THE GOVERNANCE OF PRIVACY THROUGH CODES OF CONDUCT:

INTERNATIONAL LESSONS FOR U.S. PRIVACY POLICY

Colin J. Bennett,*
Department of Political Science, University of Victoria, BC. Canada

Deirdre K. Mulligan*
School of Information, University of California, Berkeley

Paper prepared for presentation at the 2012 Privacy Law Scholars Conference,
George Washington University, June 7-8 2012

DRAFT: NOT FOR CITATION OR ATTRIBUTION

---

* Professor, Department of Political Science, University of Victoria, BC. Canada.
* Assistant Professor of Law at the UC Berkeley School of Information and a Faculty Co-Director of the Berkeley Center for Law and Technology. The project was supported in part by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

The recent White Paper on privacy from the Obama Administration has proposed a high-level Consumer Privacy Bill of Rights (CPBR) containing a number of common fair information principles (FIPS) to guide the development of enforceable codes of conduct to govern corporate behavior and to serve as a baseline for federal law. The White Paper encourages "the development of voluntary, enforceable privacy codes of conduct in specific industries through the collaborative efforts of multi-stakeholder groups..." It envisages a Privacy Policy Office within the Department of Commerce convening and facilitating the creation of multi-stakeholder groups "to develop voluntary but enforceable codes of conduct." These codes would be enforceable against companies that agreed to abide by them, would inform enforcement actions more broadly, and if Congress accepts the Administration's recommendations, provide the basis of a safe harbor framework under new legislation.[†]

As follow-up, the National Telecommunications and Information Administration (NTIA) issued a request for public comments on the "Multi-stakeholder Process to Develop Consumer Privacy Data Privacy Codes of Conduct."[‡] The NTIA is developing recommendations for areas amenable to the development of codes of practice; it has tentatively proposed a process to develop a code of conduct on transparency in mobile applications. The White House requested feedback on a number of questions about the process of code development including: strategies and techniques for securing broad participation with requisite expertise and diversity of views in light of extremely varying resource constraints; managing the tension between the need for expertise and commitment and inclusiveness; and, the benefits of in-person and virtual meetings and other forms of engagement.[§]

The Administration's approach reflects its commitment—and that of past Democratic administrations[**]—to flexible, market-driven responses to privacy, but couples it with substantive and procedural demands of how such solutions must meet the needs of the public. Flexible solutions are viewed as consistent with innovation and consumer-oriented, contextual responses to privacy

---

† Executive Office of the President, *Consumer Data Privacy in a Networked World* (Washington DC, February 2012).

‡ Department of Commerce, National Telecommunications and Information Administration, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, *Federal Register*, Vol. 77, No. 43, March 5, 2012 at: http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf

§ Ibid, p. 13100.

** William J. Clinton and Albert Gore JR. *A Framework for Global Electronic Commerce* 4 (1997) (promoting self-regulation as the preferred approach to protecting online privacy) at: http://clinton4.nara.gov/WH/New/Commerce/

concerns.[††] The evolving federal privacy policy is grounded in the belief that a good deal of self-regulation is desirable, and indeed unavoidable irrespective of whether additional legislative requirements are enacted. Multi-stakeholder codes are a centerpiece of the Administration's approach.

Privacy codes of practice have long been used internationally. The term, however, has no stable meaning: there are "codes of conduct" and there are "codes of conduct."[‡‡] Nor is the relationship between codes and other policy instruments clear. Clarifying the definition of code, exploring their use and history internationally and domestically, and understanding their relationship to other privacy tools helps understand the risks and opportunities in this phase of the development of US privacy policy. The Consumer Privacy Bill of Rights provides high-level guidance about the content of the codes, and the current NTIA solicitation is supposed to develop some similar recommendations on structures and processes. However pending decisions will determine the relationship between the proposed processes and future and existing mechanisms for corporate accountability. Understanding the salient similarities and differences between the proposed multi-stakeholder process, and past and current codes and code development processes (in the US and abroad), can assist in this decision- making.

Existing codes operate with various levels of compulsion along a continuum of policy instruments with command-and-control sanction at one end, and voluntarism at the other. In the middle of the continuum are a number of mixed or "co-regulatory" approaches, which allow for variable degrees of flexibility or voluntariness, and different levels of governmental involvement and compulsion.[§§] Some codes are properly "codified"; others more loosely structured. Some are developed in formal, open, transparent consultative processes; others are produced in more closed settings. Despite a huge volume of academic literature on forms of self-regulation, and on the conditions under which such forms of governance are more likely to be effective, there is in fact very little scholarly literature on privacy codes of practice per se. Discussion about privacy codes, in the United States and elsewhere, tends to proceed with a lack of clarity on basic terminology, and without appropriate levels of reflection

[††] *Consumer Data Privacy in Networked World*, p. 2 ("will help promote innovation. Flexibility will also encourage effective privacy protections by allowing companies, informed by input from consumers and other stakeholders, to address the privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single, rigid set of requirements.")

[‡‡] In some schemes, codes of conduct are called "codes of practice." We do not see any distinction between the two, and use the terms interchangeably.

[§§] Margot Priest, "The Privatization of Regulation: Five Models of Self-Regulation," *Ottawa Law Review* 29 (1998): 233-302.

on the long experience with how codes of conduct have operated in other policy sectors.[***]

This paper begins by reviewing the extensive international experience with privacy codes of practice, and by developing some useful typologies of codes based on participants, incentives, scope, function, and level of compulsion. It then examines the experience with codes and recent multi-stakeholder initiatives in the US in which privacy is addressed. It positions the Administration's initiative within the international regulatory landscape and draws on insights from new governance scholarship to offer some thoughts on the chances of success.

Codes of Practice and Privacy Governance

Codes of practice in various sectors have proliferated in recent years, as the perceived weaknesses of the more traditional, top-down, "command-and-control" forms of regulation have surfaced within a neo-liberal era characterized by a greater skepticism about the institutions of government and their capacity to generate social change. Kernaghan Webb notes that "voluntary codes harness market, peer and community energies to influence behavior, and draw on the infrastructure of intermediaries such as industry associations, standards organizations and non-governmental organizations for rule development and implementation."[†††] These efforts seek to promote "governance" more than "government." They are less about telling organizations what to do and not do, with the threat of sanction, than about encouraging them to "do the right thing." Crucial, therefore, is the use of existing market incentives. Governments in this model do not "row" but "steer."[‡‡‡] Governance is about "nudging" private actors to do the right thing, and convincing them that what is in the public interest is also in their interest. [§§§]

[***] See Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006), ch. 6. For recent efforts to inject knowledge of international experience with co-regulatory privacy codes into the U.S. policy debates see, Rubinstein, Ira, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes (March 1, 2010). I/S, A Journal of Law and Policy for the Information Society, Vol. 6, p. 356, 2011; and Hirsch, Dennis D., The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? (February 8, 2011). Seattle University Law Review, Vol. 34, No. 2, 2011 (discussing codes of conduct as pursued in various EU member states).

[†††] Kernaghan Webb (ed). *Voluntary Codes: Private Governance the Public Interest and Innovation* (Ottawa: Carleton Research Unit for Innovation, Science and Environment, 2004).

[‡‡‡] Charles D. Raab, "From Balancing to Steering: New Directions for Data Protection," in C. Bennett and R. Grant, *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press, 1999).

[§§§] Richard Taylor and Cass Susstein, *Nudge: Improving Decisions about Health, Wealth and Happiness.* New Haven: Yale University Press, 2008.

In this model, governance also relies on networks of public and private actors to achieve policy goals.[****] Those networks need to be properly defined and coordinated. The continuing interactions between the network members, which have a certain autonomy from the institutions of government, constitute the essence of the policy process. Government aims to facilitate, sustain, and feed such processes. Government then becomes decentered or fragmented, or in some interpretations "hollowed out."[††††] It no longer seeks to exercise a monopoly of policy-making authority, but rather to facilitate solid documentation of problems and the generation of solutions by those with deep subject matter expertise, and then through a process of inclusive, transparent dialogue select the most promising path forward.

Many of these trends towards governance are generally observed across most advanced industrial states.[‡‡‡‡] They are rooted in globalization, and in broader ideological shifts against "big government." The specific manifestations of different policy instruments obviously vary from jurisdiction to jurisdiction, and over time. Thus, what might be considered an appropriate tool in the governmental toolkit, is shaped by different legal, constitutional, political, and cultural perceptions about what is likely to "work" in one country rather than another, and indeed what is consistent with "our way of doing things."[§§§§]

This overall shift from command-and-sanction government to more decentered and networked models of "governance" is readily observable in privacy protection policy as well. In the 1970s, statutory privacy or data protection law, the vast majority of which was European in origin, was considered necessary and sufficient for a national privacy or data protection policy. Over time, and as non-European countries adopted similar statutes, other self-regulatory and technological instruments were added to the toolbox of potential policy instruments. In the U.S., legislators keen to harness the on-the-ground expertise of industry to assist in problem solving with respect to information privacy and security, have enacted regulatory frameworks that defer the specifics of compliance to industry standard setting.[*****] The Federal Trade Commission (FTC), which has emerged as the key regulator of privacy in the private sector, has consistently used its soft law powers of convening, fact-finding, and

---

[****] Jody Freeman, Collaborative Governance in the Administrative State, 45 UCLA L. REV. 1, 21–33 (1997)

[††††] R.A.W Rhodes, "The Hollowing out of the State," The Political Quarterly
Volume 65, Issue 2, pages 138–151, April 1994

[‡‡‡‡] See, J. Kooiman, *Governing as Governance.* London: Sage, 2003.
Rhodes, R.A.W. (1997): *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*, Open University Press.

[§§§§] Christopher Hood and Helen Margitts, *The Tools of Government in the Digital Age.* London: Palgrave MacMillan, 2007.

