interview, *supra* note 201.

281. *Id.*

282. *See id.*

283. 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 and its application in certain banking situations." Berkvens Interview, *supra* note 209. 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. *Id.* ("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. So it's clarification on voice

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.[284] 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 certainty.

Some industry representatives expressed a second reason to invest in codes of conduct: to forestall more direct government regulation. The representatives of the trade information bureaus explained that public sentiment was building for legislation to regulate the industry's use of personal information.[285] The industry saw the development of a code of conduct as an opportunity to give a positive signal to the government that legislation was not needed, and thereby "get ahead of" and prevent direct regulation that might turn out to be considerably more strict.[286] A representative of the direct marketing industry told a similar story about his sector's decision to engage in self-regulation.[287]

B. The Process of Producing Codes of Conduct

As described above, scholars disagree as to whether collaborative governance constitutes an effective process for producing rules.[288] The Dutch experience provides some support for each viewpoint.

---

logging and on the processing of video pictures. The Act says nothing, and the Code says what we do in [these areas]. . . . [W]e wanted to clarify how to deal with cameras, and . . . how [to] inform the public of the usage of these cameras."). The code helps to clarify this. *Id.* ("[T]he Act says nothing about direct marketing. The code is more explicit about what kind of use of customer data is permitted in groups of banks, and for what purposes. . . . [The Act] says that we can process data to be in compliance with the other legislation. The code gives [a] listing of such laws.").

284. *See* GREEN PAPER, *supra* note 10, at 30, 51.

285. Interview with A. van Herk (Chair), E. Rhein (Secretary) & J. Nobel (Treasurer), Dutch Assoc. of Trade Info. Bureaus (Nederlandse Vereniging van Handelsinformatiebureaus), in The Hague, Neth. (June, 2010) [hereinafter NVH Interview].

286. *Id.*

287. *See* Interview with Alexander J.J.T. Singewald, Singewald Consultants Grp., in Aalsmeer, Neth. (June 11, 2010) [hereinafter Singewald Interview] (facing the threat of legislation that would have created an "opt-in" system for direct mail advertising, the industry developed an extensive self-regulatory "opt-out" system that has proven to be highly effective). This suggests that some in industry believed codes of conduct to be valuable not only as a means to clarify and interpret the existing Data Protection Act, but also as a way to pre-empt and forestall more targeted legislation directed at their particular industry. *See* Hustinx, *supra* note 28, at 285 (discussing that self-regulation may be "advanced as a means of preventing or postponing legislation").

288. *See supra* Part II (setting out this argument and citing sources).

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.[289] They did this even though they knew that this inspection would likely reveal some violations of the Act.[290] He explained that the code negotiation process created the trust that made this possible:

> It [was] not our aim [to]. . . detect[] illegal acts whatsoever. We just want[ed] to see whether the code [was] working. . . . [They allowed us to do this because] [w]e trust[ed] each other. Personal trust. That was the basis. . . . During the process we were really listening to them. We want[ed] to solve the problems which they [had] with data protection law. 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 they operate, [then they trust you.][291]

Business representatives explained that, for their part, they shared information so as to correct regulators' misconceptions about their industry's data practices.[292]

While these interviews painted an optimistic picture, others suggested that the 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 American credit rating agencies) unearthed valuable information that the code negotiation had not revealed.[293] 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 the 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.[294]

---

289. van de Pol Interview, *supra* note 210.

290. *Id.*

291. *Id.*

292. *See* Singewald Interview, *supra* note 287 ("They also think we are doing all kinds of things we really don't do."); van der Burgh Interview, *supra* note 223 (describing how the sector decided to develop a code so as to provide "information for the Supervisor").

293. *See* Wishaw Interview, *supra* note 209.

294. *Id.* The regulators found it particularly useful to be able to review company transactions related to personal data. *Id.* This revealed that professionals such as lawyers and

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 direction. Government officials, too, can share valuable information.[295] 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.[296] 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.[297] The parties memorialized this interpretation in the Financial Institutions Code.[298] One of the negotiators of the banking code explained the value of such clarifications:

> Every Supervisor has his own policy. You have the legislation, but between the lines they have their own policy. . . . So you have to know very well what . . . the policy is, and 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.[299]

The lead negotiator for the private investigator industry provided several other examples of how code negotiation served as a vehicle for clarifying the statute.[300] He, too, identified that as the added value of the code.[301]

---

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. *See id.* The bureaus were like "spiders at the center of a web" of information transactions, and the investigation allowed the regulators to see the Web. *Id.*

295. *Cf.* Peter Hustinx, *The Use and Impact of Codes of Conduct in the Netherlands*, Paper Presented to the 16th Conference of Data Protection Commissioners, The Hague, Neth. (1994) (stating that codes of conduct can lead to an "enhanced measure of understanding on both sides"); BENNETT & RAAB, *supra* note 26, at 141 (stating that negotiating codes can enhance the understanding of privacy problems between parties).

296. van der Burgh Interview, *supra* note 223.

297. *Id.*

298. CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA BY FINANCIAL INSTITUTIONS § 5.2.2 (2003) [hereinafter PROCESSING OF PERS. DATA BY FIN. INSTS.]; *Id.* § 2.5; van der Burgh Interview, *supra* note 223.

299. van der Burgh interview, *supra* note 223.

300. For example, the Code stated that private investigators should refrain from observing people "in circumstances where these persons . . . should not suffer any restrictions on their ability to be free of restraints." PRIVACYGEDRAGSCODE SECTOR PARTICULIERE ONDERZOEKSBUREAUS [PRIVACY CODE OF CONDUCT FOR THE PRIVATE INVESTIGATION INDUSTRY] § 7.4(3) (2004) [hereinafter PRIVACY CODE OF CONDUCT FOR THE PRIVATE INVESTIGATION INDUSTRY]. It then clarified that these circumstances include "private residences, hotel rooms, bathing cubicles at swimming pools, changing rooms in stores, rest

The industry is able to clarify what is in-bounds and what is out-of-bounds in a way that is useful to the industry and that the agency approves.[302]

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 DPA was able to identify a host of issues that the industry had not yet considered:

> Is this identifiable or isn't this? 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.[303]

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 predict that it will produce a problem-solving, rather than an adversarial, mentality.[304] The interviews offered a number of 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

---

areas and toilets, [but that] . . . observing an individual in a private residence for a few moments from the public highway whilst the windows are exposed does not fall under the restrictions of this rule." *Id.* § 7.4. In another instance, the code made clear that "[o]bservation may be supported using technical" resources (such as cameras) or positioning "equipment (e.g. GPS equipment when shadowing vehicles)." *Id.* However, it then qualified this statement by setting limits on the use of GPS devices so as to protect individual privacy:

> Usage of other technical auxiliary devices, such as a Global Position System (GPS) beacon, is only permissible under restricted circumstances. . . . Deployment of these means shall be limited to company vehicles and private vehicles used for professional purposes by the person under investigation and shall further be limited to those times that are relevant to the investigation contract. Affixing a technical auxiliary device onto an individual's private property such that at all times an exact and complete picture is obtained of the places where the person under observation is or has been inflicts too great a breach of privacy and cannot find its justification in the nature of the contract.

Id. See generally Olijslager Interview, *supra* note 209 (describing these features of the Code).

301. Olijslager Interview, *supra* note 209.

302. *Id.*

303. Hustinx Interview, *supra* note 209.

304. Freeman, *supra* note 18, at 22; GUNNINGHAM & SINCLAIR, *supra* note 19, at 109; *see also* Harter, *supra* note 21, at 420.

those who may be interested in certain banking products.[305] 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] obtained."[306] 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.[307]

According to a representative for the banks, the turning point came when each party expressed its bottom-line need.[308] For the regulators, the most important thing was that the banks not use data on individual customers to create profiles of *those individuals*.[309] 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.[310] They readily agreed to create only aggregate profiles, not individual ones.[311]

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 "[p]rocessing . . . for statistical . . . purposes."[312] 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] provision[s] to ensure that the further processing of personal data [shall be effected] for these specific purposes."[313] The pharmaceutical sector and the DPA reached a very similar solution regarding that industry's desire to use the personal data of those participating in clinical trials to construct profiles of the types of people who might best be able to benefit from new drugs.[314]

Articulation of bottom line interests in a way that allows these interests to be reconciled is classic problem solving. A representative of the direct marketing sector, having himself negotiated such a solution with the DPA,[315] summed up the dynamic in this way:

---

305. Berkvens Interview, *supra* note 209.

306. Personal Data Protection Act, *supra* note 26, art. 9.

307. Berkvens Interview, *supra* note 209.

308. *Id.*

309. *Id.*

310. *Id.*

311. *Id.*

312. CODE PROCESSING PERSONAL FINANCIAL INSTITUTIONS § 5.3.2 (2010).

313. *Id.* § 5.3.1. To make matters perfectly clear, Section 5.3.3 says that "[i]n order to target marketing activities at certain groups, personal data may be analysed that have been collected within the framework of marketing activities."

