**In Search of the Holy Grail:
Achieving Global Privacy Rules**

**Through Sector-Based Codes of Conduct**

Dennis D. Hirsch

Geraldine W. Howell Professor of Law

Capital University Law School

303 E. Broad Street

Columbus, OH 43215

dhirsch@law.capital.edu

(614) 558-0997 (c)

(614) 236-6685 (o)

The movement of personal data across national borders is fundamental to the Internet economy.[[1]](#footnote-1) Yet the laws that govern such data flows remain national or, at best, regional.[[2]](#footnote-2) This mismatch creates a number of related problems. It makes it difficult to track and enforce compliance as personal data moves rapidly and unpredictably from one legal jurisdiction to another.[[3]](#footnote-3) It increases costs and risks for businesses that must track, and seek to comply with, a wide variety of privacy laws. [[4]](#footnote-4) And it creates tension and political strife between major trading partners, such as the U.S. and the E.U., whose differing approaches to privacy law threaten to disrupt data transfers across their borders.[[5]](#footnote-5) The Department of Commerce has identified the conflict between global data flows and national or regional laws as one of the most significant problems facing privacy law and policy today, explaining that “[d]isparate approaches to commercial data privacy can create barriers to both trade and commerce, harming both consumers and companies.”[[6]](#footnote-6)

At first blush, the answer to these difficulties would seem to be a clear one: develop a single, global set of privacy rules that is applicable in all jurisdictions. That would provide enable business to comply in a cost-effective way; make it easier for governments to enforce, and individuals and privacy advocates to track, this compliance; and facilitate economically vital data flows among nations. But how to achieve this? An international treaty, setting legally-binding privacy requirements for the globe, seems impossibly out of reach.[[7]](#footnote-7) Industry self-regulation, while perhaps more feasible, has been sparse and unsatisfactory in its implementation and, in any event, cannot promise legal compliance.[[8]](#footnote-8)

International policymakers and practitioners seem to be gravitating towards a third option: enforceable, mutually recognized, industry codes of conduct.[[9]](#footnote-9) This approach comes in a number of varieties, though they all follow the same general approach. National jurisdictions establish general principles for how companies should handle and protect personal information.

Individual companies then develop a privacy code of conduct that meets the legal requirements of a number of these national jurisdictions. A designated authority, endorsed by all of the participating nations, reviews the code. If the authority finds that the code does, in fact, meet the relevant requirements, it approves the code. The participating nations then treat firms that comply with an approved code of conduct as being in compliance with their respective laws. They bring enforcement actions against firms that claim to comply with a code, but fail to do so. Structured in this way, the approved code functions as a unified, enforceable, international set of privacy rules. Three initiatives currently employ codes of conduct as a way to create cross-border privacy rules: Binding Corporate Rules (BCRs);[[10]](#footnote-10) the Asia-Pacific Economic Cooperation forum’s Cross-Border Privacy Rules (CBPRs);[[11]](#footnote-11) and the U.S.-E.U. Safe Harbor Agreement.[[12]](#footnote-12) Business and regulators have been investing in these programs and view them as a way harmonize privacy laws in a world of widely disparate legal regimes.

This article argues that each of these programs contains a fundamental flaw: each relies on codes created at the level of the *individual firm*. This feature renders the code of conduct approach impractical for most companies, expensive for governments to administer and enforce, and difficult for stakeholder groups to track and monitor. The article identifies an alternative approach—*sector-based* codes of conduct (i.e. codes created at the level of the industry sector, rather than at the level of the individual company)—and explains why it avoids the problems just mentioned and holds the most promise going forward. It then examines the current legal landscape and sets out the reforms required in order to implement, and achieve the full benefit of, international, sector-based, codes of conduct.

The article proceeds as follows. Part I describes the huge growth in international data flows, the ways in which they conflict with national and regional privacy laws, and the challenges that this creates for privacy protection, commerce, and international relations. Part II draws on regulatory theory to assess whether direct government regulation (i.e. treaties implemented by national laws), pure industry self-regulation, or enforceable codes of conduct are best suited to address this problem. In so doing, it sheds light on why policymakers and practitioners have become so focused on the code of conduct approach. Part III evaluates the current code of conduct initiatives – Binding Corporate Rules, APEC Cross-Border Privacy Rules, and the US-E.U. Safe Harbor Agreement. It explains that each of these initiatives focus on firm-based codes of conduct (i.e., codes negotiated at the level of the individual firm), and that this decreases their effectiveness. It argues that sector-based, cross-border codes of conduct would work much better. Part IV analyzes whether existing legal mechanisms can support cross-border, sector-based codes of conduct. It shows that many of the necessary pieces are already in place. It identifies the legal reforms that will be needed to make this approach work and so move us closer to the Holy Grail of international data protection: clear, protective and effective global privacy rules.

**I. Global Data Flows, National Privacy Laws, and the Problems They Create for One Another.**

Technology leaps forward and changes social realities. The law evolves slowly to address these new challenges. For a time, there is a mismatch between technology and society on the one hand, and law on the other. Eventually, the law adapts to the new realities. This is an old story, repeated in many contexts.[[13]](#footnote-13) The rise of global data flows, and their conflict with slow-changing national and regional privacy laws, is this story on steroids. The establishment of the Internet, and the consequent increase in cross-border data transfers, has been dizzying in its speed, size and complexity. The disjunction between this rapidly expanding global data network, and the national and regional laws that seek to govern it, is profound and problematic.

* 1. Global Data Flows

The world wide web (www) is just that. It creates a global architecture for the transfer of digital data that does not respect national or regional boundaries.[[14]](#footnote-14) It should not be surprising, then, that the emergence of the Internet (and, subsequently, the Cloud) [[15]](#footnote-15) have exponentially increased the speed, and decreased the cost, of cross-border transfers of personal data. As Professor Paul Schwartz has explained, this has led to three, related changes in data processing.[[16]](#footnote-16)

First, it has increasingly made data processing into a cross-border affair. Prior to the rise of the Internet, most data processing data took place within the boundaries of a single nation. [[17]](#footnote-17) The transfer of data across national borders was “an occasional event, an exception and not the rule.”[[18]](#footnote-18) Today, cross-border data transfers are ubiquitous.[[19]](#footnote-19) The low cost of international data transfer has allowed companies to locate operations, and develop relationships with other businesses and customers, throughout the world. [[20]](#footnote-20) They then collect personal data from, and/or share data with, each of these individuals or entities.[[21]](#footnote-21) International data transfers and economic globalization build on and reinforce one another. Fast, cheap and reliable international data transfers support the growth of global business. Increased economic globalization, in turn, widens the demand for, and investment in, rapid and inexpensive cross-border data transfers. The upshot is an “exponentially increased . . . flow of personal information across national borders.”[[22]](#footnote-22)

The second important change has been the rise in data processing networks. Previously, most companies employed localized, central databases. Insofar as they transmitted data, they sent it from one centralized database to another.[[23]](#footnote-23) These were point-to-point transactions between two discrete databases. Today, many businesses participate in multi-point data processing networks.[[24]](#footnote-24) An example would be a multi-national company that utilizes a third-party vendor for its personnel recruitment.[[25]](#footnote-25) Company offices located around the world send job postings to the vendor. Recruitment agencies, individual applicants, and current employees (making recommendations) located in many different countries send applications and other personal information to the vendor, which shares it with the HR departments at the multi-national firm and at its various locations.[[26]](#footnote-26) The company may request additional information, leading to another round of multi-point data transfers. This network of data flows involves many different entities, located in different countries, in a complex stream of data transfers. Such networks, which are increasingly common today, result in a nearly constant flow of personal information across national borders[[27]](#footnote-27) and have resulted in “a massive growth in the complexity and volume of these transfers.” [[28]](#footnote-28) Nothing like this was possible prior to the Internet.

The third change is the shift from discrete, one-time data transmissions, to far more dynamic, ongoing transfers of personal information. In an earlier era, a company would prepare for an international transfer of personal data and then implement it at a single, pre-defined point in time. [[29]](#footnote-29) These were “static” [[30]](#footnote-30) events in the sense that they took place, and then they ended. Currently, cross-border data transfers take place on demand, continuously, and in real time. [[31]](#footnote-31) They are “dynamic” [[32]](#footnote-32) in the sense that they can occur at any given moment, have no discrete ending point, and are often difficult if not impossible to predict in advance.[[33]](#footnote-33) An example would be a technology company that has set up support centers in India, Costa Rica and Bucharest. When a customer contacts the company, the firm uses an algorithm based on factors such as time of day and customer location to determine which service location should handle the contact.[[34]](#footnote-34) It then gives that center access to the customer’s personal information and directs the customer to it.[[35]](#footnote-35) The result is an international flow of personal data relating to customer service calls that is context-dependent, “extremely dynamic and cannot necessarily be predicted in advance.”[[36]](#footnote-36)

In sum, the rise of the Internet has exponentially increased the volume of international transfers of personal data. [[37]](#footnote-37) It has also changed the nature of these transmissions from transfers that were generally local, point-to-point, and discrete, into global data flows that are increasingly cross-border, networked, multi-point, continuous and dynamic.[[38]](#footnote-38)

* 1. The Conflict between Global Data Flows and National Data Protection Laws

 Democratic nations broadly agree on the core privacy protections that should apply in the commercial sphere. [[39]](#footnote-39) The Organization for Economic Co-Operation and Development’s (OECD) widely-endorsed list of Privacy Principles is the best reflection of this consensus.[[40]](#footnote-40)

The important differences between national systems occur, not with respect to these broad principles, but in how countries interpret and apply them. [[41]](#footnote-41) Examples abound. Some nations define “personally identifiable information” (PII) more broadly than others.[[42]](#footnote-42) Some exclude certain types of personal information, even if it falls within the definition of PII. Countries disagree on what constitutes adequate notice so that “data collectors [may not be able to] use the same notice for residents of different jurisdictions.”[[43]](#footnote-43) Nations differ as to the meaning of meaningful choice, and as to when choice can be opt-out, and when it must be opt-in. The European Union requires companies to notify the data subject of their data collection activities, and the data protection authorities of their data processing operations.[[44]](#footnote-44) The United States does not. Nations also differ significantly in the execution and enforcement of their divergent privacy laws.[[45]](#footnote-45) Some, such as the E.U. nations, have omnibus privacy laws. Others, such as the United States, use sectoral laws.[[46]](#footnote-46) Some provide more oversight and enforcement; some less.[[47]](#footnote-47) Some have active data protection authorities; some more passive DPAs; and some, such as the US, have no DPA at all.

These differences are particularly salient on the Internet where personal data is more likely to travel among a variety of legal jurisdictions and where these “[i]nternational data flows . . . [force] divergent data protection policies and rules to confront each other with ever greater frequency.”[[48]](#footnote-48) They cause major difficulties both for governments and individuals who wish to protect personal information as it travels across the globe, and for businesses that depend on the cross-border transfer of personal data.