[*****] Bamberger, Kenneth A., Technologies of Compliance: Risk and Regulation in a Digital Age. Texas Law Review, Vol. 88, p. 669, 2010.

reporting, to push industry to develop policies and technical mechanisms to advance the privacy interests of consumers.[†††††]

Today, the conventional wisdom everywhere is that law is necessary, but not sufficient; it obviously needs to be supplemented by other policy instruments, fashioned and implemented within a broader policy network.[‡‡‡‡‡] Codes of practice, along with privacy impact assessments, privacy standards, privacy seals, privacy-enhancing technologies, and binding corporate rules comprise the contemporary "toolbox."

It should also be noted that contemporary efforts to encourage best practices in the private sector tend to be framed in terms of "accountability." The October 2009 discussion paper from the Centre for Information Policy Leadership's "Accountability Project" is premised on the need to shift "the focus of privacy governance to an organization's ability to demonstrate its capacity to achieve specified objectives" and "vesting the organization with both the ability and the responsibility to determine appropriate, effective measures to meet those goals."[§§§§§] However, this and the further analysis from this project never mention "codes of practice" as necessary elements of privacy governance. Some Canadian privacy commissioners have also encouraged accountability frameworks as necessary components of internal privacy management.[******] Again codes of practice are not mentioned.

So, are privacy codes of practice perhaps a policy instrument of the past, whose value has been discredited and whose functions are now assumed by other mechanisms of self-regulation? As explained below, they have played, and continue to play, a role in several existing national and international data protection regimes. Why have privacy codes of practice been conceived and adopted as instruments of self-regulation or co-regulation? In what form do they appear? What is their scope? What legal function do they perform?

[†††††] Bamberger, Kenneth A. and Mulligan, Deirdre K., Privacy on the Books and on the Ground (November 18, 2011). Stanford Law Review, Vol. 63, January 2011

[‡‡‡‡‡] Bennett and Raab, *The Governance of Privacy.*

[§§§§§] Center for Information Policy Leadership, "Data Protection Accountability: The Essential Elements" October 2009 at:
http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf
Center for Information Policy Leadership, "Demonstrating and Measuring Accountability: A Discussion Document," October 2010 at:
http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

[******] Privacy Commissioners of Canada, British Columbia, Alberta, *Getting Accountability Right with a Privacy Management Program* (March 2012) at:
http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf

Privacy Codes of Practice: The International Experience

Incentives and Purposes

Reviewing the early experience with privacy codes of practice under the Dutch law, Peter Hustinx, formerly President of the Netherlands *Registratiekamer* (the Dutch Data Protection Authority), and now the European Data Protection Supervisor once stated that codes of practice can serve four purposes: *to avoid legislation; to anticipate legislation; to implement legislation; and to supplement legislation.*[††††††] Although these incentives are not mutually exclusive, they provide a useful axis for the consideration of codes in this analysis.

In circumstances where private corporations are not covered by statutory privacy protection law, there is often a strong motivation for the organization or their trade associations to try to prove that self-regulation works and that governmental intervention is therefore unnecessary. Privacy codes of practice have played a central role as defensive strategy, especially at the time during the 1980s and 1990s when most states had not adopted privacy laws, and particularly in North America. Before the Canadian Personal Information Protection and Electronic Document Act (PIPEDA) was enacted in 2000, for instance, most major trade associations produced codes designed for this purpose, based on the 1981 OECD Privacy Guidelines. Their content varied, however, and they generally lacked any means of enforcement.[‡‡‡‡‡‡]

In the United States the advent of various marketing techniques—direct mail, telemarketing, fax, email, online behavioral[§§§§§§]—has often been followed by the adoption of a self-regulatory framework to address privacy issues.[*******] These codes have been viewed as weak by privacy advocates, have historically lacked meaningful oversight and enforcement mechanisms, and have had varied levels

[††††††] Peter Hustinx, "The Use and Impact of Codes of Conduct in the Netherlands," (paper presented to the 16th International Conference on Data Protection, the Hague, 6-8 September 1994), p. 3

[‡‡‡‡‡‡] Colin J. Bennett, *Implementing Privacy Codes of Practice,* (Rexdale: Canadian Standards Association, 1995); Lola Fabowale, *Voluntary Codes: A Viable Alternative to Government Legislation* (Ottawa: Public Interest Advocacy Centre, May 1994).

[§§§§§§] Network Advertising Initiative, *Self-Regulatory Principles for Online Preference Marketing by Network Advertisers* (2000) http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf.

[*******] Privacy and American Business handbooks of company and industry U.S. privacy codes: from 1994 (168 pp), 1995 (130 pp.), and 1996 (148 pp.), along with P&AB commentaries opening each volume.

See, *e.g.*, *Guidelines for Ethical Business Practice*, DIRECT MARKETING ASSOCIATION (May 2011), http://www.dmaresponsibility.org/Guidelines/ (self-regulatory guideless addressing, among other things, mail marketing, digital marketing, telephone marketing, and mobile marketing); *Self-Regulatory Code of Conduct*, NETWORK ADVERTISING INITIATIVE (2008), http://networkadvertising.org/Principles.pdf.

of commitment from relevant industry players.[†††††††] In recent years the FTC, in part due to the role such self-regulation is supposed to play under the US-EU Safe Harbor Agreement, has pushed industry to adopt meaningful oversight, enforcement, and consumer remedy mechanisms.[‡‡‡‡‡‡‡] However, the legitimacy of these self-regulatory privacy codes is continuously called into question on both substantive and procedural grounds. Recently more inclusive, multi-stakeholder efforts have emerged to address privacy issues. Pulling together civil society, the academy and sometimes regulatory bodies as well as industry, efforts such as the Platform for Privacy Preferences and Tracking Protecting working groups at the World Wide Web Consortium, the Antispyware Coalition, and the Global Network Initiative have taken a more inclusive and open approach to participation and brought in various methods for easing enforcement. Perspectives on the legitimacy and utility of such efforts has been decidedly more mixed.[§§§§§§§]

As legislation becomes more imminent, codes of practice can take on a further purpose. First, they can be used politically to shape the content of legislation and eventually to inform regulatory and court interpretation of adequate

---

[†††††††] Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, ELECTRONIC PRIVACY INFORMATION CENTER (Mar. 4, 2005), http://epic.org/reports/decadedisappoint.html (concluding that self regulation efforts in a number of Internet contexts have, for the most part, failed to protect consumers); Pamela Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, WORLD PRIVACY FORUM (Nov. 2, 2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (identifying the failures of the Network Advertising Initiative (NAI), including its failed privacy technologies, its focus on outdated technology, its lack of representation from the majority of behavioral advertising companies, and the lack of transparency and independence of TRUSTe, its third party enforcement program).

[‡‡‡‡‡‡‡] *See Self-Regulatory Principles for Online Behavioral Advertising*, FEDERAL TRADE COMMISSION 47 (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (calling upon "industry to redouble its efforts in developing self-regulatory programs, and also to ensure that any such programs include meaningful enforcement mechanisms."). For examples of industry self-regulatory efforts of this type, *see* TRUSTE, http://www.truste.com/ (last visited Apr. 25, 2012); *BBB Accredited Business Seal for the Web*, BETTER BUSINESS BUREAU, http://www.bbb.org/us/bbb-online-business/ (last visited Apr. 25, 2012); ANTI-SPYWARE COALITION, http://www.antispywarecoalition.org/ (last visited Apr. 25, 2012).

[§§§§§§§] For example with respect to P3P see, Lawrence Lessig, "The Architecture of Privacy,"; Jason Catlett, "Open Letter 9/13 to P3P Developers" (Junkbusters, 1999), online, Internet, 15 Oct. 2003; Deirdre Mulligan, Ari Schwartz, Ann Cavoukian, and Michael Gurski, P3P and Privacy: An Update for the Privacy Community (Center for Democracy and Technology, 2001), online, Internet, 19 Oct. 2003; and, Karen Coyle, A Response to "P3P and Privacy: An Update for the Privacy Community" (Center for Democracy and Technology, 2000), online, Internet, 19 Oct. 2003. With respect to the Tracking Protection working group see papers submitted to the first workshop on the issues expressing a wide range of views http://www.w3.org/2011/track-privacy/papers.html compliance.[********] Second, by preparing member organizations for their future legislative commitments, the better codes of conduct can then anticipate legislation. If the content of the rules is reasonably close, and if they have been attended by some genuine efforts at implementation throughout the organization(s), then they till the ground, reducing the disruption caused by legislation. Some of the codes of practice developed in Canada in the 1990s, such as those by the Canadian Banking Association and the Canadian Marketing Association, operated to prepare member organizations for imminent regulation. When PIPEDA was then introduced, these associations could allay the concerns of their members and, at the same time, convince them that statutory rules would limit "free-riders" which can undermine incentives to participate and erode public confidence.[††††††††] Once PIPEDA established the rules, however, the industry association codes became less relevant and most have now atrophied.

In other countries, codes of practice play a more explicit role in the regulatory regime. In countries such as the Netherlands or New Zealand, they operate to both implement and supplement legislation (see below). They can include explicit guidance on how, in a particular sector, the requirements of the law should be interpreted and implemented. And they may also supplement those requirements in some key respects. The level of detail provided in the enacted legislative scheme may determine the extent to which existing codes continue to play a role in shaping industry behavior and whether new codes are developed. The level of policing and the size of penalties for breach may also influence the extent to which industry actors seek out the greater certainty and uniformity provided by detailed codes. Legal systems that provide less clarity about acceptable implementations but heavy sanctions may encourage industry to agree upon implementation rules as a way to hedge against uncertain enforcement. On the other hand, ambiguous mandates with weak oversight or limited penalties may not encourage such collective efforts to manage risk. The isomorphism of practice cultivated through code generation may be of greatest benefit to large or high-profile industry players as their practices are likely to receive heightened scrutiny.

[********] In Canada, for instance, a multi-stakeholder process convened under the Canadian Standards Association built upon existing codes and fashioned a national standard on privacy protection, which ultimately constituted the framework for PIPEDA.