314. Interview with Matthijs van Blokland, Senior Policy Adviser on Legal Affairs, Nefarma, in Amsterdam, Neth. (June 15, 2010) [hereinafter van Blokland Interview].

315. According to the representative for the direct marketing industry, the initial disagreement concerned whether the industry should be prohibited from having any com-

> 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.[316]

3. *Agency Capture and Industry Influence*

The interviews did not suggest full-scale agency capture. The DPA appeared to have well-defined institutional values that were independent of and different from industry interests.[317] Both government officials and industry representatives told of contested, protracted negotiations,[318] and industry representatives complained about regulators being too "technical" and "legalistic."[319] 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.[320] 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 private investigator industry's compliance with the statutory requirement that companies notify a data subject when collecting personal infor-

---

mercial communications with children at all or whether it should be allowed to do so with parental consent. Singewald Interview, *supra* note 287. 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. *Id.* The industry agreed not to do this, and this became part of the code. *Id.*; FEDMA Code, § 2.6.4. "Once we learned what their real opinion was, we were able to address it." Singewald Interview, *supra* note 287.

316. Olijslager Interview, *supra* note 209.

317. For example, a former DPA official explained that the DPA's "reputation was at stake" in the codes that it negotiated. Hustinx Interview, *supra* note 209. "[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." *Id.* This sense of an agency reputation, and the need to protect and build it, suggests an independent set of values. *Id.* ("This is an independent government agency whose task it is to insist on adequate safeguards.").

318. *Id.* (describing the difficult five-year process for negotiating the Financial Institutions Code); van de Pol Interview, *supra* note 210 (describing the "heavy discussions" between the DPA and the direct marketing industry over that sector's code).

319. NVH Interview, *supra* note 285 (stating that government officials do not understand the industry, take a "formal approach based on laws," and are not open to industry input).

320. *See* Scruggs, *supra* note 96, at 147 (stating that corporatist tradition that brings in extensive sets of interest groups leads to reduced risk of agency capture); Niles, *supra* note 142, at 399 (stating that threat of agency capture is greater where the agency regulates only a single industry).

mation about that person.[321] Private investigators complained that this requirement was particularly burdensome when an employer hired them to investigate an employee, and the person later turned out to be innocent.[322] In these circumstances, the employer often insisted that the employee not be told of the investigation for fear of damaging the employment relationship.[323] The private investigators pushed to be let out of the requirement in these instances.[324] While the DPA did not grant this wish in its entirety, it did make a significant concession. The DPA agreed that it would be acceptable for the employer that had hired the private investigator to assume the obligation to notify the employee in question and that, where the employer provided proof to the investigator that it had given such notification, the private investigator itself would not be required to do so.[325] This problematic solution put the burden of notifying the innocent employee in the hands of the one party that did not want that notification to occur—the employer.[326] While it purportedly required the employer to document the notification, it did not compel anyone to check the accuracy of this documentation.[327] This created a significant risk of non-compliance. Indeed, a later study of the private investigator industry found widespread violation of the notification requirement[328] and explained that most violations occurred where an employee was found to be innocent because, in those cases, the employer did not want to damage its relationship with the employee.[329]

The private investigator story is indeed 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).[330] In the Netherlands, trade information bureaus, such as Experian, use their large

---

321. Personal Data Protection Act, *supra* note 26, arts. 33-34.

322. Wishaw Interview, *supra* note 209.

323. *See id.*

324. Olijslager Interview, *supra* note 209.

325. *Id.*; Wishaw Interview, *supra* note 209; Interview with Carlo Cahn, Sec.-Gen. of the Dutch Private Investigators Assoc. (de Nederlandse Veiligheidsbranche), in Amsterdam, Neth. (July 2, 2010) [hereinafter Cahn Interview].

326. 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[s] was an illusion in terms of informing them of the investigation. But we did not push it. They were proposing texts. We said okay. I always knew that it was a very weak point." van de Pol Interview, *supra* note 210.

327. Wishaw Interview, *supra* note 209.

328. *See* Regioplan Policy Research, *Evaluation of the Privacy Code of Conduct for Private Detective Agencies*, 85, 89-90 (Oct. 2007).

329. *See id.* at 88.

330. *See* Nederlandse Vereniging van Handelsinformatiebureaus, http://www.nvhinfo.nl/htm/nvh_home.htm?30 (last visited July 14, 2013).

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 or employer, about a given individual's whereabouts, financial situation, or employment status.[331] The DPA took the position that the industry had to obtain the individual's consent before doing so—a position that the industry believed would undermine its debt collection-related service.[332] In the face of strenuous industry argument, the DPA remained committed to its position.[333] Negotiations over the renewal of the trade information bureau code broke down over this issue, and the code expired.[334] 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. As will be discussed further below, the code negotiation process should be designed to minimize this possibility by, for example, including public interest stakeholders in the discussion.[335]

4. *Adaptability*

The proponents of collaborative governance and the Obama Administration claim that this method is more nimble and adaptive than traditional notice-and-comment rulemaking[336] and that this quality is particularly important for regulation of the information economy.[337] Dutch policymakers also articulated this idea when explaining why they opted for codes of conduct over traditional rules.[338]

The Dutch codes of conduct tell a very different story.[339] Government and industry representatives reported that while some negotiations could proceed smoothly and be wrapped up after two or three meetings,[340] they

331. NVH Interview, *supra* note 285.

332. *Id.*

333. *Id.*

334. *Id.*

335. *See infra* Subsection V.A.2 (suggesting this).

336. *See supra* notes 89-95 and accompanying text.

337. *See* GREEN PAPER, *supra* note 10, at 19-20; *cf.* BENNETT & RAAB, *supra* note 26, at 141 (explaining the view that codes are "flexible instruments and once negotiated can be adapted to changing economic and technological developments").

338. *See supra* Subsection IV.A.1.

339. Some interviewees did describe codes as an adaptive form of regulation. Singewald Interview, *supra* note 287; Wierdak Interview, *supra* note 201; van Blokland Interview, *supra* note 314. However, these statements were at odds with the facts that they and others described regarding the amount of time it took to negotiate codes and the static nature of these documents once adopted, as described below.

340. 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

were just as likely to require ten or even twenty meetings and from three to four years of work.[341] A former regulator explained 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.[342] 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."[343]

The Dutch experience is also at odds with the proponents' and the 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.[344] To the contrary, a majority of the codes expired after their initial five years had ended, and in some cases, it took years for the industry and government to agree on a new version.[345] During this period, the expired code lost its legal status and the industry, its safe harbor.[346] 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 loath to re-

---

since this gave the parties a legal foundation from which to work and the codes in which the industry hired an information privacy specialist to represent it during the code negotiation process. Hustinx Interview, *supra* note 209.

341. *Id.* The Financial Institutions Code was one of these. It took five years to reach agreement. van der Burgh Interview, *supra* note 223; Hustinx Interview, *supra* note 209. These time frames conflict with the Dutch Personal Data Protection Act, which requires the DPA to reach a decision within thirteen weeks of an industry's submission of the draft code. Personal Data Protection Act, *supra* note 26, art. 25(4). As was explained above, this disparity is due to the fact that most of the negotiations occur before the sector formally submits the draft code to the DPA. *See supra* notes 224-27 and accompanying text. The time frames discussed here reflect the actual length of time that the sector and regulators worked on the code, not the formal thirteen-week period that the statute describes.

342. Wierdak Interview, *supra* note 201; *see also* Hustinx Interview, *supra* note 209 (describing "extensive meetings, sometimes negotiations, sometimes about texts, article by article. Some were very . . . frustrating for both sides").