1. Problems for privacy protection

The differences between national privacy regimes, combined with the explosion in global data transfers, pose a fundamental challenge for the protection of individual privacy. At the most basic level, a processor may move a person’s data from a jurisdiction with stringent and well-enforced privacy laws, to one with lenient and poorly enforced rules.[[49]](#footnote-49) Some companies may purposely operate this way in order to take advantage of “regulatory arbitrage.” [[50]](#footnote-50) Global data flows, combined with national privacy laws, can accordingly result in the migration of personal data to those nations with the weakest law or, at minimum, to temporary gaps in privacy protection as the data moves through such a jurisdiction.[[51]](#footnote-51)

Even where each of the relevant nations has implemented meaningful privacy laws, the cross-border nature of today’s data transfers make it difficult to track compliance with them. For example, the dynamism and unpredictability of global data flows make it difficult to tell where personal data are at any given moment, which entity is responsible for them,[[52]](#footnote-52) or which jurisdiction’s laws apply.[[53]](#footnote-53) This difficulty in establishing clear jurisdiction can, in turn, in inhibit enforcement,[[54]](#footnote-54) and make it hard for individuals to seek remedies for violations.[[55]](#footnote-55) The overall effect is to create “uncertainty and instability of the protection of individuals[’ privacy].”[[56]](#footnote-56)

1. Problems for business

The lack of consistency among national laws also creates significant problems for the businesses that engage in cross-border transfers of personal data and desire to comply with legal requirements.[[57]](#footnote-57) These companies must closely track the flow of their data in order to know which jurisdiction’s rules apply at any given moment. They must understand and monitor compliance with the privacy laws of each jurisdiction through which their data travels. Finally, they may need to seek multiple regulatory approvals for routine, cross-border data transfers.[[58]](#footnote-58) These tasks make it far more costly and burdensome to achieve compliance than it would be if companies were able to follow a single set of privacy rules throughout their data’s lifecycle.[[59]](#footnote-59) As the Department of Commerce has recognized, companies face “difficulties in complying with the multiplicity of foreign data protection rules and regulations.”[[60]](#footnote-60)

Differing privacy laws also confront business with uncertainty. Given the dynamism of global data flows, companies may find it impossible to predict where, and at what time, they will transfer data across borders and to comply with the relevant laws. In order to engage in such cross-border transfers they will need to face the risk of non-compliance and enforcement. In addition, conflicts between nations and/or regions with respect to the adequacy of their respective privacy laws can raise the prospect of data embargoes.[[61]](#footnote-61) The European Union considers US privacy law inadequate and may limit data transfers to the United States,[[62]](#footnote-62) although the relevant governments have managed to avoid this so far by means of the Safe Harbor Agreement and other understandings. Still, the prospect of a data embargo creates profound uncertainty for businesses that depend on the free flow of personal data across national borders.[[63]](#footnote-63) Such uncertainty can drive up the cost of capital, inhibit investment and innovation, and cause tension between international allies.

The difficulties that consumers face, and those that businesses confront, reinforce and build on one another. When consumers lose faith in the law’s ability to protect their personal information this can cause them to pull back from the online environment and from the businesses that are deeply enmeshed in it. This can, in turn, hurt the companies whose business models depend on a certain level of consumer trust and participation in the Internet economy.[[64]](#footnote-64) By the same token, companies that face increased compliance costs and uncertainties are likely to pass these costs on to consumers, insofar as they can. This can lead to higher prices for the goods and services that consumers would like to purchase. Further harmonization of national privacy laws could accordingly result in lower prices for consumers.[[65]](#footnote-65)

For all of the above reasons the jumble of inconsistent national privacy laws conflicts with the contemporary trend towards increasingly global data flows, and so poses a challenge to the continued growth and vibrancy of the Internet and of the global economy.[[66]](#footnote-66) The emergence of a unified set of privacy rules, on the other hand, would diffuse this threat and provide benefits both to consumers and to industry.[[67]](#footnote-67) The Department of Commerce has called for “a new global framework for privacy protection that will decrease the cost of doing business globally, provide consumers with consistent levels of protection worldwide, and contribute to global economic growth.” [[68]](#footnote-68) The question is: how to achieve this?

**II. Regulatory Options**

Regulatory theory identifies three basic types of regulation: direct regulation, self-regulation, and co-regulation.[[69]](#footnote-69) In direct regulation, government creates rules, monitors compliance with them, and enforces them.[[70]](#footnote-70) In self-regulation, industry takes on these roles.[[71]](#footnote-71) It writes its own rules; monitors company compliance with them; and sanctions those industry members that fail to comply. Co-regulation stands in between direct and self-regulation. It encompasses those initiatives in which government and industry expressly and intentionally share responsibility for the drafting, monitoring, and/or enforcing of rules.[[72]](#footnote-72) Enforceable codes of conduct--in which government provides the broad requirements, companies draft codes that flesh out and implement this framework, and regulators assess whether the code properly interprets the government requirements—involve significant government-industry cooperation and are an example of co-regulation.[[73]](#footnote-73) Cross-border privacy rules could follow any of these three regulatory approaches. Before settling on co-regulatory codes of conduct, it is important to explore how direct or self-regulation would work.[[74]](#footnote-74)

1. Direct Regulation

To establish cross-border privacy rules through direct regulation, participating countries would first adopt a treaty or convention establishing international privacy requirements. Each ratifying nation would then promulgate national laws and regulations that closely tracked the international template, and would enforce these requirements against companies in their jurisdiction. In such a way, direct, government regulation would establish uniform, cross-border privacy rules.

The strengths of such an approach would be those commonly associated with direct regulation. Governments would likely establish relatively uniform, socially-protective sets of rules. The uniformity would make it easier for regulators to monitor compliance with, and to enforce, these rules.[[75]](#footnote-75) It would also create a level playing field for business.[[76]](#footnote-76)

Direct regulation would also face important obstacles and present significant downsides. The first obstacle is a practical one. It is extremely difficult to establish an international treaty of any sort. This task becomes even harder when the treaty in question would address an issue, such as privacy, as to which there are deep cultural and regional differences.[[77]](#footnote-77) It is one thing to set out a broad set of privacy principles, as the OECD has done, and get a variety of nations to sign on to them. It is quite another to negotiate a detailed treaty establishing concrete privacy requirements and convince countries to ratify, implement and enforce them. Practical difficulty is one of the major downsides of a direct regulation approach. It is may explain why there have been no serious attempts to create such a treaty.

Even if it were possible to impose cross-border privacy rules through direct regulation, regulatory theory suggests that this may not be the optimal approach for this particular area. Direct government regulation works better in some contexts than in others. It can do a good job of regulating slower-moving areas of the economy that pose significant risks to the public. The regulation of toxic pollutants from manufacturing operations would be one such example.[[78]](#footnote-78) However, direct government regulation is not well-suited to areas, such as privacy regulation, where the technologies and business models change rapidly and continuously.[[79]](#footnote-79) In these situations, it is difficult for government officials to know enough about the industries in question to craft intelligent rules that account for business realities. Moreover, government regulation’s lengthy time frame (e.g. notice-and-comment rulemaking) often fails to keep pace with fast-moving technological and business changes. [[80]](#footnote-80) Business realities end up ‘lapping’ the government rules intended to regulate them, rendering these rules out-of-date or even obsolete.

1. Self-Regulation

It is for these reasons that some consider self-regulation to be the best approach to privacy governance.[[81]](#footnote-81) They maintain that self-regulation, which comes from industry itself and so is able to tap into business knowledge, is more likely to produce intelligent and effective rules than government regulation.[[82]](#footnote-82) They further argue that self-regulatory bodies, which do not need to comply with notice-and-comment procedures and other legal requirements, should be able to update their rules far more quickly than government regulators can.[[83]](#footnote-83) Self-regulation should therefore do a better job of keeping pace with rapidly evolving technological and business realities. Finally, proponents of self-regulation maintain that companies, which often resist government-imposed rules, will be more likely to accept rules that they and their peers have drafted.[[84]](#footnote-84) Self-regulation will accordingly promote greater industry buy-in and compliance.

Companies can use self-regulation to establish cross-border privacy rules. Indeed, this has already occurred in at least two contexts. Some multi-national corporations establish corporate privacy policies designed to meet legal requirements in all the jurisdictions in which they operate, and require each of their units to comply with them.[[85]](#footnote-85) This is a form of cross-border privacy self-regulation at the level of the individual firm.

In 2000, the International Commerce Exchange (ICX) sought to do the same thing on a much broader scale. It drafted a privacy code of conduct designed to meet the requirements of the E.U.’s 1995 Data Protection Directive.[[86]](#footnote-86) It hoped to convince officials at the level of the European Commission that the code constituted “adequate” protection for the purposes of the Directive, and to have them approve it.[[87]](#footnote-87) With such approval in hand, companies from any economic sector of the economy that complied with the code could transfer E.U. citizens’ personal information to any location in the world without running afoul of the adequacy requirement.[[88]](#footnote-88) Such companies would still have had to comply with the privacy laws of the non-E.U. countries to which they were sending the data. But for the purposes of the E.U. adequacy requirement, the ICX code would have provided companies with a single, cross-border set of privacy rules that would have allowed them to transfer data anywhere in the world. As it turned out, ICX was never able to obtain European approval of its draft code.[[89]](#footnote-89) The ICX project therefore stands today as an example of industry self-regulation, rather than as one of industry-government co-regulation.

The fact that few today know about the ICX project demonstrates one of the weaknesses of self-regulation as a method of establishing global privacy rules. Self-regulation, by definition, does not involve formal government approval. As a consequence, it neither provides the legal safe harbor that companies need to engage confidently in cross-border data transfers, nor absolves firms from the costly duty of having to track and comply with multiple national privacy laws. For these reasons, it does not really address the mismatch between global data flows, and national data protection laws. It does not solve the problem. That may be why few companies have adopted the ICX, self-regulatory code.

Regulatory theory suggests additional reasons to be cautious about self-regulation.

Business has an incentive to draft self-regulatory rules that appear to offer solid protection but are not, in fact, very stringent. Self-regulation accordingly tends to be more lenient than government requirements, and may not achieve public goals like privacy.[[90]](#footnote-90) Theory further predicts that self-regulatory organizations will lack the incentive rigorously to monitor and enforce rules against the very member organizations that provide them with financial support.[[91]](#footnote-91)

There is some evidence for this in the privacy area.[[92]](#footnote-92) It appears that self-regulation, like direct government regulation, may not be the best vehicle for establishing cross-border privacy rules.

1. Co-Regulation

The foregoing may explain why policymakers are focusing so heavily on co-regulation.

Proponents of co-regulation argue that it combines the advantages of self-regulation with those of direct regulation. Like self-regulation, co-regulatory methods such as enforceable codes of conduct allow industry to draft the specific privacy rules (e.g. the codes). They therefore draw on industry knowledge and expertise in much the same way that self-regulation does.[[93]](#footnote-93) They are also more likely to get industry to accept and buy-in to rules that they or their peers have drafted.[[94]](#footnote-94) Like direct regulation, co-regulatory strategies generally call on government to establish the privacy framework to which all industry-drafted rules must conform. They also get regulators involved in assessing, monitoring compliance with, and enforcing, these rules.[[95]](#footnote-95) This government involvement increases the chances that the rules will truly protect the public interest, and that companies will comply with them.[[96]](#footnote-96) In sum, co-regulation promises rules that are stringent, intelligent and up-to-date, that government enforces and industry accepts. This is an attractive picture for an area like privacy law where technologies and business models change too quickly for direct regulation, but the stakes are too high to rely solely on industry self-regulation.

Co-regulation also has weaknesses. It envisions a government-industry negotiation over rules. Such regulation through “deal-making” can lead to sweetheart deals that favor industry interests over those of the public.[[97]](#footnote-97) Much depends on how well the government regulators are able to exercise their authority (the company needs their approval, after all) and push back against company desires for more less rigorous rules. Public interest stakeholders can counter industry influence. Including them in the discussion can increase the chances of a well-balanced set of rules.[[98]](#footnote-98) Another weakness is that co-regulation can sometimes provide certain companies with an advantage over others. Insofar as the approach allows individual companies to draft their own codes of conduct and negotiate them with the regulators, this could lead to some companies having more advantageous arrangements, and some less.

Finally, co-regulation may be less nimble and adaptive than self-regulation. In self-regulation, industry can develop, update and change its rules all on its own. It does not need government approval to do so. In co-regulation, industry and government generally invest significant time and resources to reach agreement on a set of rules. This often makes them hesitant to re-open negotiations in order to update the rules. In at least one important example of privacy co-regulation, the negotiated industry codes of conduct largely remained unchanged over their five-year initial term.[[99]](#footnote-99) Government and industry negotiators reconvened to update the code only when the expiration of the code required them to do so.[[100]](#footnote-100)

**III. Current Initiatives**

Policymakers appear to believe that co-regulation’s strengths outweigh its weaknesses. The three leading cross-border privacy rule initiatives all employ co-regulatory enforceable codes of conduct. These are: Binding Corporate Rules (BCRs), APEC Cross-Border Privacy Rules (CBPR), and the US-E.U. Safe Harbor Agreement.

1. Binding Corporate Rules

Article 25 of the 1995 Data Protection Directive allows companies to transfer personal data from an E.U. Member State to a non-E.U. nation only where the laws of the non-E.U. nation “ensure[] an adequate level of protection.”[[101]](#footnote-101) This requirement can pose a significant obstacle for multi-national companies that that wish to transfer personal data between operations in the E.U. and those in countries that have not yet passed laws establishing “adequate” privacy protections.