[††††††††] Colin J. Bennett, "Rules of the Road and Level-Playing Fields: The Politics of Data Protection in Canada's Private Sector," *International Review of Administrative Sciences,* Vol. 62, No. 4, December 1996.

Codes of Practice and other Policy Instruments

Businesses publish a diverse range of privacy materials. There is no canonical naming system for these documents. A range of imprecisely defined terms circulates around the privacy policy network to describe these various non-legal instruments used to develop, adopt, and implement privacy-related obligations. Public and private organizations might develop different types of documentation to state their privacy policies, or communicate them to employees, regulators, customers, clients and others. Significant efforts have been made in recent years to develop short notice privacy policies to provide accurate, but at the same time accessible, statements of commitment. But can any documented attempt at self-regulation be described as a code of practice? We think not, and believe that it is important to reserve the label of a code of conduct to self-regulatory policy instruments that have some particular characteristics.

If these instruments are to have wider statutory or evidentiary value under a legislated regime, it is essential to distinguish the Privacy Code (with a large 'C') from the other diverse material that is published by business on privacy, including the operational guidelines that are communicated to employees to remind them of their obligations, and the briefer statements of policy provided to the public.[‡‡‡‡‡‡‡‡]

Codes of conduct should thus be codified. They should be more than a set of public relations pledges or statements of good intention. They should of course contain a set of commitments, typically organized around a version of the fair information principles (FIPS) although we have argued elsewhere that FIPS alone is insufficient guidance in some areas.[§§§§§§§§] Codes of practice or conduct should entail guidance about practice and conduct. They should, therefore, be inward as well as outward looking. Codes of conduct are not only statements of "what we do", but also "how we do it." That entails internal privacy management and accountability. Privacy policies, of the kind automatically generated by privacy policy generators for websites, do not constitute codes of practice.

In *The Governance of Privacy,* Bennett and Raab distinguished between privacy codes of practice based on the scope of application:[*********] organizational, sectoral, functional, technological and professional. Many privacy codes have been developed by discrete public and private organizations over the years. Many of

---

‡‡‡‡‡‡‡‡ See, Bennett, *Implementing Privacy Codes of Practice,* pp. 64-5. And an important distinction emphasized in the guidance from the New Zealand Privacy Commissioner.

§§§§§§§§ Deirdre K. Mulligan and Jennifer King, "Bridging the Gap between Privacy and Design," forthcoming University of Pennsylvania Journal of Constitutional Law Summer 2012 (arguing that platforms should be informed by other concepts of privacy including contextual integrity (Nissenbaum) and boundary regulation (Altman)).

********* Bennett and Raab, pp. 155-159.

the earlier examples came from larger multi-national companies, such as American Express, Equifax and Readers Digest and predated the widespread use of the Internet for electronic commerce. Some of these are still in existence, and are applicable. Rarely, however, have privacy codes been developed by small or medium sized enterprises. For some reason and at some point, the standard terminology for the instrument governing the online collection of personal information became the "privacy policy." Arguably, the privacy policies of companies like Google, Facebook and Microsoft aim to achieve the same goals as the company codes of conduct of earlier eras. Where companies operate in the international arena, they have also encouraged to develop "Binding Corporate Rules" (BCRs) to apply the same set of privacy standards and processes to the personal information captured by any of the company's entities anywhere in the world.

Some privacy codes have been conceived and developed at a sectoral level. Some sectors are relatively easy to distinguish when they are related to administratively and legally determined set of regulatory institutions and rules. Others are more fluid. Where one sector begins and another ends is increasingly difficult to determine. No economy has ever been neatly divided into sectors. National and international trade associations, whose role is typically that of lobbying and representation have also been expected to offer policy guidance to their members in many areas of economic activity, including privacy. Some associations have a relatively inclusive membership and can therefore rely on a level of compliance that might exclude free riders; banking codes of practice are the clearest example. In the privacy arena, sectoral codes have been developed nationally and internationally with varying degrees of success for banking, insurance, marketing, telecommunications, cellular providers, health and many others.

Some codes of practice cut across these traditional sectors and activities and are better defined in functional terms. The most typical example is marketing. Codes of conduct have been developed by national marketing associations in the United States, Canada, the UK and elsewhere, as well as by the Federation of European Direct Marketers (FEDMA) in Europe. Codes for marketing have also been developed by the Mobile Marketing Association (MMA) to cover "advertisers, aggregators, application providers, carriers, content providers, and publishers, (collectively, "Mobile Marketers"), so that they can effectively, and responsibly, leverage the mobile channel for marketing purposes."[††††††††††] The Network Advertising Initiative's (NAI) Code of Conduct is probably the most important self-regulatory instrument applying to online behavioral advertising.[‡‡‡‡‡‡‡‡‡] Marketing cuts across many other sectors, and yet entails

[††††††††††] http://www.mmaglobal.com/policies/code-of-conduct
[‡‡‡‡‡‡‡‡‡] http://networkadvertising.org/Principles.pdf

some functionally specific issues that require special consideration and rule making.

Codes might also attend the application of particular technologies. There were early examples of codes of practice for electronic fund transfers and smart card technologies. A more recent example is a British code for the "Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment.[§§§§§§§§§§] There have also been several national efforts to develop a code of practice for the use of Radio Frequency Identification Devices (RFID) in the product supply chain, based on global guidelines promulgated by EPCGlobal.[**********]

A final category of codes applies to specific professions, especially those engaged in information-processing activities, such as computer professionals, librarians and survey researchers.[††††††††††] Others have been developed for professions in the medical and health field.[‡‡‡‡‡‡‡‡‡‡] Privacy rules tend to embedded in more general codes of ethics for many professional associations. Their enforcement also occurs at an individual level. Where membership of that association is a condition for participation in the profession, a range of professional disciplinary procedures can reinforce enforcement.

Codes of conduct might also be distinguished from privacy standards, a label which should be reserved for instruments to which organizations might be certified or registered. Standards imply not only a common yardstick for measurement and comparison, but also a process through which organizational claims about adherence to those norms can be objectively tested. There are now a range of standards, issued through the International Standardization Organization (ISO), which entail privacy obligations; those in the ISO 27000 series on information security are probably the most well known. The logical corollary of any standard is a mark or seal indicating that the organization has successfully gone through a conformity assessment procedure. But privacy seal programs, in and of themselves, are not codes of conduct, either.

Codes of conduct might also be distinguished from privacy impact assessments (PIAs) which are specific and prospective assessments of the privacy implications of a "project, programme, service, produce of other initiative which involves the processing of personal information and, in consultation with

---

[§§§§§§§§§§] http://www.dft.gov.uk/publications/body-scanners-interim-code-of-practice/

[**********] *Radio Frequency Identification (RFID) in Retail Consumer Privacy Code of Practice* at: http://www.gs1.org/epcglobal/public_policy/fact_sheets/epc_overview

[††††††††††] Code of Ethics of the American Library Association at: http://www.ala.org/advocacy/proethics/codeofethics/codeethics; Council of American Survey Research Organizations, CASRO Code of Ethics and Standards for Survey Research at: http://www.casro.org/codeofstandards.cfm

[‡‡‡‡‡‡‡‡‡‡] An example is the privacy code of the Canadian Medical Association: http://www.cma.ca/privacy stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts."[§§§§§§§§§§] PIAs are a decisional tool that can be used to facilitate implementation and adherence to a code of conduct with respect to specific projects etc. The consensus position in privacy professional circles would suggest that use of PIAs be a mandatory component of operationalizing a code. Ideally the PIA is used to assess impacts and risks in terms that are broader than legal compliance. They should be process, rather than output, oriented. And they should entail a systematic effort to determine and manage legal, reputational, economic and social risk. But they are also secondary instruments, and reliant upon an existing set of privacy norms. They are not normative instruments themselves. That, at least, seems to be the general consensus of the literature on PIAs, even though many do not live-up to the ideal.[***********]

We suggest, however, that the term code of conduct should really be reserved for instruments that can be applied collectively by multiple organizations. The scope might be defined on a sectoral, functional, technological or professional level. But the common and contemporary usage suggests that a code of conduct must potentially apply to more than one organization. That usage is also implied in the contemporary US context.

The term "codes of practice" or "codes of conduct", we suggest, should be reserved for those instruments that are:

- Codified according to the most appropriate national and/or international privacy standard
- Broader than either the short or long form privacy policy that appears on the website
- Directed both internally to employees and externally to the public and regulators
- Broadly applicable to more than one organization
- Clear as to scope and application.

The Relation of Privacy Codes to Privacy Law

Peter Hustinx, former President of the Dutch DPA, once argued that codes of practice do offer some clear advantages even within a legislated data protection regime. At their best, codes bring a level of specificity and sophistication to the

[§§§§§§§§§§] David Wright and Paul de Hert (eds). *Privacy Impact Assessments* (Springer, 2012), p. 5.

[***********] See, *Privacy Impact Assessments: An International Study of their Application and Effects* (Report for the UK Information Commissioner, 2007) at: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf implementation of privacy in practice. The procedure of negotiating codes enhances the understanding of the privacy problem within different sectors. It also allowed his office to gain a better appreciation of the relevant privacy issues and directly to influence the process of self-regulation. Codes are more flexible instruments than legislation and once negotiated can be adapted to changing economic and technological developments. Codes also allow organizations to publicize their privacy policies and to remove suspicions about the improper collection, processing and dissemination of personal data. They allow an "enhanced measure of understanding on both sides."[†††††††††††] Similar advantages have been noted by Canadian analyses of the subject.[‡‡‡‡‡‡‡‡‡‡‡] However, codes play varying roles in legislative regimes depending on their actual and perceived legal force. Some are merely exhortatory; others have varying roles within the legal system with evidentiary value during investigative processes.