343. MINISTRY OF JUSTICE, FIRST EVALUATION OF THE PERSONAL DATA PROTECTION ACT, Summary at 3 (2007).

344. Email from Richard Wishaw, former official, Dutch DPA (June 13, 2013, 11:25 EST) (on file with author); Email from Jacqueline Wierdak, former official, Dutch DPA (June 14, 2013, 4:08 EST).

345. *See* Appendix: Dutch Data Protection Codes of Conduct (identifying the codes that expired); Wierdak Interview, *supra* note 201; van der Burgh Interview, *supra* note 223 (describing how the Financial Institutions Code lapsed for two years while negotiations over the revised code dragged on and concluded that "[i]t takes quite a lot of time to look into texts").

346. Wierdak Interview, *supra* note 201.

open the discussion until they are absolutely forced to do so.[347] 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 expire before negotiating a new code with the DPA.[348] 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.[349] 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 that require only industry and the 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.

C. The Substance of the Codes of Conduct

As discussed above, commentators 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.[350] The proponents argue that collaborative methods will tend to produce rules that are more tailored to business realities, and more cost-effective, workable, creative, and up-to-date than those that notice-and-comment rulemaking generally yields.[351] Others, however, maintain that collaborative processes will generate rules that are lenient and anti-competitive.[352]

1. *Tailoring and Workability*

The Dutch codes offer quite a few instances in which the negotiation process led to more tailored and workable rules. One such example concerns the private investigator industry. The Data Protection Act requires companies to notify data subjects *before* they collect personal information

---

347. *See* BENNETT & RAAB, *supra* note 26, at 142 (stating that government approval of codes "can bureaucratize a process that, in theory, is supposed to allow the flexibility of self-regulation").

348. *See* Appendix: Dutch Data Protection Codes of Conduct (identifying the codes that expired).

349. *See supra* notes 89-95 and accompanying text.

350. *See supra* Part II.

351. *See supra* Section II.A.

352. *See supra* Section II.B.

about them.[353] Obviously, such a requirement runs directly counter to the private investigators' business model, which is premised on collecting information about individuals without their knowledge. After negotiation, the industry and the DPA agreed that investigators could notify the data subject *after* the investigation, rather than before, and memorialized this arrangement in the code.[354] Assuming that investigators do provide such notice,[355] this should enable the notification requirement to serve its intended purpose—i.e., allowing 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 not transmit financial data without the data subject's prior consent.[356] 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.[357] 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.[358] The banks protested that this was unworkable since few such payees would give their consent.[359] After some negotiations, the parties worked out a solution.[360] The Code states that banks can share personal data for the "normal settlement of payment transactions" and for "verification and reconstruction purposes."[361] 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 educate the data protection authority about the specific features of the industry and how they

353. Personal Data Protection Act, *supra* note 26, arts. 33-34.

354. PRIVACY CODE OF CONDUCT FOR THE PRIVATE INVESTIGATION INDUSTRY, *supra* note 300, § 8.1; Interview with Pieter Ijfs, Dir., De Fraude Experts, in Amsterdam, Neth. (June 7, 2010) [hereinafter Ijfs Interview]; Wishaw Interview, *supra* note 209.

355. Above, I described some situations in which the investigators have not provided such notice at the conclusion of the investigation. *See supra* notes 321-29 and accompanying text. This is a separate, albeit highly important, issue.

356. van der Burgh Interview, *supra* note 223.

357. *Id.*

358. *Id.*

359. *Id.*

360. *Id.*

361. PROCESSING OF PERS. DATA BY FIN. INSTS., *supra* note 298, § 5.2.3.

relate to the data protection law. Regulators would not otherwise know enough about the industry to regulate it intelligently."[362]

2. *Cost-Effectiveness*

Government-industry negotiations can also lead to more cost-effective rules. For example, the Data Protection Act requires that a company notify the DPA each time it begins to process personal data.[363] 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.[364] The financial industry believed that this would "cause an enormous burden of red tape."[365] It accordingly sought permission to streamline the notification requirement in two ways. First, it asked that each bank be allowed 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.[366] Second Rabobank, a large cooperative bank, requested that it be able to make a single notification on behalf of its hundreds of member banks, rather than requiring each member bank itself notify the DPA.[367] The banking representatives argued that, in addition to reducing compliance costs, these reforms would give regulators a more comprehensive picture of the banks' information processing than would multiple piecemeal notifications, and so would improve regulators' understanding of how a given bank handled personal data.[368] Ultimately, the DPA accepted this interpretation of the statute.[369] This reduced the banks' compliance costs considerably.[370]

---

362. van der Burgh Interview, *supra* note 223. A representative for the direct-marketing industry expressed a similar sentiment, in slightly more evocative language: "You know the 'Streets of San Francisco,' the police series? . . . There was a guy who always ended the briefing: 'let's do it to them before they do it to us.' . . . [T]hat's my motto, let's do it to ourselves [through a code] before they do it to us." Singewald Interview, *supra* note 287. This is better because then you get to "workable solutions." *Id.*

363. Personal Data Protection Act, *supra* note 26, art. 27; Berkvens Interview, *supra* note 209.

364. Berkvens Interview, *supra* note 209.

365. *Id.*

366. *Id.*

367. *Id.* Rabobank, a large cooperative bank in the Netherlands, had one central bank and more than 1,000 member banks. *Id.* The central office requested permission to file a single notification on behalf of all of these member banks. *Id.*

368. *Id.*

369. *Id.* The DPA's permission to Rabobank to make a single notification on behalf of its members took the form of a letter to the bank that served as a supplement to the financial institutions code. Email from Jan Berkvens, Deputy Dir., Legal & Fin. Affairs, Rabobank Nederland, to Dennis Hirsch, Professor of Law, Capital University Law School (Mar. 4, 2013, 10:24 EST) (on file with author).

370. Berkvens Interview, *supra* note 209.

3. *Leniency*

Some have argued that that industry domination of the negotiation process will result in overly lenient rules. As already described, in one instance, the private investigator industry pushed for, and achieved, a lenient interpretation of the Act.[371] That said, it would be unwise to draw sweeping conclusions from this one example. As was also described 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.[372] 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 Official, who personally negotiated several of the codes of conduct, said the following about the agency's position during 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 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 isn't able to take the initiative. . . . It's up to the company or organizations 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.[373]

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.

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.[374] The DPA initially found this to be perplexing but did not object.[375] Later, a party commenting on the draft

371. *See supra* notes 321-29 and accompanying text.
372. *See supra* notes 330-34 and accompanying text.
373. van de Pol Interview, *supra* note 210.
374. McLaggan-van Roon Interview, *supra* note 233.
375. *Id.*

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.[376] 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.[377] At the time, however, the DPA did not require the industry to change the code.[378] 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

Collaborative governance scholars also disagree on its impact on compliance. As was explained in more detail above,[379] 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, along with industry self-policing.[380] Others counter that collaborative approaches will encourage regulators to adopt a cooperative rather than an enforcement-oriented mindset and that most sectors will not have the will to enforce rules against their own members.[381]

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.[382] 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.[383] It promised to "change course" and put greater priority on inspections and enforcement.[384]

It remains to be seen whether the DPA's new effort will make a difference. One former DPA official predicted that it would not, for reasons that echo the proponents' concerns about the efficacy of government en-

376. *Id.*
377. *Id.*
378. *Id.*
379. *See supra* notes 124-32, 147 and accompanying text.
380. *See supra* Subsection II.A.3 and accompanying text.
381. *See supra* Subsection II.B.3 and accompanying text.
382. *See supra* note 125 and accompanying text.
383. *See* Jacob Kohnstamm, *Preface to the* DATA PROT. AUTH.'S 2007 ANNUAL REPORT, at 69 (2007).
384. *Id.* at 69-70.

forcement.[385] He maintained that the DPA, which he said 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.[386] "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's relatively small actions. . . . In most cases, it is reactive."[387] This suggests that the DPA may lack the resources comprehensively to monitor data practices across the economy.[388] This, coupled with the fact that the DPA lacks authority to issue significant fines for violations of the Act,[389] suggests that traditional agency enforcement may not be enough to ensure compliance with the Act.

2. *Building Awareness*

Can the codes of conduct help to promote compliance? Business representatives and 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.[390] 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.[391]

As a result, "everybody, the back offices, front offices, the lawyers, they all learned a lot about their [own] processes in relation to the data protection issue."[392] A DPA official confirmed that the code drafting and negotiation

385. van de Pol Interview, *supra* note 210.