Binding Corporate Rules (BCRs) provide a way to accomplish such transfers without violating the Directive.[[102]](#footnote-102) The multi-national company creates a legally-binding set of rules[[103]](#footnote-103) (which can take the form of a code of conduct) that, if followed, provide “adequate” protections for personal information. It commits that its entire corporate group—including its operations in non-E.U. nations—will be bound by, and will follow, these rules. It then submits these Binding Corporate Rules to a “lead DPA” which evaluates whether, in fact, the rules provide “adequate” protection.[[104]](#footnote-104) In making this assessment, the lead DPA consults with, and receives comments from, the DPA’s of other Member States in which the company operates.[[105]](#footnote-105) If, after receiving these comments, the lead DPA determines that the corporate rules do, in fact, provide an “adequate” level of protection, it approves them. The company can then transfer personal data among its various E.U. and non-E.U. operations so long as it does so in compliance with the approved rules. This is co-regulation in the sense that the company and the relevant DPAs work together to negotiate and craft the rules.

Binding Corporate Rules create legal safe harbor with respect to the Article 25 adequacy requirement. That is their key function. However, they do not necessarily create a safe harbor with respect to the data protection laws of specific E.U. Member States; nor do they necessarily do so with respect to the laws of the non-E.U. nations to which the company transfers the data.[[106]](#footnote-106) This limits BCR’s ability to create global privacy rules. Compliance with a set of approved BCRs ensures only that the company complies with the Article 25 adequacy requirement when it transfers personal information outside of the EU. It does not guarantee that the corporation is in compliance with the relevant national data protection laws.[[107]](#footnote-107) Thus, a company with an approved BCR must still undertake the costly task of complying with a variety of different data protection laws; and regulators, individuals and others seeking to evaluate that company’s compliance still face the uphill battle of determining which jurisdiction applies and whether the firm is in compliance with that particular set of laws. BCRs are further limited in that they are valid only within the corporate group for which the DPA’s have approved them. They do not cover transfers from members of that group to other entities outside the group.[[108]](#footnote-108)

B. APEC Cross-Border Privacy Rules

Companies in the Asia-Pacific region also seek to transfer data across national borders.

Asia-Pacific Economic Cooperation forum (APEC), an organization of twenty-one Asian and Pacific Rim countries that includes the United States, Canada, Japan, China, Russia, Mexico and Chile, among others,[[109]](#footnote-109) has developed a regulatory initiative to facilitate these transfers: The APEC Cross-Border Privacy Rules (CBPRs) initiative.[[110]](#footnote-110) As with BCRs, the APEC initiative relies heavily on co-regulatory codes of conduct.

The APEC approach is rooted in a set of Privacy Principles that all APEC member states have endorsed.[[111]](#footnote-111) A participating company prepares a code of conduct or other set of “cross-border privacy rules” that explains how the APEC Privacy Principles apply to its specific operations. It then submits this code to an APEC-approved Accountability Agent.[[112]](#footnote-112) The Accountability Agent, which may be a government body or an independent third-party, reviews the code to ensure that it properly fulfills the APEC Privacy Principles. If the Agent finds the code to be satisfactory, it approves it.[[113]](#footnote-113)

What exactly this approval means is not entirely clear. It does not provide the company with a safe harbor with respect to national laws. Even those companies with approved codes are still subject to the privacy laws of the individual APEC nations.[[114]](#footnote-114) That said, companies that follow an APEC-approved code of conduct can feel more comfortable than they otherwise would that their behavior complies with the laws of APEC member states or that, even if it turns out that they do not, these countries will not enforce their laws as harshly as they otherwise would. Thus, APEC privacy codes provide some comfort to firms that engage in cross-border transfers among APEC states. It remains to be seen whether this is sufficient incentive to encourage companies to develop an APEC privacy code, and whether such a system truly will facilitate cross-border data transfers.

C. The US-E.U. Safe Harbor Agreement

The US-E.U. Safe Harbor Agreement, too, uses company codes of conduct to address the cross-border data transfer issue. The U.S. Department of Commerce and the European Commission developed the Safe Harbor Agreement to respond to the 1995 Directive’s “adequacy” requirement which, once U.S. laws were deemed to be “inadequate,” promised to disrupt vital data transfers between to two trading partners.[[115]](#footnote-115) The Safe Harbor Agreement seeks to address this problem and facilitate cross-border data flows between the E.U. and the U.S.[[116]](#footnote-116)

The Agreement defines a set of principles—the Safe Harbor Privacy Principles—that both E.U. and U.S. officials agree approximate the requirements of E.U. data protection law.[[117]](#footnote-117) A company can then develop its own set of privacy and data governance practices—essentially, a code of conduct—that translates the Safe Harbor Principles and explains how the company will comply with them. Alternatively, it can join a “self-regulatory privacy program” that has an established set of such practices, and commit to following them.[[118]](#footnote-118) Individual companies self-certify to the Department of Commerce, and in their own posted privacy policy, that they are following such a code and are in compliance with the Safe Harbor Principles.[[119]](#footnote-119) So long as they meet this commitment, companies are deemed to provide “adequate” protection for the purposes of the 1995 Directive and can transfer personal data to and from the E.U. However, firms that fail to follow through are subject to FTC enforcement under Section 5 of the FTC Act for engaging in a “deceptive” business practice.[[120]](#footnote-120) Companies that fail to sign up for the Safe Harbor program altogether are deemed not to provide “adequate” protection and are, in theory, prohibited from processing the personal data of E.U. citizens.

The U.S.-E.U. Safe Harbor Agreement is similar in many ways to BCRs and APEC CBPRs. One salient difference is that, while the BCR and APEC CBPR initiatives currently allow only individual companies to develop code of conduct, the Safe Harbor program allows self-regulatory privacy programs to do so as well and to allow many different companies, from a variety of economic sectors, to “join” the organization and commit to complying with its set of practices.

D. The Current Initiatives are Flawed

The current initiatives—BCRs, CBPRs, and the U.S.-E.U. Safe Harbor Agreement—share some common virtues. They provide companies (and, in the case of the Safe Harbor Agreement, self-regulatory privacy programs such as TRUSTe) with a means to create an approved, cross-border set of privacy rules. And they do this through a co-regulatory mechanism that utilizes industry knowledge to produce intelligent rules. Each works only with respect to certain borders (for BCRs, the borders of E.U. nations; for CBPRs, those of APEC member nations; and for the Safe Harbor Agreement, that between the E.U. and the U.S.) and so none provides a truly global solution. Still, each takes an important step towards the goal of broadly applicable, cross-border privacy rules.

The three initiatives also suffer from the same, fundamental weakness: *they rely on individual companies, rather than industry sectors, to draft the cross-border privacy rules*.[[121]](#footnote-121) That is, they are company-based codes, rather than sector-based ones. This has a number of important drawbacks that those who promote and write about cross-border privacy rules do not appear as yet to have grappled with.

To begin with, it is expensive to write a comprehensive privacy code and negotiate it with the relevant authority. Only the largest and most sophisticated companies have the resources and expertise to do this.[[122]](#footnote-122) Small and medium –sized businesses, and even some large companies, will not be able to develop their own company-specific code of conduct that meets the requirements of the 1995 Data Protection Directive, APEC Privacy Principles and/or U.S.-E.U. Safe Harbor Agreement.[[123]](#footnote-123) As a consequence, only the largest and most knowledgeable companies will be able to take advantage of BCRs, CBPRs and the Safe Harbor Program (unless they participate in a self-regulatory privacy program, the drawbacks of which are detailed below.)[[124]](#footnote-124) The roster of companies that have successfully negotiated the BCR process bears this out. The list of 39 companies includes such firms as Accenture, American Express, British Petroleum, Citigroup, e-Bay, General Electric, ING Bank and Shell International.[[125]](#footnote-125) What of all the other companies that also transfer personal data between and among E.U. member states but cannot afford to draft and negotiate a BCR? They are left without a streamlined mechanism for compliance with E.U. “adequacy” requirements. The same can be said of APEC Cross-Border Privacy Rules, and of the U.S.-E.U. Safe Harbor Agreement insofar as it uses company codes of conduct.[[126]](#footnote-126)

Were more firms to become able to take advantage of “company-based” codes (so named because they are drafted and negotiated at the level of the individual company or firm), this would create another large problem—high administrative costs for regulators.[[127]](#footnote-127) Data Protection Authorities (in the case of BCRs) and government agencies serving as APEC Accountability Agents would have to review, negotiate and approve an individual code for every company that wanted to engage in an international data transfer. This would present a significant, possibly insurmountable, burden for these resource-strapped public bodies. The APEC CBPR program seeks to minimize this by anointing independent “accountability agents” to review and approve the codes. But this has a downside of its own in that, insofar as accountability agents are private rather than public entities, they may not sufficiently protect the public interest.

Company-based codes also suffer from another problem; they frustrate public participation and so reduce accountability. Privacy NGOs have even fewer resources than regulatory agencies. If a significant number of companies were to submit codes for the BCR or CBPR programs, or to self-certify compliance with a code under the Safe Harbor program, stakeholders would lack the resources to keep track of, much less participate in, the many submissions, negotiations and approvals.[[128]](#footnote-128) Company-specific codes will escape public scrutiny by overwhelming it with sheer numbers.

Of course, it may turn out that only a small number of companies have the resources and sophistication to establish firm-based, cross-border rules. If so, then regulators and stakeholders may be able to manage supervision of these codes. But the small number of participating companies will exacerbate the first problem identified – the uneven playing field between those large companies that are able to draft and negotiate their own set of cross-border privacy rules, and the small and medium -sized enterprises that lack the resources and expertise to do so. This will hurt the very start-up and emerging companies on which the information economy depends for innovation.

Before leaving this topic it is important to note that, while the Safe Harbor program allows individual companies to develop privacy codes, it also allows self-regulatory privacy programs to do so.[[129]](#footnote-129) This could allow many companies to come together under the banner of a single safe harbor organization such as TRUSTe, and so reduce the resource and administrative burdens associated with code drafting and approval. This “economy-wide” approach to cross-border codes (so named because safe harbor organizations, eager for members, are generally open to companies from any sector of the economy) mitigates one set of problems, but replaces it with another. As regulatory theorists have explained,[[130]](#footnote-130) the principal virtue of industry-drafted codes of conduct is that they are able to tap into private sector knowledge and produce rules that are tailored to the realities of the business world. When a company or trade association that represents a particular sector drafts a code, it generally achieves this benefit. Companies and sectors have particular realities that characterize them, and the drafters can tailor a code to address them. By contrast, when a safe harbor organization or other such entity drafts an *economy-wide* code that is open to companies from all different sectors, it is not able to tailor it to particular realities. Such codes must, necessarily, remain broad enough to encompass firms from many different lines of business that have divergent characteristics. Such codes will therefore fail to take advantage of the principal attribute of codes of conduct and the main reason why policymakers look to them—the ability to draw on firms’ knowledge of their own, particular realities, and tailor the rules to account for them.

**IV. Sector-Based Privacy Codes: A Better Solution**

There is another way to structure enforceable codes of conduct. Industry sectors can draft them. This is how the Dutch, who pioneered the use of enforceable privacy codes of conduct, design them. An industry sector, usually represented by a trade association, drafts a code of conduct that applies the Dutch Data Protection Act to the realities of its specific sector.[[131]](#footnote-131) Once the Dutch DPA approves the code, any company in that sector that complies with it inhabits a legal safe harbor with respect to the statute.[[132]](#footnote-132) The Dutch DPA has approved twenty sector-based codes of conduct, including codes drafted by the pharmaceutical, banking, insurance, direct marketing, and credit rating industries.[[133]](#footnote-133) These codes are tailored to the business realities of the specific sector that they govern.[[134]](#footnote-134)

Policymakers could use the same approach with respect to cross-border privacy rules. They could utilize sector-based—as opposed to company-based or economy-wide— codes of conduct. Doing so would ameliorate many of the problems that the other two approaches produce. Sector-based codes would be accessible, not only to the largest and most sophisticated firms, but to small and medium-sized ones as well. Such smaller companies could organize themselves—either through a trade association, or otherwise—and pool their resources to support the drafting and negotiation of a code of conduct for their sector. This would make participation in a sector-based code system feasible for such companies in a way that developing a company-based code would not be. More companies would accordingly have access to sector-based codes than to company-based ones.