The early versions of European data protection legislation, with the exception of the UK and Ireland, tended to omit references to codes of practice, and were generally not seen as consistent with the more detailed regulation of private conduct through the civil code legal systems. The 1995 *EU Data Protection Directive* did, however, provide:

> 1) The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
>
> 2) Member states shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member states shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.[§§§§§§§§§§§]

[†††††††††††] Peter Hustinx, "The Use and Impact of Codes of Conduct in the Netherlands," (paper presented to the 16th International Conference on Data Protection, the Hague, 6-8 September 1994), p. 3.

[‡‡‡‡‡‡‡‡‡‡‡] Bennett, *Implementing Privacy Codes of Practice,* p. 51; Lola Fabowale, *Voluntary Codes: A Viable Alternative to Government Legislation* (Ottawa: Public Interest Advocacy Centre, May 1994).

[§§§§§§§§§§§] EU, Data *Protection Directive*, Article 27.

Similar wording is included in the newly published Draft Regulation, which is beginning its passage through the European legislative process.[************] Current European data protection laws should, have transposed these provisions in a variety of ways.[††††††††††††] However, they tend to be infrequently applied in countries other than the UK.

In countries outside Europe, codes of practice are mentioned as desirable instruments that the DPA might encourage. Under Canada's PIPEDA, for instance, the only mention of codes of practice is in the context of specifying the powers of the Office of the Privacy Commissioner one of which is to "encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10."[‡‡‡‡‡‡‡‡‡‡‡‡] No codes of practice have been developed as a result of this provision, although a few that predate PIPEDA remain in existence. This is somewhat ironic, given that the very privacy principles inherent in PIPIEDA were negotiated as a self-regulatory code of practice under the auspices of the Canadian Standards Association (CSA).[§§§§§§§§§§§§]

In Australia, much hope was placed in the development of codes of practice when the 2000 Privacy Act was passed. Codes were seen as a crucial element in the system of co-regulation under the oversight of the Australian Privacy Commissioner. Detailed guidance about code development and submission was promulgated in 2001.[*************] Properly constructed codes, when approved, were supposed to supplement compliance with the National Privacy Principles: "The co-regulatory approach offered by the legislation allows for some flexibility in how organisations approach their privacy obligations but, at the same time, ensures that minimum enforceable standards apply to the protection of personal information." The scheme envisaged each code to be overseen by an independent "code adjudicator" to whom complaints would be addressed first for resolution, and before involvement from the Privacy Commissioner. So far only four codes have been approved by the Australian Privacy Commissioner,[†††††††††††††] one of which (on insurance) has been revoked, and another of which (on biometrics) is under challenge.[‡‡‡‡‡‡‡‡‡‡‡‡‡] A further code submitted by the

[************] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[††††††††††††] See Hirsch, Dennis D., The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? (February 8, 2011). Seattle University Law Review, Vol. 34, No. 2, 2011 (discussing codes of conduct as pursued in various EU member states).

[‡‡‡‡‡‡‡‡‡‡‡‡] Canada, Personal Information and Electronic Documents Act, Sec. 24c.

[§§§§§§§§§§§§] Canadian Standards Association, Model Code for the Protection of Personal Information (Rexdale: CSA, 1995).

[*************] Privacy Commissioner of Australia: http://www.privacy.gov.au/materials/types/guidelines/view/6482

[†††††††††††††] http://www.privacy.gov.au/business/codes/register

[‡‡‡‡‡‡‡‡‡‡‡‡‡] http://www.privacy.org.au/Papers/OAIC-BiomCodeRevoc-120321.pdf

Internet Industry Association is currently under consideration.

The system for negotiating and promulgating codes of practice is spelled out in greater detail in the New Zealand *Privacy Act* than in any other law.[§§§§§§§§§§§§§] A detailed guidance note from the Privacy Commissioner has also supplemented these provisions.[**************] The crucial aspect of the New Zealand approach is that codes of practice negotiated under the *Privacy Act* have the force of law. A breach of a ratified code of practice is as serious as a breach of the information privacy principles expressed in the law, triggering the complaints and enforcement procedures in the legislation. According to the Privacy Commissioner the codes might restate the principles and provide for "specific departures, procedures, standards or exceptions. Or a new set of rules can substitute for the principles. Either way there must be a rule or standard against which a complaint can be measured. The purpose of a code of practice is to increase relevance, certainty, precision and clarity, not to substitute some other language which might create uncertainty."[††††††††††††††]

Several codes have been issued under the New Zealand scheme, the most important of which are in the areas of telecommunications, health and credit reporting, each of which has been amended and updated in recent years. Some have been revoked. Others are issued on a more temporary basis, such as that which allowed personal information sharing during the state of emergency caused by the Christchurch earthquake.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Each is affixed with the "Seal of the Privacy Commissioner" to signify that the code is consistent with the *Privacy Act*, and was developed in accordance with its procedures.

A slightly more flexible regime exists in the Netherlands. The original Dutch law of 1988 was the first European data protection statute where codes of practice were given an explicit legislative role. The revised law of a decade later states the following: "An organisation or organisations planning to draw up a code of conduct may request the Data Protection Commission to declare that, given the particular features of the sector or sectors of society in which these organisations are operating, the rules contained in the said code properly implement this Act or other legal provisions on the processing of personal data." Moreover, "the Commission shall only consider requests where, in its opinion, the requester or requesters are sufficiently representative and the sector or sectors concerned are

---

[§§§§§§§§§§§§§] New Zealand *Privacy Act* 1993, Sections 46-53 at: http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

[**************] New Zealand Privacy Commissioner, *Guidance Note on Codes of Practice under Part VI of the Privacy Act,* December 5, 1994.

[††††††††††††††] New Zealand Privacy Commissioner, *Guidance Note on Codes of Practice*, December 5, 1994: http://privacy.org.nz/guidance-note-on-codes-of-practice-under-part-vi-of-the-privacy-act/

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡] http://privacy.org.nz/codes-of-practice/

sufficiently precisely defined in the code.[§§§§§§§§§§§§§§]

Accompanying guidance from the Dutch DPA explains that "codes of conduct are a means of allocating the responsibility for the details of the standards for protecting personal data within society. The law provides the general standards, rights, obligations, procedures and sanctions. Next, the general standards are worked out into specific standards by specifying codes of conduct for a particular sector." It goes on to state "a great deal of confidence is placed in codes of conduct. Therefore, the Dutch DPA carefully tests the code of conduct against article 25 Wbp [Dutch Data Protection Act]. Among other things, this involves the correct interpretation of the law, a careful description of the sector, the representativeness of the organization that prepares the code of conduct and the guarantees of independence in the settlement of disputes." The Dutch DPA is willing to cooperate and give advice during the process of code development.[***************] However, the codes are not formally binding on the courts. Certainly if an organization can prove that it has met the requirements of its code, then it will have a strong case in any proceedings. Conversely, if a complainant can demonstrate that the provisions of the code have been breached, then this constitutes *prima facie* evidence of liability under the law. Codes then tend to have indirect, rather than direct, legal effect in the Netherlands.

Similar powers are granted to the British Information Commissioner under the 1998 *Data Protection Act.* The Commissioner shall: "(a) where he considers it appropriate to do so, encourage trade associations to prepare, and to disseminate to their members, such codes of practice, and (b) where any trade association submits a code of practice to him for his consideration, consider the code and, after such consultation with data subjects or persons representing data subjects as appears to him to be appropriate, notify the trade association whether in his opinion the code promotes the following of good practice."[†††††††††††††††] Section 52 permits the Commissioner to lay before Parliament any code of practice, which has happened once with respect to a code of practice on data sharing. The Commissioner explained the legal status as follows:

> The Information Commissioner has prepared and published this code under section 52 of the Data Protection Act. It is a statutory code. This means it has been approved by the Secretary of State and laid before Parliament. The code does not impose additional legal obligations nor is it an authoritative statement of the law. However, the code can be used in evidence in any legal proceedings, not just proceedings under the DPA. In determining any question arising in proceedings, courts and tribunals must

[§§§§§§§§§§§§§§] Netherlands Data Protection Act, Article 25: http://www.dutchdpa.nl/Pages/en_wetten_wbp.aspx

[***************] http://www.dutchdpa.nl/Pages/en_ind_cbp_taken_gedrag.aspx

[†††††††††††††††] UK Data Protection Act 1998, Sec. 51(4) take into account any part of the code that appears to them to be relevant to that question. In carrying out any of his functions under the DPA, the Information Commissioner must also take into account any part of the code that appears to him to be relevant to those functions.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡]

Where codes are not laid before Parliament, the legal status is a little less clear, as for example with a 2009 code relating to Privacy Notices. Here the Commissioner only stated that "I will take its standards into account when, for example, I receive a complaint that information has been collected in an unreasonable way."[§§§§§§§§§§§§§§§] This seems to be the status of the other codes developed over the history of the British Data Protection Act, first passed in 1984. British Commissioners are generally careful not to "endorse" codes, in the fear that their provisions might come into possible conflict with the legislation. The first Data Protection Registrar tended to "welcome" them as offering helpful guidance to employees, thus reducing the need for regular intervention from the staff of the office.[****************] He also rejected the notion that detailed statutory codes should be prepared for each sector and that compliance with the codes would replace compliance with the law: "The great effort required to define sectors and develop precise codes in fine detail would, in my view, divert resources from encouraging compliance with the powerful and flexible principles."[††††††††††††††††]

To summarize, codes of practice/conduct therefore play a role under a variety of regulatory conditions. They may influence the proceedings of the courts and those of other regulatory agencies. More specifically, the relevant DPA may:

1) Encourage codes of practice
2) Encourage and give advice about the contents of codes of practice
3) Encourage, give advice and check codes of practice for conformity with the relevant legislation
4) Encourage, give advice, check for conformity and provide a stamp of approval
5) Take them into account during investigations and proceedings
6) They must take them into account during investigations and proceedings
7) They may draft them if industry fails to[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡]

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] ICO, Data Sharing Code of Practice (ICO, 2011) at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx
[§§§§§§§§§§§§§§§] ICO, Privacy Notices Code of Practice, 2009: at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf
[****************] UK Data Protection Registrar, *Third Report* (London: HMSO, 1987), p. 9.
[††††††††††††††††] UK Data Protection Registrar, *Fifth Report* (London: HMSO, 1989), p. 238.
[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] See Hirsch supra at 477-78 discussing Irish and UK law which allow the Data Protection Authority to draft codes of conduct for industry in some instances.