386. *Id.*

387. *Id.*

388. *See* Cahn Interview, *supra* note 325 (stating that it is impossible for authorities fully to monitor compliance).

389. Personal Data Protection Act, *supra* note 26, art. 66.

390. *Cf.* BENNETT & RAAB, *supra* note 26, at 141 ("The procedure of negotiating codes may enhance the understanding of the privacy problem within different sectors.").

391. Berkvens Interview, *supra* note 209.

392. *Id.* The DPA Commissioner in charge of negotiating the private investigator code suggested that a similar evolution had occurred there. van de Pol Interview, *supra* note 210. 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. *Id.* ("[W]e gave

process builds industry awareness of its data practices.[393] 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.[394] This, too, can promote compliance.

3. *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 a hand in writing. One industry representative reported that

> it'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 the government, then] they have to accept it but they will not comply because they were not involved.[395]

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.[396]

Industry actions appeared to be consistent with these reports. For example, 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 do so.[397] This suggests that

---

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 always wanted to do. [The process of developing the code] raised awareness.").

393. McLaggan-van Roon Interview, *supra* note 233 (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).

394. *Id.*

395. Singewald Interview, *supra* note 287. A private investigator involved in the drafting of that industry's code of conduct expressed a similar sentiment that companies are more likely to accept it if they have a role in shaping the Code. Ijfs Interview, *supra* note 354 ("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 then something is construed with our interests in mind, then it is much easier to accept and abide than it being forced upon us.").

396. Wishaw Interview, *supra* note 209.

397. Berkvens Interview, *supra* note 209 (banking industry); van der Burgh Interview, *supra* note 223 (banking industry); van Blokland Interview, *supra* note 314 (pharmaceutical industry); NVH Interview, *supra* note 285 (trade information bureaus); Olijslager Interview, *supra* note 209 (private investigators); *see also* Wishaw Interview, *supra* note 209 (affirming 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

the process of developing codes of conduct increased the sectors' ownership over and acceptance of the rules. On a related front, Peter Hustinx, the former Chair of the Dutch DPA, has reported that the DPA's discussions with industry sectors regarding codes of conduct facilitated the "development of norms" as to how personal information should be protected.[398]

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, but out of a desire to rein in smaller, less responsible firms—the "cowboys," as one industry representative called them.[399] 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.[400] 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 membership, that firms commit to comply with the code.[401] Finally, they expelled or otherwise sanctioned member firms that violated the code in a significant

---

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, what is not allowed with reference to the Data Protection Act, [and] the interaction between the business units." Berkvens Interview, *supra* note 209.

398. Hustinx, *supra* note 28, at 286.

399. Singewald Interview, *supra* note 287 (describing "the cowboy companies . . . [who] don't care").

400. *Cf.* BENNETT & RAAB, *supra* note 26, at 141 (stating that codes allow organizations to "remove suspicions" about their collection and use of personal data).

401. 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. Olijslager Interview, *supra* note 209; PRIVACY CODE OF CONDUCT FOR THE PRIVATE INVESTIGATION INDUSTRY, *supra* note 300, § 2. This turned the code into a legally binding requirement for all private investigation firms, even those that did not belong to the industry association.

way.[402] Companies believed that such measures would preserve the industry's reputation and head off public pressure for direct government regulation.[403] 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."[404]

5. *Self-Policing: Monitoring Peers*

While trade associations seemed eager to engage in policing of smaller companies that they perceived to be irresponsible, they seemed far less inclined to monitor whether their core members, the more established firms, were in fact complying with the code that they had agreed to follow.[405] In-

---

402. Wierdak Interview, *supra* note 201 (describing procedures); Singewald Interview, *supra* note 287 (stating that the direct marketing industry expels); Olijslager Interview, *supra* note 209 (stating that the 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. Singewald Interview, *supra* note 287. 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. Wishaw Interview, *supra* note 209; NVH Interview, *supra* note 285. The association ultimately figured out on its own the identity of the offending firm and pressured it into leaving the organization. NVH Interview, *supra* note 285.

403. As a representative of the trade information bureaus explained:

> The 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.

NVH Interview, *supra* note 285. A representative of the direct marketing industry expressed a similar sentiment, stating that the code provided a way to "protect our own business from [others in our industry]. . . . Our mantra is: 'united we stand, divided we fall.'" Singewald Interview, *supra* note 287; *see also* Wierdak Interview, *supra* note 201; Wishaw Interview, *supra* note 209 (stating that 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 to the authorities that we take the data protection issue very seriously," Berkvens Interview, *supra* note 209, and representatives for the trade information bureaus said they developed theirs "to show the outer world how we are handling the data." NVH Interview, *supra* note 285.

404. NVH Interview, *supra* note 285; *see also* Wishaw Interview, *supra* note 209 (stating that the code of conduct builds trust among customers and that it can be a competitive advantage within an industry).

405. van Blokland Interview, *supra* note 314 (pharmaceutical industry); van der Burgh Interview, *supra* note 223 (banking industry); NVH Interview, *supra* note 285 (trade information bureaus).

stead, with one exception,[406] the associations eschewed monitoring and focused instead on responding to consumer complaints or DPA enforcement actions.[407] Typically, industries used an independent supervisory board for this purpose.[408] The industry code would authorize the board to hear individual complaints and perhaps to expel those companies it found to be in violation of the code.[409] However, neither the board, nor any other arm of the trade association, would monitor compliance or otherwise seek to uncover violations.[410]

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 violations.[411] Any system that relies on individual complaints to identify violations is therefore bound to miss many of them. Indeed, the lead data protection attorney for one industry association candidly said that, due to the lack of monitoring, "we don't know" whether firms in the sector are abiding by the code, or not.[412]

There have, as yet, been no comprehensive studies of industry compliance with the Dutch codes of conduct. Yet existing evidence suggests that industry's reactive system, even when combined with the DPA's rather limited enforcement efforts, is not terribly effective. In 2004 the Ministry of

---

406. *See infra* notes 419-22 and accompanying text.

407. Several codes of conduct do require firms to audit and certify their own compliance. These include the private investigators' code, the banking code, Olijslager Interview, *supra* note 209, and the direct marketing code, Singewald Interview, *supra* note 287. 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* PROCESSING OF PERS. DATA BY FIN. INSTS., *supra* note 298, § 9 (annual self-audit), *with* CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA BY FINANCIAL INSTITUTIONS. § 10 (2010) (less frequent); *see also* Olijslager Interview, *supra* note 209.

408. Singewald Interview, *supra* note 287 (direct marketing industry); Olijslager Interview, *supra* note 209 (private investigators); NVH Interview, *supra* note 285 (trade information bureaus); van der Burgh Interview, *supra* note 223 (banking industry).

409. *Compare* Singewald Interview, *supra* note 287 (stating that the Direct Marketing Association can expel members who violate the DMA's data protection code of conduct), *with* Berkvens Interview, *supra* note 209 (stating that the banking association is not authorized to take formal action against a member that violates the data protection code of conduct).

410. van Blokland Interview, *supra* note 314 (pharmaceutical industry); van der Burgh Interview, *supra* note 223 (banking industry); NVH Interview, *supra* note 285, (trade information bureaus).

411. The industry representatives that I interviewed reported that a very few individuals had availed themselves of the trade associations' complaint process. *See* van der Burgh Interview, *supra* note 223 (noting that he "hardly ever" receives complaints); NVH Interview, *supra* note 285 (noting only six complaints against trade information bureaus since 2003).

412. van der Burgh Interview, *supra* note 223.

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.[413] 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.[414] Compliance with the requirement to notify employees who had been investigated but then found innocent—the very requirement that the industry had fought over in the code negotiation process[415]—was particularly poor.[416] The study's "main conclusion . . . [was] that there is an incomplete compliance with the Privacy Code."[417] It attributed this, in part, to the industry 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.[418] While one must be careful not to read too much into 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, and industry trade associations lack the incentive to do so, 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.[419] The Association trained a group of independent "certifying professionals" on how to assess compliance with the industry code of conduct.[420] It then required each member company 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

413. Regioplan Policy Research, *supra* note 328, at 9.

414. The report found that, in more than half of their cases, private investigation firms violated the requirement that they utilize the least intrusive form of investigation. *Id.* at 88. They violated the requirement that interviews be conducted by two or more investigators, and that they be recorded on tape, nearly two-thirds of the time. *Id.* at 89.