A sector-based system would also reduce regulators’ administrative costs. There are simply fewer sectors than there are companies. Concentrating the code negotiation process at the level of the sector would therefore reduce the resources needed to supervise and engage in this process. The Dutch codes support this point. Since 1989, when the Dutch DPA first started negotiating sector-based codes of conduct, it has approved twenty such codes.[[135]](#footnote-135) This is a reasonable task that even a small national agency, such as the Dutch DPA, has been able to handle. While an international system would likely produce a greater number of sector-based codes, the relevant agency would have a proportionately larger amount of resources at its disposal. It should be able to handle this task.[[136]](#footnote-136)

For much the same reasons, sector-based codes should be more amenable to public participation than their company-based counterparts. Stakeholder organizations will have a smaller number of codes to review and monitor. These groups should find this to be a much more manageable task. Each of the above reasons explains why sector-based codes would likely function better than the company-based codes on which the current initiatives rely so heavily.

They also stack up well against the economy-wide codes that the Safe Harbor program utilizes. Economy-wide codes’ main weakness is that they must speak in broad terms so that many different types of companies can participate in them.[[137]](#footnote-137) They cannot tailor themselves to the specific realities of a company or sector. Sector-based codes, on the other hand, can do this. The drafters of a sector-based code—typically a trade association that represents that sector—can draw on the experience and knowledge of companies in that branch of industry. They can build this into the code and so produce a document that intelligently accounts for the specific technological and business realities of that particular sector. The sector-based Dutch codes demonstrate this as well.[[138]](#footnote-138)

The bottom line is that sector-based codes will possess the most important advantages of company-based and economy-wide codes, while avoiding their most significant weaknesses. Initiatives seeking to establish cross-border privacy rules should employ sector-based codes in place of, or in addition to, these other two types of codes. The following table depicts the current initiatives and where the recommended, sector-based approach would fit among them.

**TABLE 1: CROSS-BORDER PRIVACY RULES**

**Level at Which Regulate Type of Regulation**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Direct regulation** | **Self-regulation** | **Co-regulation** |
| **Company** | International treaty implemented through national law | Corporate privacy policies | BCRsCBPRsSafe Harbor  |
| **Sector** | International treaty | Network Advertising Initiative (NAI)[[139]](#footnote-139) | **Proposed approach** |
| **Economy as a whole** | International treaty | ICX Code | Safe Harbor  |

A. Cross-Border Privacy Rules Through Sector-Based Codes: An Implementation Strategy

In theory, there should be a relatively simple, elegant way to achieve international, sector-based codes of conduct. First, an industry sector would draft a code of conduct that complies with the EU’s 1995 Data Protection Directive and with the APEC Privacy Principles, and that tailors these requirements to its particular realities. Next, the sector would submit the code to European authorities who would review it for compliance with the Directive. If these officials approved it, then individual companies that followed the terms of the code would be deemed to be in compliance with the data protection laws of all 28 E.U. member states. The code would constitute a legal safe harbor with respect to all E.U. member states.

The sector would then take the same code and submit it to an APEC Accountability Agent who would review it for compliance with the APEC Privacy Principles. If the Agent approved the code, then it would constitute a legal safe harbor (or something close to it) with respect to the twenty-one APEC member economies, including the United States, China, Japan, Russia. Once this happened, companies that followed the twice-approved code could transfer data across borders with confidence that they were complying with the laws of the most significant European and Asian-Pacific nations. The code would constitute a nearly global set of cross-border privacy rules.[[140]](#footnote-140)

Is such an approach realistic? To assess this it is important, first, to examine the E.U. and APEC systems on the level of process. Does each system have procedures in place that would allow it to approve a sector-based code? If so, would this act truly create a legal safe harbor for companies that followed the approved code? It is also important to examine the E.U. and APEC systems with respect to substance. Are these systems’ privacy requirements sufficiently congruent that a single code could integrate them into a single set of rules? Or do they conflict with one another such that it is not possible to combine them in this way? The remainder of this section will analyze the proposed strategy on the levels of both process and substance.

B. Global Codes: Process

Do the E.U. and APEC systems have a process for approving sector-based codes of conduct?

1. E.U. approval

In seeking to answer this question with respect to the E.U. system, it is important to look both at E.U. law as it exists today (i.e. the 1995 Data Protection Directive), and as it is likely to be in a few years time (i.e. the proposed General Data Protection Regulation). Under either scenario, E.U. law should offer a clear mechanism for evaluating sector-based codes that, if approved, will constitute a legal safe harbor with respect to all E.U. member nations.

a. The 1995 Data Protection Directive

Article 27 of the 1995 Directive expressly authorizes “trade associations” representing a branch of industry to draft a code of conduct and submit it to the Article 29 Working Party.[[141]](#footnote-141)

The Working Party “shall determine . . . whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive.” [[142]](#footnote-142) If they are, the Directive instructs the Working Part to “approve[]” the code, and the European Commission to publicize this approval.[[143]](#footnote-143) Such an approved, EU-wide code is known as a “Community Code.” A Community Code differs from a BCR in that it constitutes a legal safe harbor with respect to the laws of all 28 E.U. Member States, whereas BCRs ensure compliance only with the Article 25 “adequacy” requirement. It also differs in that a Community Code is proposed by and applicable to an industry *sector*, whereas a BCR is proposed by and applicable to an individual *company.* Given that a Community Code represents compliance with the data protection laws of all E.U. member states, a multi-national company that followed a Community Code throughout its operations should also meet the Article 25 “adequacy” test. So long all of its corporate group complied with the Code, it should be able freely to transfer data outside the EU.

The Federation of European Direct and Interactive Marketing Associations (FEDMA) Community Code provides an example of how this process would work. FEDMA drafted and proposed a Community Code. In 2003, the Article 29 Working Group approved it.[[144]](#footnote-144) The code incorporates the requirements of the 1995 Directive and tailors them to the particular realities of the direct marketing industry.[[145]](#footnote-145) It provides a legal safe harbor, valid with respect to the data protection laws of all 28 E.U. member states, for any European direct marketing firm that complies with it. In 2010, the Article 29 Working Party approved an “annex” to the FEDMA code that covers online marketing.[[146]](#footnote-146)

It is worth noting that the direct marketing industry is the only sector that has successfully established a Community Code. This under-utilization of the Article 27 Community Code process is likely a reflection of the significant costs involved in drafting and negotiating a code of this type. Still, the Article 27 process, as illustrated by the Article 29 Working Party’s approval of the FEDMA code, appears to provide just the process needed to establish sector-based, international privacy rules that would function throughout the E.U. In theory, any sector could propose such a code to the Article 29 Working Party. If the Working Party approved it, the code would provide a legal safe harbor with respect to the data protection laws of all E.U. member states. Thus, at least with respect to the European Union ,a clear process exists for implementing EU-wide, sector-based privacy codes.

b. The proposed General Data Protection Regulation.

European data protection law is in flux. On January 25, 2012, the European Commission proposed a new General Data Protection Regulation that, if adopted, would replace the 1995 Data Protection Directive.[[147]](#footnote-147) The proposed General Regulation would be directly binding on regulated parties in the E.U. and so would harmonize data protection law throughout the European Union. This new set of laws, or some version of it, is likely to replace the 1995 Directive within the next few years. Like the 1995 Directive, the proposed General Regulation provides a means for developing EU-wide, sector-based codes of conduct. Section 38 of the proposed Regulation (Jan. 25, 2012 draft) requires national supervisory authorities and the European Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors.”[[148]](#footnote-148) Where the association proposing the code represents data controllers in a number of different Member States (as would be the case in the strategy that this article proposes), the proposed Regulation allows the organization to “submit draft codes of conduct . . . to the Commission.”[[149]](#footnote-149) It gives the Commission (i.e. the European Commission) the authority to “adopt implementing acts for deciding that codes of conduct . . . submitted to it . . . have general validity within the Union.”[[150]](#footnote-150)

This proposed procedure appears in many respects similar to the one that the Article 27 of the 1995 Directive currently makes available. It allows trade associations to submit sector-based codes of conduct to the Commission. It authorizes the Commission to approve such codes, and so to give them “general validity” throughout the European Union. The only meaningful difference is that, under the 1995 Directive, the Article 29 Working Party reviews and approves the code whereas, under the proposed General Regulation, the Commission handles this task. But other that that the proposed Regulation, in its current form at least, keeps in place the process now available under Article 27 of the 1995 Directive for the approval of Community Codes.

Both existing, and proposed, E.U. data protection laws appear to provide exactly the process needed to establish legally-approved, EU-wide, sector-based code of conduct.

c. APEC approval

It is far less clear whether the APEC Privacy Framework, as currently constituted, would support the approval of sector-based codes. The APEC Cross-Border Privacy Rules program clearly allows individual *companies* to submit codes of conduct to an Accountability Agent, and to seek the Agent’s approval that the code complies with the APEC Privacy Principles. But nothing in APEC’s published procedures suggest that an *industry sector* could submit such a code and obtain approval of it. If sectors are to be able to utilize the E.U. and APEC processes to establish internationally privacy rules, it will be important for APEC expressly to open its process to sector-based codes. Absent such a change, large, sophisticated companies will be able to take advantage of the APEC cross-border rules process but, for the most part, small and medium-sized enterprises will not.

The APEC process also falls short in its creation of a legal safe harbor. As explained above, APEC guidance makes clear that an Accountability Agent’s approval of a company code *does not* guarantee compliance with the data protection laws of APEC member nations, and *does not* create a legal safe harbor with respect to them.[[151]](#footnote-151) This means that firms operating in the APEC framework will still have to track and comply with the data protection laws of many different nations; and regulators, individuals or other stakeholders trying to check on compliance will find it hard to know which jurisdiction’s rules apply at any given moment in personal data’s cross-border journey. Thus, the APEC CBPR system will not fully address the problems that cross-border data transfers create for business, or for data subjects and other stakeholders.This contrasts with the Article 29 Working Party’s approval of a Community Code (or the Commission’s approval of a sector-based code under the proposed Regulation) which clearly *does* create a legal safe harbor—and so a single set of rules—with respect to the entire E.U.

The APEC system needs to change in two ways in order to allow for the implementation of sector-based, cross-border codes. It needs to open up its code approval process to industry sectors. And it needs increase the legal significance of Accountability Agent approval so that it more closely approximates a legal safe harbor. Not only will this facilitate cross-border data transfers among the APEC nations. It will also enable the APEC and E.U. code approval systems to operate in concert with one another and so to produce cross-border privacy rules that encompass the E.U., United States and much of Asia.

C. Global Codes: Substance

This raises the second major question: can these two systems work in harmony? Is there sufficient substantive overlap? This is a tricky question because the law in this area is a moving target. The APEC Privacy Principles appear to be stable for now. But European data protection law is not. As was mentioned above, the European Commission has proposed a General Data Protection Regulation that would replace the 1995 Data Protection Directive.[[152]](#footnote-152) The proposed Regulation would directly bind regulated parties in the E.U. and would not require member state implementing legislation. In this way, it would further harmonize E.U. data protection law. The General Data Protection Regulation will likely take the place of the 1995 Directive within the next few years.