With this analysis in mind, what has been the history of privacy codes of practice in the United States, and what model is being contemplated under current policy?

PRIVACY CODES OF PRACTICE IN THE US

Self-regulatory codes of practice, as we have defined them, have played a limited role in the U.S. As discussed below, the heavy reliance on self-regulation, evolutions in U.S. corporate privacy structures to more firmly incorporate privacy, and increasingly aggressive external scrutiny by a range of players would seem sure to predispose the U.S. private sector to these instruments. But our examination finds limited, and primarily strategic and defensive use of such codes—more to avoid legislation or supplement the application of vague standards in a way that shelters industry practice from outside scrutiny.

More recently however, the U.S. has seen a rise in multi-stakeholder initiatives around privacy. Developing codes of practice or best practices is a key component of these initiatives. Tied to their multi-stakeholder structure they also seek to support information sharing and learning among participants. They have also both intentionally and indirectly informed the policing activities of regulators. However, these initiatives have a decidedly different motivational bent from self-regulatory codes. While a defensive catalyst (staving off some form of government action) may contribute to industry involvement, it is not the sole motivator. In fact, both initiatives discussed below have an affirmative agenda to contribute to sounder regulatory approaches to advancing privacy protections. More significantly, as discussed below, these initiatives fill regulatory gaps in instances where politics or legal authority left relevant legal institutions hamstrung—at least temporarily.

The Favorable Conditions

Several factors would appear to predispose the U.S. to privacy codes. Consistent reliance on self regulatory mechanisms to protect privacy, the rise of privacy professionals in the private sector, and increasingly active and aggressive policing through regulators and the courts would ostensibly incentivize industry to clearly signal attention and competence by creating and adopting codes. Yet despite these factors, codes of conduct, as defined above, have played a limited role in US privacy policy.

Several key privacy reports and monographs, published in the 1970s, that contain in depth examinations of sectors of U.S. private industry make no mention of industry or sectoral privacy codes.[§§§§§§§§§§§§§§§§] Similarly, a detailed study of privacy activities in seven U.S. private companies in the 1990s makes no mention of industry or sectoral codes. [*****************] Most recently, a qualitative study involving nine U.S. companies found extensive sharing of approaches, policies and practices among chief privacy officers, which was often facilitated by professional associations and trade associations, but little reference to industry or trade association codes of practice as an influence on company policy and practice.[†††††††††††††††††]

The limited use of codes is surprising given the U.S. landscape. Repeated deference to the private sector would seem to favorably dispose industry toward these instruments.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Further, the emergence of the Chief Privacy Officer and recent explosion in their numbers[§§§§§§§§§§§§§§§§§] would suggest that

---

[§§§§§§§§§§§§§§§§] Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission (July 1977) US GPO, (created by the Privacy act of 1974 to study individual privacy and record keeping in the public and private sector and to consider whether elements of the Privacy Act should be extended to entities other than executive agencies of the federal government and make recommendations to protect privacy); Databanks in a Free Society: Computers Record-Keeping and Privacy, Computer Science & Engineering Board, National Academy of Science (1972) Quadrangle Books (analyzing the role of databanks in modern society and implications for civil liberties); Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems US Dept. of Health, Education & Welfare (1973) MIT Press (studying impact of record keeping activities on citizen-state relationship with focus on Dept of HEW, now Health and Human Services; key report leading up the drafting and passage of the U.S. Privacy Act of 1974); James B. Rule, Private Live and Public Surveillance: Social Control in the Computer Age (1974) Schocken Books Inc. (documenting collection and use of information on individuals in public and private sector including banking and credit).

[*****************] H.Jeff Smith, Managing Privacy: Information Technology and Corporate America (1994) UNC Press (in depth qualitative study of information handling practices and policies in seven organizations.

[†††††††††††††††††] Kenneth A. Bamberger, and Deirdre K. Mulligan, "Privacy on the Books and on the Ground," Stanford Law Review, Vol. 63, pp. 247-316, January 2011, and Kenneth A. Bamberger, and Deirdre K. Mulligan, "New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry," Law & Policy, Vol. 33, Issue 4, pp. 477-508, 2011 (both reporting on qualitative study of operationalization of privacy in corporate sector within nine corporations).

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] See, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems US Dept. of Health, Education & Welfare (1973) MIT Press (key report leading up the drafting and passage of the U.S. Privacy Act of 1974 that called for legislation of private sector in specific areas); Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission (July 1977) US GPO, (calling for …); William J. Clinton & Albert Gore, Jr., "A Framework for Global Electronic commerce," 4 (1997) (promoting self-regulation as the preferred approach to protecting online privacy); FTC reports, etc.

[§§§§§§§§§§§§§§§§§] See Kenneth A. Bamberger, and Deirdre K. Mulligan, "Privacy on the Books and on the Ground," Stanford Law Review, Vol. 63, pp. 247-316, January 2011 (discussing rise of Chief Privacy private governance tools commonly used in other jurisdictions would flourish. U.S. CPOs use a range of tools to define and embed privacy within their organizations, yet codes do not appear to be in common use in most sectors. Bamberger and Mulligan describe rampant information sharing among the cohort of Chief Privacy Professionals interviewed—consistent with what one would expect based on past research—which was explained by the interview subjects as key to "demystifying privacy"[******************] in the face of regulatory ambiguity, there was little direct talk of industry-wide codes as a driver of firm behavior.

Increased development and reliance on industry wide codes of conduct would be a logical outgrowth of a legal environment sporting a relative lack of prescriptive law, and a rising and relatively activist privacy regulator with a broad and flexible authority (the FTC). In these circumstances codes might have been expected to provide shelter from inconsistent and unmanageable court and regulatory interpretations. Where the regulatory framework is uncertain and regulators are sending mixed signals, firms often gravitate towards similar institutional forms, shared policies and practices and strategies of engagement to manage risk.

Codes of conduct help reduce risk in several ways. Where the legal environment is uncertain industry wide codes assist firms in keeping their heads down, facilitating an isomorphism across both policy and practice that can shield them from regulatory action.[††††††††††††††††††] Codes can also provide a tool that allows industry to engage regulators and others—civil society, media, academics—in a conversation about pros and cons of general privacy protection principles while shielding actual company practices from scrutiny. Codes can assist industry in separating the wheat from the chaff in a systematic way that can facilitate the identification of outliers for enforcement and legislative scrutiny, as well as shaming and isolation by industry itself.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Finally, in disputes about the sufficiency of industry behavior under broad legal standards common in consumer protection—deceptive, unfair, reasonable—adherence to a shared

---

Officers); and, Zeinab Karake Shalhoub, "Analysis of Industry-Specific Concentration of CPOs in Fortune 500 Companies," Communications of the ACM April 2009 vol. 52 no. 4 (discussing variation across industries of CPOs) and Privacy on the Books discussing rise of CPOs, privacy professionals generally, and privacy professional organizations).

[******************] Privacy on the Ground at 131

[††††††††††††††††††] See, e.g., Kenneth J. Arrow, Uncertainty and the Welfare Economics of Medical Care, 53 AM. ECON. REV. 941, 947, 965 (1963) (describing how physician professionalism was an intermediating "nonmarket social institution" that compensated for uncertainty in the context of the severe information asymmetry between market actors); Lauren B. Edelman, Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law, 97 AM. J. SOCIOL. 1531 (1992) (discussing the importance of professional organizations in mediating legal ambiguity).

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] See the arguments by Hustinx above. See also, Bennett, *Implementing Privacy Codes of Practice* industry code can prove useful as a check on plaintiff and law enforcement construction of legal obligations.[§§§§§§§§§§§§§§§§§§]

The Chief Privacy Officers interviewed by Bamberger and Mulligan reported frequent and sustained collaboration with peers to share information about best practices, guidelines, and policies explained in part by the fact that privacy was viewed as less of a competitive issue among firms and more of an essential element of maintaining consumer trust and confidence within industry or an industry segment.[*******************] The scarce mention of industry privacy codes is interesting given the increasing importance of self-regulatory privacy efforts in recent years both domestically, and in political negotiations with the European Union. It may be readily explicable by the fact that the individuals interviewed were viewed as leaders in the field of corporate privacy and were arguably singled out by their privacy peers (including corporate, government, civil society, and academic) for their privacy management activities which likely exceed the baseline set by self-regulatory organizations.

Sectoral Codes

As discussed above, work in the 1970s suggests that codes of practice were not widely used in industry. During the mid-1980s activities and publications of Privacy and American Business, and its founders Professor Alan F. Westin—who was a Senior Consultant to the US Privacy Protection Commission—and Robert Belair, appeared to contribute to a proliferation of privacy policies at the institutional level and privacy codes at the sectoral level.[†††††††††††††††††††] Ronald Plesser, another private sector attorney and the former general counsel of the Privacy Protection and Study Commission, also worked with numerous companies and trade associations to draft privacy policies and codes. For example, the Direct Marketing Association (DMA)[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡], American Banking Association[§§§§§§§§§§§§§§§§§§§], and the Society of Human Resource Management[********************] developed codes or ethical frames to govern privacy during this time period. Other industry trade associations, such as the Cellular

---

[§§§§§§§§§§§§§§§§§§] See the arguments of Australian and British privacy commissioners above.

[*******************] Privacy on the Ground at 131-33. (explaining that sharing was good for industry because they were all somewhat joined in the public's eye "[t]hat's about doing the right thing because if they screw up . . . it screws up all of us.") Similar responses were found during interviews in Canada. The code of practice of the Canadian Bankers Association, for instance, has completely atrophied.