415. *See supra* notes 321-29 and accompanying text.

416. Regioplan Policy Research, *supra* note 328, at 88.

417. *Id.* at 13.

418. *Id.* at 14.

419. Cahn Interview, *supra* note 325.

420. *Id.*

could display a Quality Mark logo as a sign of their sound data protection practices.[421] Those that did not would face the loss of their Association membership.[422]

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.

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.

1. *A Dialogue About Statutory Meaning*

As originally designed, the Dutch code of conduct program assumed that the approved codes of conduct would be binding on the Data Protection DPA.[423] The codes would not, however, bind the courts, and they would remain free to interpret the Data Protection Act on their own.[424] But this is not the way it has worked 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, an insurance company hired a private investigation company to observe an insured who had claimed an injury. Over the course of four days the private investigator drove by the insured's home every three hours and observed him in his home carrying out activities that were incon-

421. *Id.*
422. *Id.*
423. *See supra* notes 232-33 and accompanying text.
424. *See supra* note 236 and accompanying text.

sistent with his claimed incapacity.[425] When the insurance company refused the claim, the insured brought suit on the grounds that the investigator's observation of him in his home had violated his privacy rights.[426] In ruling on this claim, the court looked to the Privacy Code of Conduct for the Private Investigation Industry and, in particular, to its provision governing observation of the subject of an investigation.[427] The court found the investigation agency to be in compliance with the Code.[428] Based largely on this finding, the court concluded that the investigator had not abridged the plaintiff's privacy rights under the Data Protection Act. In short, the court looked to the *Code* in order to interpret the Act.[429]

The interpretative process did not stop there. In its opinion, the court added its own gloss to the Code provisions governing an investigator's observation of a subject. The relevant Code provisions stated observation "conducted in the public domain" generally will not violate the subject's privacy unless it is of a "lengthy and systematic character," in which case it is only "permissible under exceptional circumstances."[430] This rather broad statement does not make clear how "lengthy" or "systematic" the observation must be before it becomes impermissible. The court decision clarified that drive-by surveillance of a person in his home every three hours over the course of four days is not "sufficiently lengthy and systematic" to make it wrongful.[431] The court decision thus interpreted, and added a judicial gloss to, the industry code.

Court decisions can also influence industry codes of conduct more directly. Industry associations want to make sure that their codes are consistent with governing law. Some will accordingly revise their codes in order to incorporate recent court decisions.[432] For instance, court decisions had held that, during an investigation, it was only appropriate to observe another without their knowledge where there were "concrete indications" of wrongdoing.[433] The private investigation industry, taking note of these court deci-

---

425. Rb. Zutphen 9 mei 2007, BB 2007, 1491 m.nt. Vergunst, Heenk en Willemse § 5.10 (Neth.).

426. *Id.* §§ 4.2, 5.3.

427. *Id.* §§ 5.5, 5.10; PRIVACY CODE OF CONDUCT FOR THE PRIVATE INVESTIGATION INDUSTRY, *supra* note 300, § 7.4.

428. Rb. Zutphen 9 mei 2007, BB 2007, 1491 m.nt. Vergunst, Heenk en Willemse § 5.10 (Neth.).

429. *Id.*; Olijslager Interview, *supra* note 209.

430. PRIVACY CODE OF CONDUCT FOR THE PRIVATE INVESTIGATION INDUSTRY, *supra* note 300, §§ 7.4.1-.2; Olijslager Interview, *supra* note 209.

431. Rb. Zutphen 9 mei 2007, BB 2007, 1491 m.nt. Vergunst, Heenk en Willemse § 5.10 (Neth.).

432. Olijslager Interview, *supra* note 209.

433. E-mail from Felix Olijslager, Dir. of the Dutch Info. Ctr. for Sec. & Law, to Dennis D. Hirsch, Geraldine W. Howell Professor of Law, Capital Univ. Law Sch. (Feb. 14, 2013, 22:03 EST) [hereinafter Olijslager E-mail] (on file with author); *see, e.g.*, Hof's-

sions, amended its privacy code in 2009 to incorporate this judicial standard. The provision governing covert use of cameras, as amended, states that "*[u]sing a concealed camera shall take place only on an incidental basis where there are concrete indications that a person is, or has been, guilty of conduct that is seriously reprehensible and/or criminal.*"[434] This example shows that, just as codes of conduct can influence how courts view statutes, so judicial interpretations can shape codes of conduct. The result is a continuing conversation between courts and industry associations through which the underlying statute becomes ever more elaborated.

> [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.[435]

2. *Migrating Codes*

The courts' adoption of code provisions also has another fascinating effect. It expands the code's reach far beyond the companies that formally sign up to comply with it. This expansion occurs along two dimensions. 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.[436] 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.

Judicial decisions can also cause codes to spread in another, even more far-reaching, way. The Data Protection Act, and judicial decisions interpreting it, binds all industries.[437] Where a court adopts a code's interpretation of the Act, that interpretation indirectly becomes part of the law binding on all industries.[438] In this way a code from one industry can,

---

Hertogenbosch 4 januari 2004, AO 2004, 7567 m.nt. Vermeulen, Beuker-Tilstra en Goorden § 4.1 (Neth.) (stating that observation is permitted where "concrete" reasons to believe wrongdoing has occurred).

434. PRIVACY CODE OF CONDUCT FOR THE PRIVATE INVESTIGATION INDUSTRY § 7.5.1 (2009) (italics in original) (on file with author); *see also* Olijslager E-mail, *supra* note 433.

435. Olijslager Interview, *supra* note 209.

436. *Cf.* Wierdak Interview, *supra* note 201 (stating that the DPA will apply interpretations contained in code to companies in that industry that have not signed up to comply with the code).

437. Personal Data Protection Act, *supra* note 26, art. 1(d) (defining "responsible party" to include any "legal person" that determines the purpose of and means for processing personal data).

438. Olijslager Interview, *supra* note 209.

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.[439] 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.[440] The insurance companies believe that this will make it more likely that courts will uphold their employees' investigatory practices.[441] 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."[442]

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 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.[443] 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 kinds of directives together in one document."[444]

---

439. *Id.*
440. *Id.*
441. *Id.*
442. *Id.*
443. Singewald Interview, *supra* note 287.
444. *Id.* (stating that a code of conduct prevents you from having to go through a whole pile of laws); Olijslager Interview, *supra* note 209 (stating that the private investigator industry uses a code to integrate two provisions governing the use of hidden cameras); Wierdak Interview, *supra* note 201 (recounting that sectors used codes to integrate requirements from various laws and statutes into a single document).

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 when the company learns that the drug being tested could be harmful.[445] The medical professionals accordingly made a practice of providing participants' initials, country of origin, birth date, birth year, and gender to the sponsoring pharmaceutical companies.[446] 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 by name, it did not qualify as "personal data."[447] But a 2007 opinion of the Article 29 Working Party[448] made it impossible to hold this view.[449] 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.[450] Under the revised definition, it became clear that the medical professionals *were* providing "personal data"[451] and that their sharing accordingly violated the Act.[452] This put the Data Protection Act squarely in conflict

445. van Blokland Interview, *supra* note 314.

446. *Id.*

447. Personal Data Protection Act, *supra* note 26, art. 1(a) (defining "personal data" as "any information relating to an identified or identifiable natural person").

448. The Article 29 Working Party is an E.U.-level entity that provides expert opinions on data protection law. *See* TASKS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY 1 (1995), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/tasks-art-29_en.pdf.

449. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 4/2007 ON THE CONCEPT OF PERSONAL DATA 13-14 (2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

450. *Id.*; van Blokland Interview, *supra* note 314.

451. van Blokland Interview, *supra* note 314.