U.S. privacy law is also in some flux. To date, U.S. privacy law has consisted of targeted statutes that regulate specific sectors (e.g. health care, financial institutions). In recent years, members of the House and the Senate have proposed comprehensive commercial privacy legislation that would expand U.S. privacy to all other economic sectors.[[153]](#footnote-153) The Commercial Privacy Bill of Rights Act of 2011, a bi-partisan bill introduced by Senator John McCain (R-Ariz) and (then) Senator John Kerry (D-MA), is the most developed of these legislative proposals and illustrates this legislative direction.[[154]](#footnote-154) The bill would establish a broad set of privacy requirements – the commercial privacy “Bill of Rights.” [[155]](#footnote-155) It would then allow sector-based trade associations (as well as other private entities) to develop a code that fleshes out the statute and applies it to their sector.[[156]](#footnote-156) If the FTC were to agree that the code properly interprets the statute, and approve it, then the bill would grant those firms that comply with the code a legal safe harbor analogous to the one that the E.U. provides for companies that follow an approved Community Code.[[157]](#footnote-157) This is a far stronger safe harbor than the one that would otherwise be available to U.S. companies under the APEC CBPR system. While Congress is unlikely to pass comprehensive privacy legislation in the near future, another major controversy regarding commercial holdings of personal data, coming on top of the recent scandal involving National Security Agency access to private-sector phone and Internet records, could cause it to act.

This evolving picture complicates the analysis of whether comprehensive E.U., APEC and (potentially) U.S. privacy laws overlap sufficiently for a cross-border code to incorporate the requirements of each. It requires that the analysis consider four bodies of privacy law: the 1995 Directive; the proposed General Data Protection Regulation; the APEC Privacy Principles; and the Commercial Privacy Bill of Rights Act (the Congressional bill that has received the most attention and that best represents how U.S. privacy law may evolve in the future.)

Table 2 depicts the substantive contours of the four existing and proposed sets of comprehensive privacy rules. The first column identifies the main types of privacy-protective requirements that such systems might include. Each of the subsequent columns are devoted to one set of privacy rules (the 1995 Directive, the proposed General Data Protection Regulation, the APEC Privacy Principles, or the Commercial Privacy Bill of Rights Act) and indicate whether that set of rules contains the listed privacy requirements. This allows one to see the extent to which these systems overlap with one another.

TABLE 2: SUBSTANTIVE OVERLAP\*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirements** | **EU 1995 Directive[[158]](#endnote-1)** | **EU General Regulation[[159]](#endnote-2)** | **APEC****Privacy****Principles[[160]](#endnote-3)** | **US Commercial Privacy Bill of Rights Act[[161]](#endnote-4)** |
| Transparency of data practices | √[[162]](#endnote-5) | √[[163]](#endnote-6) | √[[164]](#endnote-7) | √[[165]](#endnote-8) |
| Choice/Consent | √[[166]](#endnote-9) | √[[167]](#endnote-10) | √[[168]](#endnote-11) | √[[169]](#endnote-12) |
| Legitimate bases (other than consent) | √[[170]](#endnote-13) | √[[171]](#endnote-14) | √[[172]](#endnote-15) | √[[173]](#endnote-16) |
| Security safeguards | √[[174]](#endnote-17) | √[[175]](#endnote-18) | √[[176]](#endnote-19) | √[[177]](#endnote-20) |
| Accuracy | √[[178]](#endnote-21) | √[[179]](#endnote-22) | √[[180]](#endnote-23) | √[[181]](#endnote-24) |
| Access | √[[182]](#endnote-25) | √[[183]](#endnote-26) | √[[184]](#endnote-27) | √[[185]](#endnote-28) |
| Correction | √[[186]](#endnote-29) | √[[187]](#endnote-30) | √[[188]](#endnote-31) | √[[189]](#endnote-32) |
| Purpose limits use | √[[190]](#endnote-33) | √[[191]](#endnote-34) | √[[192]](#endnote-35) | √[[193]](#endnote-36) |
| Sensitive data | √[[194]](#endnote-37) | √[[195]](#endnote-38) | (√)[[196]](#endnote-39) | √[[197]](#endnote-40) |
| Accountability |  | √[[198]](#endnote-41) | √[[199]](#endnote-42) | √[[200]](#endnote-43) |
| Purpose limits collection | √[[201]](#endnote-44) | √[[202]](#endnote-45) | √[[203]](#endnote-46) |  |
| Data Minimization | √[[204]](#endnote-47) | √[[205]](#endnote-48) |  | √[[206]](#endnote-49) |
| Fair and Lawful | √[[207]](#endnote-50) | √[[208]](#endnote-51) | √[[209]](#endnote-52) |  |
| Retention and disposal | √[[210]](#endnote-53) | √[[211]](#endnote-54) |  | √[[212]](#endnote-55) |
| Privacy by Design |  | √[[213]](#endnote-56) |  | √[[214]](#endnote-57) |
| Prior check  | √[[215]](#endnote-58) | √[[216]](#endnote-59) |  |  |
| Right to Object | √[[217]](#endnote-60) | √[[218]](#endnote-61) |  |  |
| Automated decisions | √[[219]](#endnote-62) | √[[220]](#endnote-63) |  |  |
| Notification to data subject | √[[221]](#endnote-64) | √[[222]](#endnote-65) |  |  |
| Children’s data requires parent’s consent |  | √[[223]](#endnote-66) |  | (√)[[224]](#endnote-67) |
| Data Protection by Default |  | √[[225]](#endnote-68) |  |  |
| Privacy Impact Assessment |  | √[[226]](#endnote-69) |  | √ |
| Notification to data protection authority | √[[227]](#endnote-70) |  |  |  |
| Documentation of Processing |  | √[[228]](#endnote-71) |  |  |
| Right to be Forgotten and to Erasure |  | √[[229]](#endnote-72) |  |  |
| Data portability |  | √[[230]](#endnote-73) |  |  |
| Preventing harm |  |  | √[[231]](#endnote-74) |  |
| Data Protection Officer |  | √[[232]](#endnote-75) |  |  |
| Supervisory Authority | √[[233]](#endnote-76) | √[[234]](#endnote-77) |  |  |
| “Adequacy” limit for int’l transfer | √[[235]](#endnote-78) | √[[236]](#endnote-79) |  |  |
|  |  |  |  |  |

\* For Table endnotes, see pp. 49-50. These endnotes will be reformatted to fit with the table in the final version of this article.

Table 2 shows that the four comprehensive systems of privacy rules do overlap in many of the most important areas.[[237]](#footnote-158) Each system provides for: (1) transparency with respect to data practices; (2) choice/consent; (3) legitimate bases for processing other than consent; (4) reasonable security safeguards; (5) accuracy; (6) access; (7) correction; (8) purpose limitations with respect to the use of personal data; and (9) and special protections for sensitive data. In addition, three out of the four systems provide for: (10) Accountability; (11) purpose limits for with respect to the collection of personal data; (12) data minimization; (13) fair and lawful processing; and (14) limits on retention and disposal of personal data. While Table 2 also shows that these systems also differ in a number of ways, fourteen areas of overlap is a lot of common ground. Potentially, a sector could develop a code that addressed each of these requirements in a way acceptable to each of the relevant systems. Firms that complied with such a code would know that they met the most significant privacy requirements of each system.

In order to build in *all* the requirements of each system, such a code would need to go beyond the areas of overlap and include elements (e.g. data portability, or the prevention of harm) that are currently present in only one or two of the systems. To be truly universal, such a comprehensive code would have to incorporate the most stringent requirements from each set of privacy rules. This would lead to a “ratcheting up” for requirements for companies that otherwise would only be subject to one such system, or another. The increased efficiency to be gained from a single, nearly global set of privacy rules, as well as any enhanced consumer trust that their commitment to follow a stringent code may bring them, could provide firms with sufficient incentive to take such a step. The production and implementation of (nearly) global privacy codes could accordingly lead to an increase in privacy protections.

It is also important to qualify any conclusions drawn from Table 2, and to recognize what it cannot tell us. Table 2 lists only broad privacy requirements. It says nothing about how each system defines and interprets these requirements. For example, two systems may each require “consent” to the processing of personal data, thereby making it appear that they are similar. But further examination may show that one system allows opt-out consent across the board, while the other requires opt-in consent in certain situations.[[238]](#footnote-159) A drafter seeking to put together cross-border code would accordingly have to examine in detail the definitions, explanatory statements and regulatory and applicable judicial interpretations in order to compose a requirement that would truly satisfy each of the relevant systems. While such an analysis is clearly needed in order to determine whether the various privacy rule systems can actually be combined into a single code, it is beyond the scope of this article and will require additional research. Table 2 seeks only to provide a “first cut” at the analysis by determining whether the broad frameworks match up. It shows that, with respect to the most important privacy requirements, they do. On the levels of both process and substance, the conditions are sufficiently favorable to warrant further exploration of this approach.

1. Multi-Stakeholder Codes of Conduct: the White House Approach

In its 2012 report, *Consumer Data Privacy in a Networked World*, the White House expressed its enthusiasm for enforceable, privacy codes of conduct.[[239]](#footnote-160) It called for legislation that would establish a Consumer Privacy Bill of Rights,[[240]](#footnote-161) allow private groups to implement them through a code of conduct,[[241]](#footnote-162) and create a legal safe harbor where FTC approves such codes.[[242]](#footnote-163) The White House expressed its intention to include “international stakeholders” in the discussions about particular codes of conduct so that the codes could come to reflect a “transatlantic consensus on important, emerging privacy issues.” [[243]](#footnote-164) It disclosed “plans to develop additional mechanisms—such as jointly developed codes of conduct—that support mutual recognition of legal regimes.” [[244]](#footnote-165)

On one level, these White House pronouncements parallel and reinforce many of this article’s key positions. The report envisions group-based codes—perhaps even sector-based codes—rather than individual company codes. It envisions using codes of conduct to
“support mutual recognition of legal regimes.” While this latter statement may be vague and undeveloped, it nonetheless shows support for and an interest in using codes in this way. Read in light of the White House report, this article’s thesis begins to seem quite realistic.

The White House report also goes beyond this article’s analysis in ways that raise interesting questions about how best to implement the code negotiation process. The report calls for “multi-stakeholder groups” to develop the codes, and states that such groups will consist of “individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups.”[[245]](#footnote-166) These groups must reach “consensus” on the code before companies can adopt it.[[246]](#footnote-167) Clearly, stakeholders must be involved in the code negotiation process. But is such a large group workable? This is a far greater array of parties than negotiate the Dutch codes or the APEC Cross-Border Privacy Rules. The size and complexity of such groups raise questions about transaction costs and the ability to reach consensus on broad and meaningful requirements. Pursuant to the White House agenda, the National Telecommunications and Information Administration has, for the past year, been facilitating a multi-stakeholder process of this type to develop a code of conduct on Mobile App Transparency.[[247]](#footnote-168) The process, which began with over 200 representatives present at the initial negotiation, has made important progress. However, it remains to be seen whether it can produce a meaningful code with a substantial number of adoptees.

Another difference is the White House’s intention to proceed with multi-stakeholder codes of conduct *even in the absence* of comprehensive privacy legislation.[[248]](#footnote-169) Under such a scenario, neither the FTC nor any other agency will independently assess and approve the code. Instead, the report envisions that the government’s role be limited to “help[ing] the parties reach clarity,” and that it not get involved in “substituting its own judgment” for that of the multi-stakeholder group.[[249]](#footnote-170) This precludes the use of mutually *approved* codes of conduct that could create a cross-border legal safe harbor for firms that followed a code. It also means that the codes will not create a legal safe harbor – one of the key attractions for industry. Will such a code be able to attract a sufficient number of industry participants? Again, the NTIA’s current experiment with the multi-stakeholder negotiation over Mobile App Transparency appears to be a valuable one that could provide important lessons about this regulatory approach.

**V.** **Recommendations**

While some aspects of the discussion, such as how best to structure stakeholder involvement in the code negotiation process, will require further study, this article’s main points are clear. First, in a world of increasingly global data flows, cross-border privacy rules can play an important role in fostering the Internet economy and in enhancing privacy protections for individuals. Second, when it comes to developing global privacy rules, co-regulation is likely to be more practical than direct regulation, and more effective than self-regulation. Third, co-regulation at the level of the industry *sector* will likely prove more effective than co-regulation at the level of the *firm* or at the level of the *economy* as a whole. The three cross-border privacy rule initiatives—the U.S.-E.U. Safe Harbor Agreement (U.S.-E.U. Safe Harbor); the EU’s Binding Corporate Rules program (BCR); and the Asian-Pacific Economic Cooperation’s Cross-Border Privacy Rules initiative (CBPR)—utilize a form of co-regulation, but do so at the level of the firm, or of the economy as a whole. That design flaw weakens these approaches. Governments and industry should experiment with *sector-based co-regulation* as a supplement to the existing initiatives.