[†††††††††††††††††††] P&AB handbooks of company and industry U.S. privacy codes: from 1994 (168 pp), 1995 (130 pp.), and 1996 (148 pp.), along with P&AB commentaries opening each volume.

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] DMA's Guidelines for Ethical Business Practice

[§§§§§§§§§§§§§§§§§§§] http://www.aba.com/About+ABA/ABA_privprinpublic.htm

[********************] *Code* of Ethical and *Professional* Standards in *Human Resources, Society for Human Resource Management (2011) www.shrm.org/about/**code**ofethics/Documents/chapter-coe.pdf*

Telecommunications Industry Association,[††††††††††††††††††††] have issued best practice and guidelines documents. The majority of these codes were exclusively advisory. However some involve methods for policing and penalties.

In the mid-1990s in response to increased privacy activity at the Federal Trade Commission, pressure from the Clinton Administration, and pressure driven by the EU-US Safe Harbor negotiation to ease US business activity in light of the effective date of the EU Data Protection Directive with its prohibition on transferring EU members personal data to jurisdictions with inadequate protection, several self-regulatory privacy initiatives emerged.

TRUSTe[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡], the Better Business Bureau's online privacy program[§§§§§§§§§§§§§§§§§§§§], and the American Institute of Certified Public Accountants (AICPA) Web Trust program[********************] were formed to provide privacy rules to govern electronic commerce generally, while the Children's Advertising Review Unit developed a privacy program focused on providing a privacy code to address web sites targeting children. Unlike earlier trade association developed codes of conduct these initiatives set out procedures for assessments (typically company self-assessments with some level of review by the self-regulatory program personnel), provided mechanisms for identifying non-compliance (typically consumer or other third-party complaints), and established mechanisms to assist aggrieved consumers. The Online Privacy Alliance began in 1998 functioning more as an umbrella group for self-regulatory privacy activities than a developer of industry codes. In addition existing trade associations in relevant industries stepped up their privacy activities. For example, in 1999 the Direct Marketing Association, whose code of ethical practices has been around for many years, made compliance with the privacy principles a condition of membership.[†††††††††††††††††††††]

In addition, two sectoral self-regulatory codes emerged due to specific and intense regulatory scrutiny. In both instances the sector's data collection and use practices were viewed as particularly troublesome from the perspective of the

[††††††††††††††††††††] CTIA Best Practices and Guidelines for Location based Services http://www.ctia.org/business_resources/wic/index.cfm/AID/11300

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] http://www.truste.com/

[§§§§§§§§§§§§§§§§§§§§] BBBOnLine Privacy Program Created to Enhance User Trust on the Internet, June 22, 1998, http://www.bbb.org/us/article/bbbonline-privacy-program-created-to-enhance-user-trust-on-the-internet-163; http://www.bbb.org/us/bbb-accreditation-standards

[********************] http://www.webtrust.org/index.aspx

[†††††††††††††††††††††] Mark Hamstra, "DMA Announces Privacy Promise, Moves to Expel Members, Direct Marketing News," July 8, 1999 (discussing action against 17 DMA members who hadn't endorsed the Privacy Promise and the contents of the Promise which went into effect July 1, 1999, and appointment of a compliance coordinator to oversee testing program (mystery shopper) to check compliance). See also Mary J. Culnan and Robert J. Biew, "Consumer Privacy: Balancing Economic and Justice Considerations," Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 323-342, at 333-4 (discussing self-regulatory initiatives to adopt FIPS to internet).

U.S. market-based approach to privacy. The Individual Reference Services Group represented the data broker industry and developed a code of practice in response to pressure from the FTC. The Network Advertising Initiative represented online network advertisers. Each industry was viewed as unlikely to be responsive to traditional market pressures due to their lack of relationship with consumers whose data their business models relied on. Data brokers have no independent relationship with consumers, but rather gather data from public and private sources to create individual profiles that they than sell to support other entities' decisions about how to interact with an individual. Individuals have little knowledge of these entities, they have no control over whether their information resides in these companies' databases, and they have no ability to use voice or exit strategies to effect their policies and practices. Similarly, network advertisers are invisible to web users, and have no direct relationship with them. As with the reference service bureaus they are immune from traditional forms of consumer pressure—voice and exit.

The codes developed in response to FTC pressure were immediately viewed as weak and quickly became weaker due to the limited number of industry actors who committed to them. While the self-regulatory privacy programs have been criticized for lax implementation of FIPS, and lax oversight[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡], CARU's privacy program has been generally viewed as more successful. The latter may in part be due to the enactment of legislation addressing children's online privacy that provides a floor for its efforts.

Thus while the external environment in the US appears rather primed to foster a strong private sector movement to develop codes, they appear to be the exception not the rule and to arise only in response to rather pointed threats of regulatory intervention.

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Chris Jay Hoofnagle, "Privacy Self Regulation: A Decade of Disappointment," March, 4 2005 Electronic Privacy Information Center (overview of past studies and new data revealing failure of industry self-regulation to move practices toward compliance with FIPS); EPIC, "Surfer Beware II:Notice Is Not Enough," 1998 (reporting on survey of the privacy practices of 76 new members of the Direct Marketing Association and finding only 8 consistent with new DMA policies issued in 1997); Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," (2000) Washington DC (finding limited compliance with notice, choice, access, and security principles set out by FTC as essential to privacy self-regulation); Mary J. Culnan and Robert J. Biew, "Consumer Privacy: Balancing Economic and Justice Considerations," Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 323-342, at 338 (concluding that "self-regulation is unlikely to work 100% of the time as there will always be bad actors or organizations who have implemented the formal trappings but not the substance of fair information practices, creating a need for baseline privacy legislation…" but noting that due to dynamics of technical and market change "the voice of activists, government and the media will continue to play an important role in motivating the business community to self-regulate, while at the same time, leading the broader social conversation on the fair use of personal information at the national and global levels."); Pam Dixon, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation," November 2007, World Privacy Forum;

Multi-stakeholder Initiatives

More recently two multi-stakeholder initiatives have emerged to develop voluntary codes or best practices for particular industries. These efforts are distinct from self-regulatory codes in terms of the breadth of participation—including advocacy organizations, academics and other stakeholders—and engagement with the general public. While only one of these efforts has produced a code, under our definition, both are instructive on the issues concerning process and participation identified in the White Paper.

The Anti-Spyware Coalition, convened by the Center for Democracy & Technology in 2005, is a group of public interest organizations and "companies that design or distribute legitimate anti-spyware technologies."[§§§§§§§§§§§§§§§§§§§§§] The organization's mission is to craft consensus definitions and best practices to assist industry, regulators and consumers in efforts to eliminate spyware and other potentially unwanted technologies. The activities of the Coalition include the development of consensus definitions of spyware, best practices for assessing spyware by anti-spyware companies, process documents outlining testing and decisions about blocking and removal, guidance for resolving conflicts between software vendors around spyware related issues, and educational materials.[**********************]

The ASC does not require conformance with the Coalition's documents, nor police member companies' behavior. Nor does it certify anti-spyware companies, or offer seals or certifications affirming conformance with its various documents. Thus, unlike the self-regulatory seal programs discussed above, it does not demand compliance with a set of practices, it does not oversee or enforce compliance with its documents, and it does not directly assist consumers who have been harmed by spyware to obtain redress. Despite these limitations the ASC has provided some of the same benefits as a code. The shared definitions and practices developed by the ASC empowered the private sector to police itself and assist consumers in a manner perceived by the public, regulators, and other market players as legitimate.[††††††††††††††††††††††] In so doing it facilitated policing by regulators.

[§§§§§§§§§§§§§§§§§§§§§] http://www.antispywarecoalition.org/about/FAQ.html

[**********************] http://www.antispywarecoalition.org/documents/index.htm

[††††††††††††††††††††††] The evolution of private sector responses to spam was rife with concerns about illegitimate and unaccountable behavior. From the actions of the Real-time Black Hole list, which were herald by some and despised by others, that help close ports used to relay spam but also resulted in legitimate mail being suppressed, to actions by private companies such as AOL which at times resulted in blocking wanted messages—including time sensitive political messages—the spam debates were weighed down by a lack of shared definitions and commitment to transparent and accountable rules to guide identification and blocking.

It also improved the ability and consistency of industry self-policing. The existence of shared practices, standards, and approaches empowered anti-spyware vendors by limiting their potential exposure to legal claims—such as interference with competition and trade libel—by distributors or developers of blocked or removed software. The definitions, standards and best practices assisted anti-spyware companies in developing transparent processes and redress mechanisms to address concerns about arbitrary and unaccountable behavior further increasing the level of trust and legitimacy of the anti-spyware community, bolstering self policing of behavior and regularizing the behavior of self-help tools that further addressed privacy and security risks facing consumers.

Further, the ASC rubric provided a foundation for regulators and courts to use in policy making and enforcement. This proved particularly significant given the broad and flexible mandate of the FTC and state consumer protection agencies to protect individuals against deceptive and unfair practices. As the ASC documents reveal, whether a given product is spyware does not turn exclusively on the function of the product, but rather is informed by the disclosures, knowledge, expectations, context of use and processes. Thus, policing this market requires some subtle line drawing.

The consumer protection authorities—and consumers—benefit from the broad flexible enforcement authorities that allow them to evolve policy and enforcement strategies to meet ever-changing market place challenges. They are however, also wary of over-reaching, which can lead legislators and the public to question their legitimacy. In extreme instances it can imperil their funding.