452. *Id.*

with the health care regulation, which implicitly *required* such sharing of data.[453]

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.[454] After some negotiation, the DPA agreed that the industry could have these two pieces of information, but no more.[455] The parties implemented the agreement in Section 2.7 of the pharmaceutical industry code, which provides that "date and [year of] birth are not usually traceable to an individual" and so do not constitute information that renders a person identifiable.[456] This short phrase allowed the pharmaceutical companies to resolve the tension between two conflicting statutes.[457]

V. 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;[458] lead to more tailored, workable, and cost-effective rules;[459] increase industry awareness of its privacy impacts and give it a sense of ownership over the rules needed to mitigate them;[460] initiate an iterative process by which broad statutory requirements get interpreted and clarified;[461] and provide a means to resolve conflicts between statutes.[462] Yet the Dutch codes also reveal significant weaknesses in this regulatory method. The Dutch codes are slow-moving and static, not nimble and adaptive.[463] In some situations at least, industry can exert too much leverage in the drafting process, resulting in overly lenient rules.[464] Sectors do not routinely monitor their members' observance of the rules and, in one industry at least, a study

---

453. *Id.*

454. *Id.* 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.

455. *Id.*

456. CODE OF CONDUCT CONCERNING THE PROCESSING OF PERSONAL DATA § 2.7 (2002) (pharmaceutical industry); van Blokland Interview, *supra* note 314.

457. *See* Singewald Interview, *supra* note 287, (stating that the direct marketing industry uses a code to resolve conflicting statutory requirements).

458. *See supra* notes 289-91, 305-16 and accompanying text.

459. *See supra* notes 353-70 and accompanying text.

460. *See supra* notes 390-98 and accompanying text.

461. *See supra* notes 423-35 and accompanying text.

462. *See supra* notes 445-57 and accompanying text.

463. *See supra* notes 339-48 and accompanying text.

464. *See supra* notes 321-29, 371-72 and accompanying text.

found wide-spread non-compliance.[465] Established players can use the codes to strengthen their own position and discourage new entrants.[466]

What lessons can be drawn from such a mixed picture? On 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 United States' 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 United States is to utilize this approach, then it must do so in a way that is sensitive both to the strengths, and to the very real weaknesses, of this regulatory method. It must design its program so as to minimize the weaknesses and maximize the strengths. The remainder of this Part suggests how policymakers might build on the Dutch experience in order to achieve this.

A. Minimizing Weaknesses

To begin with, 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.[467] 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's study of compliance in the private investigator industry, though limited to a single industry sector, showed widespread non-compliance.[468] The United States, with many more businesses for regulators to oversee, may well suffer from the same problem.

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,

465. *See supra* notes 405-18 and accompanying text.
466. *See supra* notes 374-78 and accompanying text.
467. *See supra* notes 385-88 and accompanying text.
468. *See supra* notes 405-18 and accompanying text.

instead, in the hands of approved, professional auditors. It is worth noting that the private investigator sector did not fight this requirement.[469] Instead, the more established members embraced it as a way to demonstrate their sound practices and differentiate themselves from less responsible competitors.[470] Neither the U.S. privacy bills, nor the White Paper, include third-party audits of code compliance or of privacy management systems. The Dutch experience suggests that they should.[471]

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. This Article contains only one clear example of this—the instance in which the private investigator industry was able to convince regulators that the employer who hired the investigation company, not the investigation agency itself, should notify an innocent employee that he had been investigated.[472] 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 to include other stakeholders such as consumer or privacy advocacy groups.[473] 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.[474] However, the paucity of such groups in the Netherlands made it impossible for industry associations to comply with the requirement, and the 2000 Act accordingly dropped it.[475]

The United States 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

469. Cahn Interview, *supra* note 325.

470. *Id.*

471. *Cf.* BENNETT & RAAB, *supra* note 26, at 171 (arguing that a code-based self-regulatory process should include "a verification of those practices through some external and independent conformity assessment process").

472. *See supra* notes 321-29 and accompanying text.

473. *Cf.* Rubinstein, *supra* note 18, at 381 (calling for "openness" in co-regulatory privacy initiatives).

474. Law on Personal Data Files, *supra* note 26, art. 15(2).

475. Hustinx Interview, *supra* note 209 (stating that there were no appropriate candidates, that sometimes it was impossible to find an appropriate stakeholder, and that this made the stakeholder input mechanism unworkable).

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 Paper calls upon multi-stakeholder groups to develop the codes of conduct.[476] 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."[477] This is a 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 its own. Government officials need industry information in order to regulate the fast-changing information economy. One of the main reasons for using codes is that they can 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?[478] Government officials who played key roles in the Dutch code negotiations answered with 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."[479] These government officials believed that including public interest stakeholders at the initial drafting stage could undermine this sense of trust and so either choke off the vital information flow or drive it underground.[480] 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. [T]he public part of a parliament serves the deal-making which happens elsewhere. [B]ringing 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 [for] the meeting.[481]

Thus, according to the Dutch regulators, bringing stakeholders in at the initial drafting stage could actually make the process less transparent by

476. WHITE PAPER, *supra* note 10, at 23.

477. *Id.*

478. *Cf.* Harter, *supra* note 101, at 84 (explaining why "negotiation is a process best carried on in private").

479. van de Pol Interview, *supra* note 210.

480. McLaggan-van Roon Interview, *supra* note 233 (including stakeholders at an early stage would make the negotiations too difficult).

481. Hustinx Interview, *supra* note 209.

driving the real discussions underground. 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.[482] In the first, industry and government would collaborate on an initial, tentative draft.[483] In the second, public interest stakeholders such as consumer or privacy groups would join the discussion and provide their reactions and ideas.[484] 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).[485] 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.[486] This could add transparency and accountability to the process without undermining the trust and information-sharing that can emerge from government-industry interactions.[487] 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.[488] U.S. policymakers should consider using such a staged approach.

3. *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 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.[489] Measures such as these could reduce any cartel-like tendencies in the code drafting process.

---

482. Interview with Lokke Moerel, Head of Privacy Practice, De Brauw, Blackstone & Westbroek, in Amsterdam, Neth. (Apr. 16, 2010).

483. *Id.*

484. *Id.*

485. *Id.*

486. *Id.*

487. Wishaw Interview, *supra* note 209 (supporting this idea).

488. van der Burgh Interview, *supra* note 223.

489. *See* GUNNINGHAM & SINCLAIR, *supra* note 19, at 108.

4. *Improve Adaptability*

The Dutch codes also display a third, important weakness. They are slow-moving, largely static instruments. Some took years to negotiate. Many remained unchanged during their five-year term.[490] Others expired at the end of their initial five-year period because industry and regulators could not reach agreement on whether and how to update them.[491] 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.[492]

How to make codes and safe harbor programs more adaptable? This is a difficult question. There are ways to speed up and streamline the approval process. For example, the FTC could decide that notice-and-comment procedures apply only to the first version of a code, and not to subsequent iterations. Or, it could take the position that "de minimis" code changes that do not pose a threat to individual privacy do not require agency approval. But such measures run the risk of enhancing adaptability at the expense of accountability. Who, after all, would decide whether a given change is de minimis? If it is the FTC, then the process is not so streamlined after all. If it is the regulated industry, this creates a dangerous conflict of interest.

Another approach might be to think, first, about what is it that makes the process static. The Dutch experience suggests that it is the high transaction costs involved in negotiating an approved code of conduct. Once the parties have made it through the exhausting process and reached an agreement, neither side is eager to reopen negotiations. The approved code thus sits untouched for its five-year period (and perhaps longer if the code expires).

One way to combat this might be to require that, subsequent to code approval, the negotiating parties continue to meet on a regular basis to discuss code implementation and possible improvements. The process would never "end." The parties would always be looking for ways to improve their agreement—to make it more protective of individual privacy, more workable for business, and more in touch with changing realities on the ground. Such an approach might prevent the parties from becoming locked into the initial agreement, and instead cause them to see the process as one of continuous learning and improvement. Professor Freeman has called this a "commitment to provisionalism."[493] She argues that negotiated forms of regulation, such as codes of conduct, should build in a "system for evaluat-

490. *See* Appendix: Dutch Data Protection Codes of Conduct.
491. *Id.*
492. *See supra* notes 89-95, 263-65 and accompanying text.
493. Freeman, *supra* note 18, at 29.

ing and reassessing those agreements on a regular basis" in order to "facilitate revisiting and modifying rules."[494]

The literature on adaptive natural resource management is relevant here.[495] Adaptive management emphasizes "an iterative, incremental decision-making process built around a continuous process of monitoring the effects of decisions and adjusting decisions accordingly.[496] It stresses the establishment of monitoring and adjustment mechanisms that allow regulators to learn and to act based on that learning. Were the code negotiation process to incorporate such an adaptive process—to institutionalize continuous monitoring, feedback, and adjustment—it could both keep the negotiation process from becoming ossified and, at the same time, increase monitoring and accountability.[497] Further research and experimentation are essential to determining how to increase code adaptability without sacrificing accountability. Adaptive management theory may offer a useful starting place for that inquiry.