Fourth, E.U. and APEC privacy rules may overlap sufficiently to allow a single code to satisfy both regimes. Further study will be required to confirm this. Fifth, the E.U. and APEC systems each include code approval mechanisms that could, with some important modifications, serve as the basis for approving and enforcing sector-based codes that bridge these two regional initiatives. In order for this to occur:

* The E.U. should retain Article 27 of the 1995 Data Protection Directive which allows the Article 29 Working Group to approve sector-based codes and create a legal safe harbor with respect to all E.U. Member State data protection laws.
* If the E.U. adopts the General Data Protection Regulation, then it should retain Article 38 of the proposed GDPR which allows the Commission to approve sector-based data protection codes and so create a legal safe harbor with respect to the GDPR.
* APEC should authorize Accountability Agents to approve *sector-based* codes, not just those that individual companies submit.

* APEC should further define and strengthen the safe harbor that an approved code creates with respect to the national data protection laws of APEC member states. Doing so will increase firms’ incentive to participate in the APEC CBPR system.[[250]](#footnote-171)

Government adoption of these recommendations would establish a workable system of cross-border privacy rules to govern data flows across all E.U. and APEC member states. Such a system would incorporate the 28 E.U. member nations, as well as the United States, Canada, Japan, China and other APEC countries. Taken together, these steps would bring us closer to that Holy Grail of contemporary privacy law: global privacy rules.

1. *See* Paul M. Schwartz, *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment* (The Privacy Projects, 2009) (describing commercial data transfers across national borders). [↑](#footnote-ref-1)
2. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stan. L. Rev. 1315, 1336-1339 (2000) (describing the conflict between international data flows and national laws). [↑](#footnote-ref-2)
3. *See infra* notes 49-56 and accompanying text. [↑](#footnote-ref-3)
4. *See infra* notes 57-65 and accompanying text. [↑](#footnote-ref-4)
5. *See infra* notes 62-63 and accompanying text. [↑](#footnote-ref-5)
6. Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy* 53 (2010). [↑](#footnote-ref-6)
7. *See infra* note 77 and accompanying text. [↑](#footnote-ref-7)
8. *See infra* notes 90-92 and accompanying text. [↑](#footnote-ref-8)
9. *See infra* notes 101-120 and accompanying text. [↑](#footnote-ref-9)
10. *See infra* notes 101-108 and accompanying text. [↑](#footnote-ref-10)
11. *See infra* notes 109-114 and accompanying text. [↑](#footnote-ref-11)
12. *See infra* notes 115-120 and accompanying text. [↑](#footnote-ref-12)
13. *See* Dennis D. Hirsch, *Introduction: The Information Economy, The War on Terror and the Evolving Landscape of Information Privacy Law*, 6 I/S: J. of L. & Pol’y for the Info. Society 409, 409-12 (2010) (describing this process in a number of areas of law) [hereinafter Hirsch, *Information Economy*]. [↑](#footnote-ref-13)
14. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1322 (“the entire architecture of the Internet is based on the principle of geographic indeterminacy. . . . Data may be collected in one location, processed elsewhere, and stored in yet another site.”) [↑](#footnote-ref-14)
15. Cloud computing is “the location of computing resources on the Internet in a fashion that makes them highly dynamic and scalable.” Schwartz, *Managing Global Data Privacy, supra* note 1, at5 (The Privacy Projects, 2009). [↑](#footnote-ref-15)
16. Schwartz, *Managing Global Data Privacy, supra* note 1. [↑](#footnote-ref-16)
17. *Id.* at 5, 10. [↑](#footnote-ref-17)
18. *Id.* [↑](#footnote-ref-18)
19. Reidenberg, *International Data Privacy Rules*, *supra* note 2, at 1316-17; *see also* Dep’t of Commerce, *Commercial Data Privacy*, *supra* note 6, at 19 (“[u]nlike traditional mass media, the Internet is global.”) [↑](#footnote-ref-19)
20. Schwartz, *Managing Global Data Privacy, supra* note 1, at 17 (IT revolution facilitated globalization). [↑](#footnote-ref-20)
21. *Id.* at 20 (data transfers based on process optimization, not physical proximity). [↑](#footnote-ref-21)
22. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1317. [↑](#footnote-ref-22)
23. Schwartz, *Managing Global Data Privacy, supra* note 1, at 17 (data goes “from one established database to another”). An example would be a subsidiary that transferred human resources data from its own local data base, to that of its parent company. *Id.* at 11 (providing such an example). [↑](#footnote-ref-23)
24. *Id.* at 8. [↑](#footnote-ref-24)
25. *Id.* at 15. [↑](#footnote-ref-25)
26. *Id.* at 23. [↑](#footnote-ref-26)
27. *Id.* at 8, 15. [↑](#footnote-ref-27)
28. *Id.* at 8. [↑](#footnote-ref-28)
29. *Id.* at 16. [↑](#footnote-ref-29)
30. *Id.* at 5. [↑](#footnote-ref-30)
31. *Id.* at 5 (“Modern information systems respond to data requests rapidly and I many instances in real time”); *id.* at 8. [↑](#footnote-ref-31)
32. *Id.* at 13. [↑](#footnote-ref-32)
33. *Id.* at 22. [↑](#footnote-ref-33)
34. *Id.* at 14. [↑](#footnote-ref-34)
35. *Id.* at 59. [↑](#footnote-ref-35)
36. *Id.* at 22. [↑](#footnote-ref-36)
37. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1317; Schwartz, *Managing Global Data Privacy, supra* note 1, at 8. [↑](#footnote-ref-37)
38. Professor Schwartz provides another example that nicely captures this set of developments. A marketing firm in Spain obtains a list of potential customers from a global Customer Relationship Management (CRM) system in the U.S. It shares this list with its call center in Mexico, which uses it to execute a telemarketing campaign in Spain. The Spanish marketing company then shares the results of its telemarketing effort with the U.S. vendor, which uses it to update the information in its global CRM system. Schwartz, *Managing Global Data Privacy, supra* note 1, at 13. [↑](#footnote-ref-38)
39. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1325. [↑](#footnote-ref-39)
40. *See* [*http://oecdprivacy.org/#principles*](http://oecdprivacy.org/#principles)(last visited June 29, 2013) (listing the OECD Privacy Principles). [↑](#footnote-ref-40)
41. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1330-1332. [↑](#footnote-ref-41)
42. *Id.* at 1332; [↑](#footnote-ref-42)
43. *Id.* at 1338. [↑](#footnote-ref-43)
44. Council Directive 95/46, arts. 10, 11 (notification to data subject), art. 18 (notification to DPA), 1995 O.J. (L 281) 31 [hereinafter 1995 Directive]. [↑](#footnote-ref-44)
45. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1330. [↑](#footnote-ref-45)
46. *Id.* at 1330-31 [↑](#footnote-ref-46)
47. *Id.* at 1334-35. [↑](#footnote-ref-47)
48. *Id.* at 1318. See also Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 Iowa L. Rev. 471 (1995) (transferring data between U.S. and Europe faces significant challenges). Reidenberg, *International Data Privacy Rules, supra* note 2, at 1336 (“The Internet places divergent rules in proximity through architectural features that promote geographic indeterminacy.”) [↑](#footnote-ref-48)
49. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1337 (stating that some jurisdictions have far weaker information privacy rules than others). [↑](#footnote-ref-49)
50. *Id.* at 1332. [↑](#footnote-ref-50)
51. Dep’t of Commerce, *Commercial Data Privacy*, *supra* note 6, at 54 (differing national privacy laws can lead to “gaps in protection for consumers whose data are transferred across borders, since it is not always clear who has jurisdiction over data and what protections exist for foreign consumers.”) [↑](#footnote-ref-51)
52. *Id.* at 1323 (when multiple entities interact with data this can “obscure the responsibility for data protection”). [↑](#footnote-ref-52)
53. *Id.* at 1336 (explaining that multiple nations may assert jurisdiction over a networked set of data transfers). [↑](#footnote-ref-53)
54. *Id.* at 1336 & n. 114, *citing* Jack L. Goldsmith, *Cyberanarchy*, 65 U. Chi. L. Rev. 1199, 1216-21 (1999). [↑](#footnote-ref-54)
55. Sunni Yuen, *Exporting Trust With Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry,* 9 Colum. Sci. & Tech. L. Rev. 41, 42 (2007-2008). [↑](#footnote-ref-55)
56. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1351. [↑](#footnote-ref-56)
57. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 31 (Feb. 2012) (“Differences in national privacy laws create challenges for companies wishing to transfer personal data across national borders.”) [↑](#footnote-ref-57)
58. *Id.* (“Complying with different privacy laws is burdensome for companies that transfer personal data . . . because legal standards may vary among jurisdictions, and companies may need to obtain multiple regulatory approvals to conduct even routine operations.”) [↑](#footnote-ref-58)
59. Dep’t of Commerce, *Commercial Data Privacy*, *supra* note 6, at 54 (the lack of cross-border interoperability in privacy principles and regulations creates barriers to cross-border data flow and significant compliance costs for companies.”) [↑](#footnote-ref-59)
60. *Id.*  [↑](#footnote-ref-60)
61. *Id.*  [↑](#footnote-ref-61)
62. Reidenberg, *International Data Privacy Rules, supra* note 2, at 1337-38. [↑](#footnote-ref-62)
63. *Id.* at 1351. [↑](#footnote-ref-63)
64. Dep’t of Commerce, *Commercial Data Privacy*, *supra* note 6, at 15 (stating that the maintenance of “consumer trust is vital to the success of the digital economy”); Reidenberg, *International Data Privacy Rules, supra* note 2, at 1351 (“The uncertainty and instability of the protection of individuals will be harmful to international data flows and the wider development of a robust online community.”) [↑](#footnote-ref-64)
65. Dep’t of Commerce, *Commercial Data Privacy*, *supra* note 6, 56. [↑](#footnote-ref-65)
66. White House, *Consumer Data Privacy*, *supra ,* note 57, at 31 (“it is critical to the continued growth of the digital economy that [governments] strive to create interoperability between privacy regimes”); Dep’t of Commerce, *Commercial Data Privacy*, *supra* note 6, at 14 (“Improving the global interoperability of data privacy approaches could enable increased exports of U.S. services and strengthen the American economy.”) [↑](#footnote-ref-66)
67. *Id.* at 56 (stating that “mutual recognition of substantively similar commercial data privacy laws around the world can build increased practical protection for consumers and reduce barriers and compliance costs for business”). [↑](#footnote-ref-67)
68. Dep’t of Commerce, *Commercial Data Privacy*, *supra* note 6, at 57. [↑](#footnote-ref-68)
69. *See generally*, Christopher T. Marsden, Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace 46 (2011) (distinguishing between government regulation, self-regulation, and co-regulation); Hans-Bredow-Institut, Final Report: Study on Co-Regulation Measures in the Media Sector 17 (2006) (same); Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation?*, 34 Seattle U. L. Rev. 439, 465 (2011) (same) [hereinafter, Hirsch, *Online Privacy*]; Bert-Jaap Koops, Miriam Lips, Sjaak Nouwt, Corien Prins & Maurice Schellekens, *Should Self-Regulation be the Starting Point?*, *in* Starting Point for ITC Regulation: Deconstructing Prevalent Policy One-Liners 109 (Koops, Prins, Schellekens & Lips eds., 2006) (same); Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Regulatory Codes*, 6 I/S: J. L. & P. for Info. Soc’y, 355, 357 (2010); Neil Gunningham & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective,* 19 L. & Pol’y 363, 365-66 (1997). [↑](#footnote-ref-69)
70. Rees, *supra* note 69, at 9; Margot Priest, *The Privatization of Regulation: Five Models of Self-Regulation,* 29 Ottawa L. Rev. 233, 237-38 (1997-98); Koops, et al., *supra* note 69. [↑](#footnote-ref-70)
71. Rees, *supra* note 69, at 9; Priest, *supra* note 69, at 238 (describing “entirely voluntary systems of regulation”). [↑](#footnote-ref-71)
72. Marsden, *supra* note 69, at 46; Rubinstein, *supra* note 69, at 357; Gunningham & Rees, *supra* note 69, at 366. [↑](#footnote-ref-72)
73. Rubinstein, *supra* note 69, at 357-58. [↑](#footnote-ref-73)
74. In some sense, most regulation could be said to be co-regulatory. Government frequently consults industry—either through notice-and-comment rulemaking, or more informally—when it engages in direct regulation. By the same token, industry often looks to government for input and feedback when it engages in self-regulation. To demarcate co-regulation it helps to think of a continuum with pure industry self-regulation on one end (i.e. no government involvement); and pure government regulation on the other (i.e. no industry role). *See* Gunningham & Rees, *supra* note 69, at 366 (describing a “continuum, with pure forms of self-regulation and government regulation at opposite ends”). Co-regulation encompasses those initiatives that stand towards the middle of this continuum—the programs in which government and industry intentionally and expressly combine their efforts and collaborate on the production, monitoring and enforcement of rules. [↑](#footnote-ref-74)
75. James Salzman & Barton H. Thompson, Environmental Law and Policy 49 (2003). [↑](#footnote-ref-75)
76. Howard Latin, *Ideal Versus Real Regulatory Efficiency: Implementation of Uniform Standards and “Fine-Tuning” Regulatory Reforms*, 37 Stan. L. Rev. 1267, 1271 (1985) [↑](#footnote-ref-76)
77. *See* Virginia Haufler, A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy 82 (2001) (discussing difficulty of direct, top-down regulation due to lack of consensus on the “mechanisms and standards for international privacy protection”). [↑](#footnote-ref-77)
78. Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation can Learn from Environmental Law*, 41 Georgia L. Rev. 1, 34 (2006) [hereinafter Hirsch, *Inner Environment*]. [↑](#footnote-ref-78)
79. *Id.* at 35; Neil Gunningham, *Environmental Management Systems and Community Participation: Rethinking Chemical Industry Regulation*, 16 UCLS J. Envtl. L. & Pol’y 319, 327 (1998). [↑](#footnote-ref-79)
80. Hirsch, *Inner Environment*, *supra* note 78, at 35; Richard