In emerging markets where practices to be policed require nuanced line drawing, the existence of agreement among industry and civil society about appropriate rules of the road smooths the path for regulatory action by providing some insulation against claims of illegitimacy. The impact of the ASC in this respect can be seen very specifically in the FTC's action against Sears Holding Management Corporation for their "MY SHC Community."[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Despite a very detailed disclosure of the level of spying Sears would conduct on members of the MY SHC Community the FTC brought an action against them. While the spying was quite extensive and the disclosure rather abysmal, the terms of service agreement would quite likely have been found acceptable by a

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Decision and Order, Sears Holdings Mgmt. Corp., Docket No. C-4264, F.T.C. File No. 0823099 (Aug. 31, 2009), available at: http://www.ftc.gov/os/caselist/0823099/index.shtm court.[§§§§§§§§§§§§§§§§§§§§§§§] Some members of the private bar were outraged at the FTC's action stating that it, "flies in the face of established law."[***********************] Despite this extremely chilly reception from the private bar, industry did not aggressively push back. Sears behavior, which included downloading a program that ran surreptitiously in the background and transmitted information on the users' web browsing all across the web, including secure sessions—such as shopping carts, online application forms, checking accounts, and web-based email and instant messaging services—as well as information about the user's computer, was inconsistent with the ASC guidelines. Under the ASC's documents it was readily identifiable as spyware.

Industry wanted to distance itself from this sort of blatant over reaching and the ASC documents gave them a way to do so. Through regulatory actions addressing spyware the ASC process had contributed to narrowing the range of legitimate practices and interactions with users. It empowered regulators, but at the same time provided industry with time and detailed guidance about how to stay on the right side of the enforcement stick. So while having no independent oversight and policing function it has played a significant role in policing.
The role of the ASC guidance—code like, though not "a code"—identifies a fifth role that codes can play: they can empower regulators by legitimating the line-drawing necessary in many enforcement actions.

More recently the Global Network Initiative (GNI) has emerged to address threats to privacy and freedom of expression in the information and communication technology sector. Formed in 2008, GNI is a multi-stakeholder initiative including companies, civil society, socially responsible investing firms, and academic institutions. It set out to craft an enforceable code of conduct for the information and communication technology (ICT) sector on privacy and freedom of expression issues. As companies sought to expand into markets with limited commitment to protecting privacy and freedom of expression in practice, the international community called on them to protect users of their services from government actions. In several instances companies were faced with public relations, shareholder, and legal actions based on their failure to provide such protection.

GNI set out to create a code that would bind industry to protect the privacy and freedom of expression interests of the users in the face of country actions to interfere with them. The ICT companies needed the capacity to push back on, or at least regularize, government conduct that was inconsistent with government obligations under international human rights agreements. They needed the help

[§§§§§§§§§§§§§§§§§§§§§§§] Alan Charles Raul, Edward McNicholas, Colleen Theresa Rutledge, and Adam Rusnak, *End of the Notice Paradigm?: FTC's Proposed Settlement Casts Doubt On the Sufficiency of Disclosures in Privacy Policies and User Agreements*, 8 PVLR 1070 (2009)
[***********************] Id.

of civil society and other stakeholders to do so in a thoughtful and credible way. They needed stakeholder participation for political legitimacy. The principles after all bind the companies to be less helpful to government requests for content removal and data access. They don't prohibit responsiveness to either in any specific case, but they leverage the companies to drive rule of law and human rights principles on the ground.

This is a novel alignment of actors for corporate social responsibility (CSR) initiatives. Typically such initiatives arise where civil society and government actors view the corporation as under delivering on its legal obligations. Such dynamics have produced codes of conduct in the garment, child labor, and other areas. These codes are best viewed as preemptive self-regulation under the Hustinx taxonomy. They stave off legislation. The GNI in contrast represents an alignment of civil society and corporate actors. Unlike the earlier CSR codes, there was no credible threat of legislation. Congress held hearings and introduced legislation. However, the complicated inter-governmental and trans-governmental dimensions of this issue made it exceedingly unlikely that a law would be agreed to and enacted. The likelihood of government action in other countries was even less likely. Governments would have to give up some of their authority to access data and determine the instances compatible with their international human rights obligations.

Simply put, governments are not today—nor in the future—going to agree to limit their own jurisdiction with respect to accessing data, including personal information, they believe relevant to addressing a crime, national security, public health or safety issue domestically. While they may choose to develop technical solutions to address publicly accessible content they view as objectionable—filters, dns poisoning, among others—they will continue to lean on companies to police hosted content that is not publicly available and more importantly demand the personal information of internet users.

Government action is the problem, and the code while being developed to bind corporate behavior is in truth better understood as an effort to indirectly regulate government behavior to make inconsistencies with human rights more transparent and more difficult. Thus we add a sixth role for corporate codes to the Hustinx taxonomy—to indirectly regulate government action. A review of the GNI principles and implementation guidelines will see that many of the guidelines bind the corporations to require governments to interact with them in a manner more consistent with rule of law and human rights.

The ASC and GNI efforts arise in areas where the impact of globalization is felt. The GNI was a response to inconsistent and incomplete legal frameworks that allowed companies to behave in ways that were incompatible with the laws and norms of their home country and in a manner contrary to human rights. In this context the global scope of a self-regulatory code is compelling, as it binds corporations globally, not jurisdictionally. Given the political and practical barriers to meaningful legislation and regulation of spyware and interactions between governments and ICT actors, these multi-stakeholder responses are of heightened value.

Conclusion: International Lessons for US Policy

There is a very strong tendency in US policy-making to proceed from an assumption of American exceptionalism. It is commonly believed that the political, constitutional, administrative and cultural differences between the US and other liberal democracies are so wide that the drawing of policy lessons from international experience is futile at best, and dangerous at worst.[†††††††††††††††††††††††] This thinking permeates policy-making in the privacy area as well. As the only advanced industrialized state without a comprehensive legal framework for the protection of personal data in public and private sectors, on the surface the US would seem to be similarly "exceptional."[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡]

This portrait is only partially true, however. The United States is "different"; the question is whether those differences should make a difference. The European theory of data protection is not essentially different from the US theory of information privacy. Both were developed at around the same time (the late 1960s and early 1970s), and both drew lessons from the other.[§§§§§§§§§§§§§§§§§§§§§§§] And the "fair information principles" upon which virtually every personal data protection statute is based are, to some extent, of US origin.[************************] Furthermore, there is considerable variation in privacy protection regimes in the rest of the world. This policy sector, like so many others, does not easily lend itself to simplistic classifications of models of privacy governance, as it perhaps did back in the 1980s. The picture today is rather one in which a complex range of regulatory, self-regulatory and technological policy instruments circulates around a truly global policy community and appears in different mixes everywhere. US policy-makers, advocates and experts are very much a part of that community.

[†††††††††††††††††††††††] Rose, Richard, *Lesson-Drawing in Public Policy: A Guide to Learning Across Time and Space*, (Chatham, NJ: Chatham House, 1993).

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] A recent survey by Graham Greenleaf counts 89 countries with data protection laws. "Data privacy laws in 89 countries and counting," *Privacy Laws and Business* February 2012.

[§§§§§§§§§§§§§§§§§§§§§§§] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992)

[************************] US Department of Health Education and Welfare, *Records, Computers and the Rights of Citizens* (Washington DC: HEW, 1973)

Codes of conduct are one of those instruments. They play a similar set of functions in the US as in other societies. The multi-stakeholder initiatives we surveyed have shown some alternative roles for codes. While not necessarily exclusive to multi-stakeholder processes, they appear more likely to fill those roles in a compelling way when they are so produced. Based on our review of privacy codes internationally and recent multi-stakeholder initiatives we believe it is useful to consider them in the broader landscape of modalities of new governance. Below we offer from some initial thoughts.

Considering the potential roles codes of practice play (to avoid law, anticipate law, implement law, supplement law, and more recently we suggest to empower enforcement activities, and to indirectly regulate government action), the codes developed under the Administration's proposal can be viewed as tools to empower enforcement under existing regulatory frameworks, to anticipate congressional action, and to implement the CPBR. The Administration appears to have joined the broader consensus that company or sectoral codes alone are an insufficient response to the troubling levels of personal surveillance in contemporary societies. Codes of conduct are not here used as a strategy to avoid privacy legislation, as they perhaps were in the 1980s and 1990s, but rather to move the agenda forward given that the Administration cannot control the lawmaking process.

Through the proposed process the Administration disassembles traditional roles of governance along several lines. It involves new players in crafting the rules—delegating to the private sector while broadening it by requiring non-industry actors to have an equal place at the table. The Administration continues the trend of involving the private sector in the development of policy by delegating the creation of specific implementation rules.[††††††††††††††††††††††††] However unlike past delegations, here the Administration is delegating not to industry—as generally occurs in the standard setting environment—but to a so-called multi-stakeholder group that it seeks to breath into creation through the force of its bully pulpit, its call to Congress to enact legislation, and by the appeal to industries' own interest.

On the interest side there is of course the potential to temper future legislation through a code that anticipates the legislative goals and perfects manageable modes of implementation. And there is always the possibility the participation in an effective MSH code development process that yields a safeharbor from action at the FTC will encourage Congress to leave a specific industry out of the legislative equation all together. However, the call on industry to work through these MSH working groups in this context is likely aided by a stick only lightly wielded in the White House Privacy paper, but which is in reality quite formidable. The US, several other countries, many civil society groups, and

[††††††††††††††††††††††††] See Bamberger;

industry have been pushing the use of MSH as venues for working out policy issues related to the Internet in global debates.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] These players have a pressing need to prove that MSH—beyond those more tightly tied to technical standards—are effective *and* preferable along a set of dimensions that other countries, civil society actors, and industry players find compelling. Such dimensions will include global interoperability of the outcomes, scalability, participation, and time to development, all of which are flagged in the Privacy paper. Thus the need to affirmatively and aggressively practice what they preach on the global stage lurks in the background herding industry actors, who might otherwise do nothing in the hopes of staving off regulation at least until the outcomes of the next election are known. Like other "new governance" models the code process situates the government in the role of convening or information pooling, while placing non-governmental actors in the role of experts.