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 Program Sector-Based*

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 current and 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 business information with regulators. This can lead to more tailored, workable, and cost-effective rules.

Safe harbor programs that include companies from many different sectors will find it difficult to tailor their rules to *particular* sectoral realities

494. *Id.*

495. *See, e.g.*, ADAPTIVE ENVIRONMENTAL ASSEMENT AND MANAGEMENT (C.S. Holling ed., 1978) (seminal book on the subject); J.B. Ruhl, *Regulation by Adaptive Management—Is it Possible?*, 7 MINN. J. L. SCI. & TECH. 21 (2005) (describing this literature).

496. Ruhl, *supra* note 495, at 28 (discussing Holling's work).

497. Freeman, *supra* note 18, at 30.

and so will lose much of this benefit.[498] 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.[499] While such an NGO might design its program on a sectoral level, it need not do so. Indeed, NGOs 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.[500]

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. For example, the FTC could negotiate safe harbor agreements with the pharmaceutical sector, the utility sector (where the emerging smart grid will make privacy issues increasingly relevant), the data broker sector, and other such branches of industry. 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.[501] The Rush Bill extends the safe harbor approach to notice and choice (Title I) and accuracy and access (Title II), but not to data minimization, data security, and accountability (Title III).[502] 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.[503] The Dutch Data Protection Act, on the other hand, sets no such limits. It calls on industry sectors to

498. 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.

499. Kerry-McCain Bill, *supra* note 9, § 501(a).

500. Rush Bill, *supra* note 12, § 401; Stearns Bill, *supra* note 12, § 9; WHITE PAPER, *supra* note 10, at 23.

501. Rush Bill, *supra* note 12, § 403(2)(D); Kerry-McCain Bill, *supra* note 9, §§ 501(a)(1), 501(c).

502. Rush Bill, *supra* note 12, § 403(2)(D).

503. Kerry-McCain Bill, *supra* note 9, §§ 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. *Id.* § 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.

address all aspects of the statute in their codes of conduct.[504] 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.[505] This indicates that comprehensive privacy legislation may well be essential to the success of collaborative efforts. 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 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 provide a structure for the industry codes and to give companies a strong incentive to come to the table and negotiate a code of conduct.[506]

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.[507] 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.[508] 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

---

504. Personal Data Protection Act, *supra* note 26, art. 25 (stating that codes of conduct "implement this Act").

505. *See supra* notes 277-83 and accompanying text.

506. *Cf.* Rubinstein, *supra* note 18, at 422 (calling for a new law that codifies fair information practices and includes a safe harbor program).

507. *See supra* note 404 and accompanying text.

508. *See* Rubinstein, *supra* note 18, at 417 (suggesting government recognition as a way to encourage firms to sign up for safe harbor programs).

cycle in which all companies in an industry come to believe they must 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 European Union, regional. Companies that transmit personal data across national boundaries accordingly have to keep track of various national and regional data protection requirements and 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 too could American sectors craft codes of conduct or safe harbor programs that bring together and incorporate the requirements of the various national and regional laws or principles. 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.[509] Similarly, the Asia-Pacific Economic Cooperation (APEC) organization's Cross-Border Privacy Rules system allows approved "Accountability Agent[s]" to certify a single set of privacy rules as being compliant with privacy principles adopted by APEC member nations.[510] 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 or principles, the resulting code would then constitute a single, globally interoperable, approved 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.[511] The U.S.–E.U. Safe Harbor Agreement takes a step in this direc-

509. Council Directive 95/46/EC, *supra* note 151, art. 27(3).

510. *See* Applications to Serve as Accountability Agents in the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System, 77 Fed. Reg. 44,582 (July 30, 2012) (describing the role of accountability agents in the APEC system).

511. Similar efforts are already being made on a firm-specific basis. Through the mechanism of Binding Corporate Rules, individual multi-national companies are obtaining

tion, and the Administration White Paper also expresses an interest in it.[512] 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 to making them free-form entities that encompass companies from many different industry sectors.

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 explained above, specific aspects of Dutch history have forged a culture based on cooperation and consensus.[513] This may predispose the Dutch to the types 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.[514]

As Robert Kagen has shown, U.S. regulatory culture is very different.[515] 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.[516] 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 the type of cooperative discussions and problem-solving that the Dutch seem to have been able to achieve and that is essential to the safe harbor approach.

---

approval of their global privacy policies from multiple countries, and so are developing a single set of rules that will constitute compliance in each of those nations. *See generally*, LOKKE MOEREL, BINDING CORPORATE RULES: CORPORATE SELF-REGULATION OF GLOBAL DATA TRANSFERS (2012). This Article proposes that branches of industry use sector-based codes of conduct to achieve a similar result for the sector as a whole.

512. WHITE PAPER, *supra* note 10, at 31-33. The author and a colleague, Ira Rubinstein, suggested the idea in comments on the Department of Commerce's Green Paper.

513. *See supra* notes 266-69 and accompanying text.

514. *See supra* notes 270-75 and accompanying text.

515. ROBERT A. KAGAN, ADVERSARIAL LEGALISM: THE AMERICAN WAY OF LAW, at ix (2001).

516. *See* DANIEL J. FIORINO, THE NEW ENVIRONMENTAL REGULATION 186 (2006) (describing difficulties in transplanting the Dutch negotiated system to the United States with its adversarial style of regulation).

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 explained above, the safe harbor approach can allow industry representatives to exert too much leverage.[517] The Dutch themselves recognized this problem and tried to bring consumer groups into the drafting process as a way to mitigate it.[518] But the small number and limited resources of these groups made this impossible.[519] Were the United States to implement the safe harbor approach, the situation would be very different. Due to its adversarial culture and its greater size, the United States 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,[520] they could serve as a counterweight 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.

APPENDIX: DUTCH DATA PROTECTION CODES OF CONDUCT

Sector	Organization	Name of Code (Dutch)	Name of Code (English)	Statute	Date Approved or Renewed	Date Expires	Expired?	English Translation?	Public Participation in Code Drafting
Personnel Recruitment Agencies and Executive Search	Organization of Personnel Recruitment Consultants (Nederlandse brancheorganisatie van bureaus voor werving, selectie en executive search (OAWS))	Gedragscode voor de werving & selectie-branche	Code of Conduct With Regard to Recruitment and Selection	WPR WBP	Nov. 28, 1990 July 30, 2004 (amended and renewed)	Nov. 28, 1995 July 30, 2009	Yes Yes	No	Prepared with "Verenigining voor Hoger Personeel" (Association for Higher Personnel)

517. *See supra* notes 321-29 and accompanying text.
518. *See supra* note 474 and accompanying text.
519. *See supra* note 475 and accompanying text.
520. *See supra* notes 476-88 and accompanying text.

Sector	Organization	Name of Code (Dutch)	Name of Code (English)	Statute	Date Approved or Renewed	Date Expires	Expired?	English Translation?	Public Participation in Code Drafting
Computing Services	Association of Computing Services and Software Agencies (COSSO)	COSSO gedragscode persoonsregist-raties	COSSO Code of Conduct (Registration of Personal Data)	WPR	Jan. 17, 1991 (for three years)	Jan. 17, 1994	Yes	No	COSSO Code prepared with "Stichting Waakzaamheid Persoonsregistratie" (Foundation for Watchfulness with Regard to the Registration of Personal Data)
Non-Profit Research Institutes Focusing on Behavioral and Social Scientific Research	Association of Research Institutes (Vereniging van Onderzoek Instituten (VOI))	VOI gedragscode persoonsregist-raties	VOI Code of Conduct (Registration of Personal Data)	WPR	May 8, 1991 (for five years)	May 8, 1996	Yes	No	Consulted the Social and Economic Council of the Netherlands (SER) and the Dutch Association for Sociology and Anthropology, also prepared with "Stichting Waakzaamheid Persoonsregistratie"
Market Research Bureaus	Association of Market Research Bureaus (Verenging van Marktonderzoekers (VMO)) and the Dutch Association of Marketing Research (Vereniging van Marktonderzoekburd eaus en de Nederlandse (NVvM)	Privacy – gedragscode markt – en opinieonderz oek	Privacy Code of Conduct for Market and Opinion Research	WPR	June 12, 1991	June 12, 1996	Yes	No	Prepared with "Stichting Waakzaamheid Persoonsregistratie"
Direct Marketing Industry	Direct Marketing Institute of the Netherlands (Direct Marketing Instituut Nederland (DMIN) (becomes the Dutch Association for Direct Marketing, Distance Selling and Sales Promotion (DMSA)) Dutch Dialogue Marketing Association (DDMA)	Gedragscode Direct Marketing Instituut Nederland	Code of Conduct by the Dutch Direct Marketing Institute Dutch Dialogue Marketing Association (DDMA) Privacy Code (follows FEDMA Community Code approved by Art. 29 Working Group)	WPR Directive 95/46/EC	Oct. 2, 1992 (for three years) June 13, 2003 (by Art. 29 Working Group)	Oct. 2, 1995	Yes	No No	Prepared with "Stichting Waakzaamheid Persoonsregistratie"