B. Stewart, *A New Generation of Environmental Regulation?*, 29 Cap. U. L. Rev. 21, 31 (2001); U.S. Congress, Office of Tech. Assessment, Environmental Policy Tools: A User’s Guide 27-28 (1995). [↑](#footnote-ref-80)
81. Haufler, *supra* note 77, at 92 (discussing those who believe that government should not seek to regulate information privacy, and should leave the task to industry self-regulation, because “government regulators simply do not have the capability to deal with the rapid changes and complex issues of the new information economy.”) [↑](#footnote-ref-81)
82. *See* Koops, et al., *supra* note 69 (discussing those who take this position); Gunningham & Rees, *supra* note 69, at 366 (same). [↑](#footnote-ref-82)
83. Gunningham & Rees, *supra* note 69, at 366 (discussing those who take this position); Jared Strauss & Kenneth S. Rogerson, *Policies for Online Privacy in the United States and the European Union*, 19 Telematics & Informatics 173, 181 (2002) (same). [↑](#footnote-ref-83)
84. *Id.* [↑](#footnote-ref-84)
85. *See* Haufler, *supra* note 77, at 22 (multi-nationals adopt global corporate policies “so that they would not have to deal with such a welter of conflicting national regulatory regimes”); Colin J. Bennett and Charles D. RAAB, The Governance of Privacy: Policy Instruments in Global Perspective 155 (2006) (multi-national corporations adopt privacy policies); Rhys Jenkins, *Corporate Codes of Conduct: Self-Regulation in a Global Economy*, Technology, Business and Society Programme Paper No. 2, U.N. Research Institute for Social Development 7, 23 (April 2001) (multi-national corporations adopt social responsibility policies in order to ensure that their entire value chain meets standards). [↑](#footnote-ref-85)
86. Privacy Law and Business International Newsletter, *International Business to Produce a Global Privacy Code*, available at <http://worldlii.org/int/journals/PLBIN/2000/3.html> (last visited July 13, 2013). [↑](#footnote-ref-86)
87. Nick Mansfield, *ICX Privacy and Data Protection Code of Conduct* 4(Shell Services Int’l, July, 2000) (copy on file with author). [↑](#footnote-ref-87)
88. *Id.* [↑](#footnote-ref-88)
89. *See* [www.icx.org.uk/about.htm](http://www.icx.org.uk/about.htm) (last visited June 14, 2013). [↑](#footnote-ref-89)
90. Bennett & Raab, *supra* note 85, at 134. [↑](#footnote-ref-90)
91. Strauss & Rogerson, *supra* note 83, at 183; Koops, et al., *supra* note 69. [↑](#footnote-ref-91)
92. *See* Hirsch, *Online Privacy, supra* note 69, at 459-464 (discussing this research); Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* (World Privacy Forum, 2007) (analysis of Network Advertising Initiative self-regulatory program). [↑](#footnote-ref-92)
93. Philip J. Harter, *Collaboration: The Future of Governance*, 2009 J. Disp. Resol. 411, 420, 422; Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. Rev. 1, 22, 26-27 (1997); Neil Gunningham & Darren Sinclair, Leaders & Laggards: Next-Generation Environmental Regulation 104 (2002); Daniel J. Fiorino, *Toward a New System of Environmental Regulation: The Case for an Industry Sector Approach*, 26 Envtl. L. 457, 485 (1996) (stating that a negotiated, sector-based approach can allow “companies to tailor rules to their own circumstances”). [↑](#footnote-ref-93)
94. Freeman, *supra* note 93, at 12, 23-24; Gunningham & Sinclair, *supra* note 93, at 109. A study of Dutch data protection codes of conduct has shown that some co-regulatory mechanisms may not be as flexible and adaptable as industry self-regulation. In the Netherlands, industry sectors draft a code of conduct and submit it to the regulator, which must approve it. This generally requires each of the parties to make a substantial investment in an in-depth negotiation before they can reach agreement on the terms of the code. This makes them reluctant to re-open the terms of the agreement, and so leads to static codes of conduct that generally do not change during their five-year term. *Id.* In self-regulation, industry sets its own rules and does not have to obtain government approval of them. This makes it easier for industry to re-open and revise these rules in order to account for changing technological or business realities. [↑](#footnote-ref-94)
95. Gunningham & Sinclair, *supra* note 93, at 108-109. [↑](#footnote-ref-95)
96. *Id.*  [↑](#footnote-ref-96)
97. *Id.* at 105 (collaborative negotiations “generate risks of a phenomenon tantamount to regulatory capture.”) [↑](#footnote-ref-97)
98. *See infra* notes 166-67 (discussing how best to integrate stakeholders into the negotiation process). [↑](#footnote-ref-98)
99. Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law*, forthcoming \_\_ Mich. St. L. Rev. \_\_\_ (2013) [hereinafter Hirsch, *Going Dutch*]. [↑](#footnote-ref-99)
100. *Id.*  [↑](#footnote-ref-100)
101. 1995 Directive, *supra* note 44, art. 25. [↑](#footnote-ref-101)
102. Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation 219 (2007). [↑](#footnote-ref-102)
103. *Id.* at 225 [↑](#footnote-ref-103)
104. *Id.* at 223. [↑](#footnote-ref-104)
105. *Id.* at 223-24. [↑](#footnote-ref-105)
106. *Id.* at 220. [↑](#footnote-ref-106)
107. Article 29 Data Protection Working Party, *Working Document on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules* 6 (Apr. 8, 2009);Kuner, *supra* note 102, at 220. [↑](#footnote-ref-107)
108. Kuner, *supra* note 102, at 227. [↑](#footnote-ref-108)
109. *See* <http://www.apec.org/About-Us/About-APEC/History.aspx> (last visited July 15, 2013); <http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx> (listing the current member countries) (last visited July 15, 2013). [↑](#footnote-ref-109)
110. *See* APEC, *APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised* (2009), available at <http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx> (last visited July 15, 2013). [↑](#footnote-ref-110)
111. See APEC, APEC Privacy Framework (2005) (listing the APEC Privacy Principles), available at <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx> (last visited July 15, 2013); *see* Table 2, *infra*, for an overview of these Principles. [↑](#footnote-ref-111)
112. Paula J. Bruening, *APEC Roundup: Update on Accountability Agents in Implementation of the APEC Framework, Development of Pathfinder Projects, More,* 9 Privacy & Sec. L. Rep. 1444 (Oct. 18, 2010). [↑](#footnote-ref-112)
113. *Id.* [↑](#footnote-ref-113)
114. APEC, *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines* (“The CBPR System does not displace or change an Economy’s domestic laws and regulations. . . . Participation in the CBPR System does not replace a participating organization’s domestic legal obligations. . . . Where domestic legal requirements exceed what is expected in the CBPR System, the full extent of such domestic law and regulation will continue to apply”); *accord* Justin Bookman, *Can ‘Cross-Border Privacy Rules’ Trump Divergent Data Protection Laws?* (Center for Democracy and Technology, Oct. 4, 2011) (APEC framework explicitly requires compliance with various national data protection laws). [↑](#footnote-ref-114)
115. Rubinstein, *supra* note 69, at 390-91. [↑](#footnote-ref-115)
116. *See* Safe Harbor Overview, <http://export.gov/safeharbor/eu/eg_main_018476.asp> (last visited July 15, 2013). [↑](#footnote-ref-116)
117. *See* Department of Commerce, *Safe Harbor Privacy Principles* (2000), available at <http://export.gov/safeharbor/eu/eg_main_018475.asp> (last visited July 15, 2013). [↑](#footnote-ref-117)
118. *Id.;* TRUSTe is one of the largest safe harbor seal programs and has developed a set of privacy requirements that companies must meet in order to fulfill the Safe Harbor Principles and join the program. *See* <http://www.truste.com/privacy-program-requirements/program_requirements_EUSH_privacy> (last visited July 15, 2013). [↑](#footnote-ref-118)
119. Rubinstein, *supra* note 69, at 391. [↑](#footnote-ref-119)
120. Dep’t of Commerce, *Safe Harbor Privacy Principles*, *supra* note 117; Rubinstein, *supra* note 69, at 391. [↑](#footnote-ref-120)
121. The Safe Harbor Agreement also employs economy-wide sets of privacy rules, i.e. those developed by safe harbor organizations and open to companies from any economic sector. These are also flawed, as explained *infra* at notes 129-130 and accompanying text. [↑](#footnote-ref-121)
122. Kuner, *supra* note 102, at 220 (“the [BCR] approval process can be lengthy, and implementation can be expensive for all but large multi-nationals”). [↑](#footnote-ref-122)
123. *Cf.* Priest, *supra* note 70, at 258 (small companies find it burdensome to engage in self-regulation). [↑](#footnote-ref-123)
124. *See infra* notes 129-130 and accompanying text. [↑](#footnote-ref-124)
125. *See* the listing of those companies that have completed the BCR process that is available at [*http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr\_cooperation/index\_en.htm*](http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm)(last visited June 15, 2013). [↑](#footnote-ref-125)
126. *Cf.* Priest, *supra* note 70, at 281 (company-based approaches to self-regulation lead disparate obligations for different firms). [↑](#footnote-ref-126)
127. *See id.* at 258 (firm-based self-regulation makes it “more costly” for government regulators); *id.* at 278 (individuated, company-based self-regulatory regime compromises efficiency). [↑](#footnote-ref-127)
128. Stakeholders typically have even fewer resources to devote to this task than government agencies do. [↑](#footnote-ref-128)
129. *See supra* note 118 and accompanying text. [↑](#footnote-ref-129)
130. *See supra* note 93 and accompanying text. [↑](#footnote-ref-130)
131. See Hirsch, *Going Dutch*, *supra* note 99 (describing this feature of the Dutch data protection code of conduct program). [↑](#footnote-ref-131)
132. *Id.*  [↑](#footnote-ref-132)
133. *Id* (providing Appendix that identifies all twenty approved Dutch codes. [↑](#footnote-ref-133)
134. *Id.* (providing examples of such tailoring). [↑](#footnote-ref-134)
135. *Id.* (providing Appendix that lists these codes). [↑](#footnote-ref-135)
136. *See* Priest, *supra* note 70 (industry-based approaches, supervised by government, provide a “strong accountability mechanism”). [↑](#footnote-ref-136)
137. *See supra* note 130 and accompanying text. [↑](#footnote-ref-137)
138. *See* Hirsch, *Going Dutch*, *supra* note 99. [↑](#footnote-ref-138)
139. The Network Advertising Initiative is a group of more than 90 online advertising companies that has adopted a code of conduct for protecting consumer privacy in interest-based advertising. *See* <http://www.networkadvertising.org/> (last visited July 15, 2013) (describing the NAI and providing a link to the 2013 NAI code of conduct). The purpose of this sector-based self-regulatory organization is to encourage best practices among industry members and so, perhaps, to obviate the need for direct government regulation of behavioral advertisers. NAI thus has a domestic, rather than an international, focus. Still, it can serve as an example of a self-regulatory, sector-based code. [↑](#footnote-ref-139)
140. It would leave out parts of South America and Africa for which there is not yet a regional organization that could approve such a code. This is an important omission insofar as it could increase the costs of doing business in these areas as compared to those in which regional authorities had approved the code. One solution would be for South America and Africa to develop regional privacy organizations similar to APEC that could adopt privacy principles and approve codes consistent with these principles. [↑](#footnote-ref-140)
141. 1995 Directive, *supra* note 44, art. 27(2), (3). [↑](#footnote-ref-141)
142. *Id.* [↑](#footnote-ref-142)
143. *Id.* [↑](#footnote-ref-143)
144. Article 29 Working Party, *Opinion 3/2003 on the European Code of Conduct of FEDMA for the use of personal data in direct marketing* (June 13, 2003). [↑](#footnote-ref-144)
145. *Id.* at 3-4. [↑](#footnote-ref-145)
146. Article 29 Working Party, *Opinion 4/2010 on the European Code of Conduct for the Use of Personal Data in Direct Marketing* (July 13, 2010). [↑](#footnote-ref-146)
147. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (January 25, 2012) [hereinafter “Draft General Regulation”] [↑](#footnote-ref-147)
148. *Id.,* art. 38(1). [↑](#footnote-ref-148)
149. *Id.* art. 38(3). [↑](#footnote-ref-149)
150. *Id.* art. 38(4). [↑](#footnote-ref-150)
151. *See supra* note 114 and accompanying text. [↑](#footnote-ref-151)
152. *See supra* note 146 and accompanying text. [↑](#footnote-ref-152)
153. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); The BEST PRACTICES Act of 2011, H.R. 611, 112th Cong. (2011); The Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. § 9 (2011). [↑](#footnote-ref-153)
154. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011). [↑](#footnote-ref-154)
155. *Id.* §§ 101-303. [↑](#footnote-ref-155)
156. *Id.* §§ 501, 502. [↑](#footnote-ref-156)
157. *Id.* [↑](#footnote-ref-157)
158. **TABLE ENDNOTES** (to be reformatted in final version):