The complicated interactions between the DOC process, and the FTC processes and enforcement actions have the potential to produce a fluid dynamism between policy and law and between modes of regulation. Through MSH activities they will hopefully prod the development of codes aligned with that policy. Significantly the FTC and other state, national and international agencies are anticipated participants in these processes. Once produced, a code will act as binding law—despite the absence of legislative action—where companies commit to adhere to them. The FTC has undisputed authority to enforce the codes terms under its existing authority. It has clarified this ability, and more, over the past 15 years specifically in the areas of information privacy and security, both offline and online.

However, while the FTC has indicated that it will be favorably disposed to codes, it is not bound to view them as ensuring practices that are fair and non-deceptive.[§§§§§§§§§§§§§§§§§§§§§§§§] Thus, they will create a floor, but not a ceiling with respect to regulators' expectations of industry behavior concerning consumer privacy. This blurring of policy, law, and enforcement is an element of new governance. In this instance the two forms of law at play—one specific the other ambiguous—can act as a check against lackluster codes or codes that languish as technology and business practices race forward. The stick of FTC action based on its general authority can be used to exert healthy pressure on the initial MSH process, but more importantly be used to ensure ongoing attention, updating,

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] For background on this increasingly heated debate about Internet governance see,

[§§§§§§§§§§§§§§§§§§§§§§§§] This is either the best or worst of both worlds. If a law was passed it would no doubt, as the Administration's recommendations to Congress do, create a process for establishing a safeharbor to protect companies complying with a code that had gone through an APA like notice and comment process, against enforcement actions. Without a law industry will have codes, but still risk FTC action.

and improvement. The process mixes modalities and forms in interesting, complicated, and novel ways across two agencies.

We believe the proposed process creates opportunities for privacy and consumer organizations who will have additional opportunities to spur discussions, new mechanisms to facilitate information flows from industry to the public, and the ability to push for binding codes while retaining the option of pressing regulators to more generally protect consumers through enforcement actions. Recently, these agencies have evidenced strong coordination and collaboration, yet have maintained their ability to think and act independently. We believe this too will create a healthy tension that will keep both agencies mindful of the primacy of the consumer interest at stake in the outcomes.

Privacy advocates will determine for themselves whether to be involved in the MSH process. Whether Congress acts to protect privacy[************************] or not, the multi-stakeholder processes that NTIA is proposing to start could contribute to improvements in privacy protection in several ways. Examining the FTC's activities starting in the 1990s through today, Bamberger and Mulligan found them to be important to moving businesses forward on privacy. Whether one conducts a head count of the number of privacy organizations that appeared as the FTC created an ongoing forum to discuss their perspective on privacy, their research findings, their views on market trends, and their critiques of industry practices, or one looks at the progress made through the constant drumbeat of privacy stories picked up by the press, or the years of settlements, cases, guidance, and regulations that have centered information privacy and security as core consumer protection issues in the digital age, the FTC's emergence in this field was a watershed event for privacy. The MSH process will bring additional resources to specific areas, contexts and sectors for purposes of code development.

This analysis admittedly views the glass as half full rather than half empty. But any reasonably positive assessment does need to be tempered by the evidence of international experiences. The early enthusiasm for codes of practice has waned in countries that initially introduced them into their data protection regimes in the 1980s and 1990s. In none of the countries have codes of conduct performed as central features of the data protection regime in question. While the 1995 EU Directive, and the new EU Draft Regulation, prompts member states to encourage their development, the uptake has been very slow. It is quite instructive, therefore, that codes of conduct rarely get a mention in the

---

[************************] We believe congressional action is inescapable, but the timing is a complete unknown. It is completely possible that a year of NTIA activities will have companies running to Congress to save them with legislation, or to create an even playing field across markets as codes ramp up. Regardless, we believe legislation in some form is ultimately inevitable. However, we also believe its an open question whether privacy will fare better or worse as a result.

contemporary literature about the governance of privacy. To some extent, other similar instruments of self-regulation have overtaken codes of practice: privacy impact assessments, privacy accountability frameworks, binding corporate rules, and short and long form privacy policies. To some extent, the advent of the Internet has been accompanied by a strong sense that the privacy problems are different, and thus the policy tools need to be different as well. Beyond these factors, there are some inherent dilemmas with integrating codes of practice into any regulatory regime.

First, there appears to be a central dilemma with the use of codes of practice within systems that have any kind of comprehensive framework privacy protection law. If a relevant regulatory authority does not formally endorse them, then they may contain language that conflicts with the wording of the law, and confusion about applicability and enforcement might ensue. If a more formal ratification process is laid out, then (as in New Zealand, Australia and the Netherlands) this can lead to the bureaucratization and lengthening of a process that, in theory, is supposed to allow for the flexibility of self-regulation, and an ability to adapt to changing economic and technological conditions.

In the U.S. the interaction between the consumer protection authorities and any legislation Congress enacts, and the MSH codes will require clarity. Currently the Administration is relying on the FTC to enforce codes of conduct against companies who choose to be bound by them under Section 5 of the FTC Act.[†††††††††††††††††††††††††] It is also imaginable that the FTC will rely on them, as they have relied on the ASC documents, in their broader enforcement actions. The codes could inform the FTC's perspective on acceptable marketplace practices and provide a baseline against which the FTC and other consumer protection agencies can police a sector regardless of participation in the code. As discussed above, this sort of baseline can free the FTC from concerns about potential pushback in light of their ambiguous regulatory framework. This may be particularly important in new markets where consumer expectations are not easily tethered to past environments and experiences in the market.

Second, the development of codes in some sectors is often hindered by competition within sectors, and by unclear boundaries and overlaps that weaken the claim that the association submitting the code is sufficiently "representative." The ability to control free-riders, and the effectiveness of voluntary codes, is greater where there are fewer industry players representing a majority of the economic activity within a sector, and where they are generally aware of each others' behavior. In general free-rider problems grow as the number of actors, which are necessary for effective action, increases. Where there is a history of effective and regularized cooperation in other areas, non-compliant behavior can

[†††††††††††††††††††††††††] White Paper at 32 be recognized, isolated and more effectively punished.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] This incoherence and overlap is only exacerbated by the recent rise of online commerce and the advent of a variety of new business models that do not fit traditional categories. For example, if a bank sells an insurance product online, which code of practice should apply – that on banking, insurance or online marketing? And under which of these codes, should a consumer complain?

In the US context, code development is expected to focus on particular sectors or contexts, many of which are associated with the digital economy. A key motivator for this work is responding to the growing problems associated with consumer surveillance both online and offline as technology increasingly mediates, enhances and monitors physical space. The NTIA's policy initiative is almost premised on the assumption that the boundaries to the network of "stakeholders" who might engage in code development are inherently fluid and porous. This is no doubt true, and no doubt a conundrum. The examination of self-regulatory initiatives in the online environment and critiques of them highlight several of the problems facing the NTIA as it structures this process. For instance, the online advertising continues to shed its skin—companies change names, are bought and sold, and reemerge. While the companies change so do the tools of the trade. No sooner has discussion started on one and potential solutions identified when the next stealthy tracking device seeps into the market. Codes have been most effective where there is a stable group of players who view themselves as having a shared set of problems. Whether this means a shared set of data to protect, or a shared set of regulators to appease doesn't matter much for this point, but it obviously matters greatly overall. The frenetic online advertising market seems like a difficult one to corral. The constantly shifting technical landscape poses an additional challenge.[§§§§§§§§§§§§§§§§§§§§§§§§§§] While the technical churn can be addressed, it requires broader, more forward thinking, which may not come naturally to businesses uncertain if they will be a going concern when the code is complete.

Third, codes of conduct can, therefore, be confusing to the consumer in a number of respects. The relation between codes can be vague, and the relationship between the code and the law is often unclear, for any consumer who is seeking redress or to exercise access and correction rights, for example. The data subject rarely knows the difference between a code, which has received the approval of the DPA, and one that has not. Regardless of the regulatory framework within which codes are situated, they invariably suffer from the perception that they are inherently "voluntary"; subtle distinctions between the varieties of self-

---

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Bryne Purchase, "The Political Economy of Voluntary Codes," in K. Webb, *Voluntary Codes*, pp. 81-82.

[§§§§§§§§§§§§§§§§§§§§§§§§§§] Generally codes should not be tethered to a specific technology—although as mentioned above some are narrowly so and designed to set cross industry guidelines for the use of the technology in the market.

regulation and co-regulation are therefore lost on the average person. In the public mind, self-regulation means that those responsible for implementation are the very organizations that have a vested interest in the processing of the personal data in the first place.

For all these reasons, the community of DPAs has tended to look skeptically on codes of conduct. For this community, codes continue to have a "voluntary" ring to them. Many DPAs are therefore often suspicious that efforts to develop codes to build sectoral flexibility into the interpretation of law are also veiled attempts to weaken regulatory standards. The community of privacy advocates harbor similar, and often stronger, suspicions. [**************************]

However, suspicion also resides within the corporate sector. In countries like Canada and Australia where codes of practice played an important role in engagement and education before law was passed, they have now receded into the background. Legal compliance becomes the dominant motivation after law is passed. The opportunity costs for self-regulatory initiatives recede. This pattern is perhaps especially noted in those regimes based on an "ombudsman" model. The complaints-driven regime can produce a "let's wait and see whether anyone complains" attitude in the business sector, and reluctance to spend resources on self-regulatory initiatives.

The US policy community should be aware of the limitations of codes of conduct that have been exposed in other countries. The American regime is not exceptional, but struggles with very similar dilemmas that have been addressed elsewhere. US policy choices also have consequences beyond American borders, to the extent that US multinational online companies may be brought into this policy framework. Our review suggests that privacy codes of conduct, while out of favor in many regimes, remain a useful policy instrument, but only within the context of a strong regulatory framework, only when they are broadly constructed through processes that include a broad range of non-corporate actors, only when they scale to all relevant actors within a defined sector, and only when the relevant regulator has the means and will to exercise its legal powers.

[**************************] Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008), pp. 130-131.