Sector	Organization	Name of Code (Dutch)	Name of Code (English)	Statute	Date Approved or Renewed	Date Expires	Expired?	English Trans-lation?	Public Participation in Code Drafting
Pharmaceu-tical Industry	Association of the Pharmaceutical Industry (Nederlandse Associatie van de Farmaceutische Industrie (NEFARMA)	NEFARMA Privacy Gedragsregels	NEFARM A Privacy Rules of Conduct	WPR WPR WBP WBP	Oct. 13, 1992 (for five years) May 7, 1998 Aug. 26, 2002 (amended and reviewed) Apr. 26, 2010 (amended and renewed)	Oct. 13, 1997 May 7, 2003 Aug. 26, 2007	Yes No Yes No	No No No No	Prepared with the Koninklijke Maatschappij tot bevordering der Geneeskunde (KNMG), de Koninklijke Maatschappij ter bevordering der Pharmacie (KNMP) en het Landelijk Patiënten/ Consumenten Platform (LP/CP)
Veterinary Products Industry	Association of Producers and Importers of Veterinary Products (Vereniging van Fabrikanten en Importeurs van Diergeneesmiddelen in Nederland (FIDIN))	FIDIN-Privacygedrags-regels	FIDIN Privacy Rules of Conduct 1998 version 2003 version	WPR WPR WBP	Nov. 27, 1992 (for five years) July 28, 1998 (amended and renewed)	Nov. 27, 1997 July 28, 2003	Yes	No	Prepared with the Koninklijke Nederlandse Maatschappij voor Diergeneeskunde (Royal Association for Veterinarians)
Mail Order	Dutch Mail Order Union (Nederlandse Postorderbond)	Gedragscode Nederlandse Postorderbond	Code of Conduct Dutch Mail Order Union	WPR	Mar. 10, 1993 (for three years) (integrated into DMSA Code Jan. 1995)		No	No	Prepared with "Stichting Waakzaamheid Persoonsregistratie"
Commercial Information Bureaus	Netherlands Association of Commercial Information Bureaus (Nederlandse Vereniging van Handelsinformaticbureaus (NVH))	Gedragscode Nederlandse Vereniging van Handelsinfor matiebureaus	Code of Conduct Association of Commercial Information Bureaus	WPR WBP WBP	June 17, 1993 Aug. 14, 2003 (amended and renewed) Aug. 25, 2011 (amended and renewed)	June 17, 1998 Aug. 17, 2008	Yes Yes	No No No	1993 Code prepared with "Stichting Waakzaamheid Persoonsregistratie"
Medical Research	Federation of Medical Research Organizations (Federatie van Medisch Wetenschappe-lijke Verenigingen)	Gedragscode Gezondheids on-derzo ek "Good gedrag"	Code of Conduct with Regard to Medical Research "Best Practices"	WPR WBP	July 14, 1995 April 19, 2004 (amended and renewed)	July 14, 2000 Apr. 19, 2009	Yes Yes	No No	1995 code prepared with medical and scientific associations, key figures from stakeholder organizations and the National Council for Public Health
Banking	The Netherlands Bankers Association (Nederlandse Vereniging van Banken (NVB))	Privacy Gedragscode Banken	Privacy Code of Conduct for the Banking Industry	WPR	Oct. 16, 1995	Oct. 17, 1998	Yes	Yes	1995 code prepared with "Stichting Waakzaamheid Persoonregistratie"

Sector	Organization	Name of Code (Dutch)	Name of Code (English)	Statute	Date Approved or Renewed	Date Expires	Expired?	English Translation?	Public Participation in Code Drafting
Insurance Companies	Association of Insurers in the Netherlands (Verbond van Verzekeraars in Nederland (VVN))	Gedragscode Verwerking Persoonsgegevens Verzekeringsbedrijf	Code of Conduct on the Processing of Personal Information by Insurance Companies	WPR	Feb. 26, 1998	Feb. 27, 2003	No	No	1998 code prepared with "Stichting Waakzaamheid Persoonsregistratie"
Financial Institutions (banks and insurance companies)	Netherlands Bankers Association and the Association of Insurers in the Netherlands (Nederlandse Vereniging van Banken en het Verbond van Verzekeraars)	Gedragscode Verwerking Persoonsgegevens Financiële Instellingen	Code of Conduct for the Processing of Personal Information by Financial Institutions	WBP WBP	Jan. 27, 2003 Apr. 13, 2010 (amended and renewed)	Jan. 28, 2008	Yes No	No No	
Private Investigation Industry	Private Investigation Industry Association (Vereniging van Particuliere Beveiligingsorganisaties (VPB))	Privacygedragscode sectorparticuliere onderzoeksbureaus van de Vereniging van Particuliere Beveiligingsorganisaties (VPB)	Privacy Code of Conduct for the Private Investigation Industry	WBP WBP	Jan. 13, 2004 Oct. 21, 2009 (amended and renewed)	Jan. 13, 2009	Yes No	Yes Yes	
Bailiffs	Royal Association of Bailiffs (Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBvG))	Privacygedragscode inzake verwerken persoonsgegevens doorleden van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBvG)	Privacy Code of Conduction on Processing Personal Data by Members of the Royal Association of Bailiffs	WBP	Feb. 18, 2004	Feb. 19, 2009	Yes	No	
Research and Statistics: Policy Research; Statistical Research; Market Research	Market Research Association (Marktonderzoekassociatie (MOA)); Association for Policy Research (Vereniging voor Beleidsonderzoek (VBO)); Society for Statistics and Research (Vereniging voor Statistiek en Onderzoek (VSO))	Gedragscode voor Onderzoek en Statistiek	Code of Conduct for Research and Statistics	WBP WBP	Feb. 18, 2004 June 21, 2010 (amended and renewed)	Feb. 18, 2009	Yes No	No	
University Research	Association of Universities (Vereniging van Universiteiten (VSNU))	Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek van de VSNU Vereniging van Universiteiten	Code of Conduct for Use in Personal Data in Scientific Research of VSNU Associated Universities	WBP	Jan. 3, 2006	Jan. 3, 2011	Yes	No	Prepared with the Social Scientific Council of the Netherlands (KNAW) and the Royal Netherlands Academy of Arts and Sciences (SWR)
Health Research	Association for Health Insurance Companies (Zorgverzekeraars Nederland)	Gedragscode Verwerking Persoonsgegevens Zorgverzeeraars	Code of Conduct on the Processing of Personal Information by Health Insurance Companies	WBP	Dec. 13, 2011	Dec. 13, 2016	No	No	

Sector	Organization	Name of Code (Dutch)	Name of Code (English)	Statute	Date Approved or Renewed	Date Expires	Expired?	English Translation?	Public Participation in Code Drafting
Grid Operators		Gedragscode Verwerking van Persoonsgegevens door Netbeheerders in het kader van Installatie en Beheer van Slimme Meters bij Kleinverbruikers van Netbeheer	Code of Conduct on Processing of Personal Information by Grid Operators in the Context of Installing and Maintaining Smart Meters	WBP	May 9, 2012	May 9, 2017	No	No	
Energy Suppliers	Netherlands Energy Association (Vereniging Energie Nederland)	Gedragscode Leveranciers Slimme Meters	Code of Conduct for Suppliers of Smart Meters	WBP	Jan. 8, 2013	Jan 8, 2018	No	No	