 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L281) 31, [hereinafter “1995 Directive”]. [↑](#endnote-ref-1)
159. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (Jan. 25, 2012) [hereinafter “proposed General Regulation”]. [↑](#endnote-ref-2)
160. Asia-Pacific Economic Cooperation, APEC Privacy Framework (2005). [↑](#endnote-ref-3)
161. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011) [hereinafter Kerry-McCain Bill]. [↑](#endnote-ref-4)
162. 1995 Directive arts. 10, 18, 19, 21. [↑](#endnote-ref-5)
163. Proposed General Regulation arts. 5(a), 11. [↑](#endnote-ref-6)
164. APEC Framework ¶¶ 15-17. [↑](#endnote-ref-7)
165. Kerry-McCain Bill § 201. [↑](#endnote-ref-8)
166. 1995 Directive art. (consent as general basis for legitimacy); 8(2) (“explicit” consent to processing of sensitive data). [↑](#endnote-ref-9)
167. Proposed General Regulation art. 6(a). [↑](#endnote-ref-10)
168. APEC Framework ¶ 20. [↑](#endnote-ref-11)
169. Kerry-McCain Bill § 202(a)(1)-(3). [↑](#endnote-ref-12)
170. 1995 Directive art. 7(b)-(f) (providing legitimate bases for processing other than the data subject’s consent to such processing). [↑](#endnote-ref-13)
171. Proposed General Regulation art. 6(b)-(f). [↑](#endnote-ref-14)
172. APEC Framework ¶ 19. [↑](#endnote-ref-15)
173. Kerry-McCain Bill § 202(a)(3)(A). [↑](#endnote-ref-16)
174. 1995 Directive art. 17 (“appropriate technical and organizational measures”). [↑](#endnote-ref-17)
175. Proposed General Regulation art. 30. [↑](#endnote-ref-18)
176. APEC Framework ¶ 22. [↑](#endnote-ref-19)
177. Kerry-McCain Bill §101. [↑](#endnote-ref-20)
178. 1995 Directive art. 6(1)(d). [↑](#endnote-ref-21)
179. Proposed General Regulation art. 5(d). [↑](#endnote-ref-22)
180. APEC Framework ¶ 21. [↑](#endnote-ref-23)
181. Kerry-McCain Bill § 303. [↑](#endnote-ref-24)
182. 1995 Directive art. 12(a). [↑](#endnote-ref-25)
183. Proposed General Regulation art. 15. [↑](#endnote-ref-26)
184. APEC Framework ¶¶ 23-25. [↑](#endnote-ref-27)
185. Kerry-McCain Bill § 202(a)(4). [↑](#endnote-ref-28)
186. 1995 Directive art. 12(b). [↑](#endnote-ref-29)
187. Proposed General Regulation art. 16. [↑](#endnote-ref-30)
188. APEC Framework ¶¶ 23-25. [↑](#endnote-ref-31)
189. Kerry-McCain Bill § 202(a)(4). [↑](#endnote-ref-32)
190. 1995 Directive art. 6(1)(b). [↑](#endnote-ref-33)
191. Proposed General Regulation art. 5(b). [↑](#endnote-ref-34)
192. APEC Framework ¶ 19. [↑](#endnote-ref-35)
193. Kerry-McCain Bill § 202(b), 302. [↑](#endnote-ref-36)
194. 1995 Directive art. 8(1). [↑](#endnote-ref-37)
195. Proposed General Regulation art. 9. [↑](#endnote-ref-38)
196. APEC Framework ¶ 14 (by requiring that privacy protections be proportionate to the threatened harm associated with the collection and use of the personal information in question, this provision implicitly differentiates between sensitive personal data (where the threat of harm is great) and other personal information. [↑](#endnote-ref-39)
197. Kerry-McCain Bill § 202. [↑](#endnote-ref-40)
198. Proposed General Regulation art. 22. [↑](#endnote-ref-41)
199. APEC Framework ¶ 26. [↑](#endnote-ref-42)
200. Kerry-McCain Bill § 102. [↑](#endnote-ref-43)
201. 1995 Directive art. 6(1)(b). [↑](#endnote-ref-44)
202. Proposed General Regulation art. 5(b). [↑](#endnote-ref-45)
203. APEC Framework ¶ 18. [↑](#endnote-ref-46)
204. 1995 Directive art. 6(1)(c). [↑](#endnote-ref-47)
205. Proposed General Regulation art. 5(c). [↑](#endnote-ref-48)
206. Kerry-McCain Bill § 301. [↑](#endnote-ref-49)
207. 1995 Directive art. 6(1)(a). [↑](#endnote-ref-50)
208. Proposed General Regulation art. 5(a). [↑](#endnote-ref-51)
209. APEC Framework ¶ 16. [↑](#endnote-ref-52)
210. 1995 Directive art. 6(e). [↑](#endnote-ref-53)
211. Proposed General Regulation art. 5(e). [↑](#endnote-ref-54)
212. Kerry-McCain Bill § 301(2). [↑](#endnote-ref-55)
213. Proposed General Regulation art. 23. [↑](#endnote-ref-56)
214. Kerry-McCain Bill § 103. [↑](#endnote-ref-57)
215. 1995 Directive art. 20 (authority conducts prior check of operations “likely to present specific risks” to data subjects). [↑](#endnote-ref-58)
216. Proposed General Regulation art. 34. [↑](#endnote-ref-59)
217. 1995 Directive art. 14 (data subject can object based on “compelling legitimate grounds”). [↑](#endnote-ref-60)
218. Proposed General Regulation art. 19. [↑](#endnote-ref-61)
219. 1995 Directive art. 15 (right of data subject not to be subject to decision that significantly affects him and is based on automated data processing). [↑](#endnote-ref-62)
220. Proposed General Regulation art. 20. [↑](#endnote-ref-63)
221. 1995 Directive arts. 10, 11. [↑](#endnote-ref-64)
222. Proposed General Regulation art. 14. [↑](#endnote-ref-65)
223. Proposed General Regulation art. 8. [↑](#endnote-ref-66)
224. This requirement can be found in the Children’s Online Privacy Protection Act (COPPA), Pub. L.105-277, Div C, Title XIII, § 1302, 112 Stat. 2681-728 (codified at 15 U.S.C. §§ 6501-6506 (1998)). If Congress were to pass comprehensive privacy legislation similar to the Kerry-McCain bill, COPPA would operate alongside of it. [↑](#endnote-ref-67)
225. Proposed General Regulation art. 23. [↑](#endnote-ref-68)
226. Proposed General Regulation art. 22, 33. [↑](#endnote-ref-69)
227. 1995 Directive art. 18. [↑](#endnote-ref-70)
228. Proposed General Regulation art. 28. [↑](#endnote-ref-71)
229. Proposed General Regulation art. 17. [↑](#endnote-ref-72)
230. Proposed General Regulation art. 18. [↑](#endnote-ref-73)
231. APEC Framework ¶ 14 (requiring the privacy protections be designed to prevent harm to individuals, and should be proportionate to the degree of harm threatened by the collection and use of the information in question). [↑](#endnote-ref-74)
232. Proposed General Regulation art. 22, 35-37. [↑](#endnote-ref-75)
233. 1995 Directive art. 28. [↑](#endnote-ref-76)
234. Proposed General Regulation art. 46. [↑](#endnote-ref-77)
235. 1995 Directive art. 25. [↑](#endnote-ref-78)
236. Proposed General Regulation art. 41. [↑](#endnote-ref-79)
237. This should not be surprising given that these sets of laws share a common root: the Fair Information Privacy Practices that the U.S. Department of Health, Education and Welfare (HEW), and later the OECD articulated. [↑](#footnote-ref-158)
238. Cf. Reidenberg, *supra* note 2, at 1332-1335 (describing instances in which jurisdictions subscribe to the same privacy principles but interpret them quite differently). [↑](#footnote-ref-159)
239. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 23-29 (Feb. 2012). [↑](#footnote-ref-160)
240. *Id.* at 9-22. [↑](#footnote-ref-161)
241. *Id.* at 23. [↑](#footnote-ref-162)
242. *Id.* at 37. [↑](#footnote-ref-163)
243. *Id.* at 33. [↑](#footnote-ref-164)
244. *Id.* at 33. [↑](#footnote-ref-165)
245. *Id.* at 23. [↑](#footnote-ref-166)
246. *Id.* at 27. [↑](#footnote-ref-167)
247. *See generally,* <http://www.ntia.doc.gov/category/privacy> (last visited July 15, 2013). [↑](#footnote-ref-168)
248. *Id.* at 24. [↑](#footnote-ref-169)
249. *Id.* at 27. [↑](#footnote-ref-170)
250. To make such a system even more useful, Congress should pass comprehensive privacy legislation, along the lines of the Consumer Privacy Bill of Rights Act of 2011, that includes a safe harbor program for industry sectors. This would increase the strength of the U.S. safe harbor beyond that which the APEC system alone would provide, and so would make it similar to the safe harbor that the 1995 Directive creates. It would ensure that, with respect to the U.S. and E.U. at least, companies that followed an approved, sector-based code gain the benefit of a strong legal safe harbor. This would encourage sectors to draft and negotiate such codes. [↑](#footnote-ref-171)