Regulation of Borderless High-Technology Economies: Managing Spillover Effects

Steven R. Salbu
Regulation of Borderless High-Technology Economies: Managing Spillover Effects

Steven R. Salbu*

I. INTRODUCTION

In October of 1998, the European Union Data Privacy Directive ("Directive") became effective.\(^1\) Consistent with Europe's serious approach to consumer privacy, the Directive mandates that Member States adopt the most rigorous privacy legislation the world has seen. The specific requirements of the Directive are complex, and I have discussed them in some detail in another article.\(^2\) Very generally, the Directive places obligations on data collectors and provides rights to data subjects. The most significant of these protections from a global privacy perspective is the Directive's "opt-in" approach, which presumes an expectation of data privacy as the default position, and (with certain exceptions) allows the processing of personal information only if "the data subject has unambiguously given his consent."\(^3\)

Beyond this substantive provision, which differs from the "opt-out" presumption that underlies US privacy policy, the Directive contains an interesting data-flow restriction. Because of its potential effect on other nations that interact with or do business in Europe, it may be the most controversial feature of the Directive.\(^4\) According to Article 25 of the Directive:

The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer

---

* Associate Dean, Bobbie and Coulter R. Sublett Centennial Professor and University Distinguished Teaching Professor, University of Texas. The author gratefully acknowledges the generous summer research support of the McCombs School of Business, University of Texas.

3. Directive at art 7(a) (cited in note 1).
4. In today's global market, entities in all nations are likely to interact or do business with Europe. Accordingly, the Directive's provisions protecting data flows are likely to have worldwide impact.
may take place only if, without prejudice to compliance with national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

Section 2 of Article 25 enumerates circumstances that help determine whether adequate protection is provided by a given third country. These include the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Countries that fail to ensure adequate protection under the provisions of Article 25 may still receive personal data transfers under the following conditions:

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
   (a) the data subject has given his consent unambiguously to the proposed transfer; or
   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
   (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
   (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
   (e) the transfer is necessary in order to protect the vital interests of the data subject; or
   (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

6. Id at art 25 §2.
7. Id at art 26.
The Directive’s data-flow restrictions recognize that European implementing legislation must account for the use of data beyond the EU if it is to provide meaningful consumer privacy protections. The restrictions have thrown down the gauntlet to the non-EU world: if nations are to ensure continued data flows from much of Europe, they must prove that they are worthy of “Safe Harbor” protection by demonstrating that they have ensured adequate data privacy.

The United States was the first nation to draft proposed Safe Harbor guidelines, and to present them to the European Union for its approval. After several rounds of negotiations, a final set of Safe Harbor provisions was drafted by the US and approved by the European Union.

The specifics of the Safe Harbor principles are beyond the scope of this article. They are listed and briefly explained in the Federal Register, which also elaborates on the principles through a set of frequently asked questions, or FAQs. Very generally, the principles allow US companies to self-certify as Safe Harbor compliant by registering with the US Department of Commerce. According to the Commerce Department’s International Trade Administration,

EU organizations . . . can ensure that they are sending information to a U.S. organization participating in the safe harbor by viewing the online list of safe harbor organizations posted on the website. The list will contain the names of all U.S. companies that have committed to the safe harbor framework. This list will be regularly updated, so that it is clear who is assured of safe harbor benefits.

Others have written in detail about the US Safe Harbor provisions. The brief description above suffices to establish the context in which to examine an interesting phenomenon: some observers believe that the US Safe Harbor principles are weak and meaningless, and do not go nearly far enough, while others see them as an

8. See Sean D. Murphy, US-EU "Safe Harbor" Data Privacy Arrangement, 95 Am J Indl L 156, 156 (2001) ("[I]n recognition of the ease with which personal data on Europeans can be transferred electronically outside the EU, the directive sought to prohibit transfers to non-EU states unless those states provide an 'adequate' level of data protection.").
intolerable European incursion into sovereignty and autonomy. Those who say the
principles are inadequate focus on the self-certification process, and the lack of
meaningful monitoring and implementation processes. Those who say the
provisions go too far argue that they are detrimental to both international trade and
the economy.

The data-flow restrictions are also subject to a more philosophical challenge: that
they surrender to what is arguably Europe's overstepping of its sovereign reach. This
position suggests that Europe has surpassed its defensible global purview and
authority by demanding implementation of European-style protections, holding
hostage data flows to create a palpable threat. The remainder of this article addresses
these philosophical issues of international policy and law. In a global, high-technology
economy, in which boundaries are becoming ever more surmountable, how can and
should nations and regions protect their interests and manage inevitable spillover
effects?

II. MANAGING LOCAL OR REGIONAL INTERESTS IN A GLOBAL
ECONOMY

The global privacy debate is significant for more than the substantive issues it has
identified. It also raises critical questions in regard to international relations, as areas
or regions try to meet their goals in regard to a technology that has little respect for
borders.

Through the EU's ambitious, wide-reaching strategy, privacy has become the
most prominent area of Internet regulation in which one region has tried very
aggressively to manage spillover effects by exerting substantial market pressure outside
its borders. The data-flow restrictions are not ambiguous: either a nation
demonstrates to the EU that it can ensure adequate levels of privacy protection, or it
loses access to personal data from the EU.

---

European Parliament Rejects Proposal; Safe Harbor Agreement in Question, Computer World 24 (July 17,
2000) (noting the European Parliament's belief that the Safe Harbor Principles lack the
establishment of an independent body to hear complaints about incursions on privacy, as well as a
mechanism for private damages for those whose privacy has been invaded).

regulations "excessive" and extending "beyond consumer concern," and suggesting they could hurt
international trade and the economy).

15. See David G. Post and David R. Johnson, The New Civic Virtue of the Net: Lessons from Models of
Complex Systems for the Governance of Cyberspace, Stan Tech L Rev para 21 (1997), available online at
(defining spillover effects as "effects of conduct [that] extend beyond pre-established geographical
boundaries—or 'spill over' into other jurisdictions").

The threat is enormous. For example, a multinational firm based in the US could lose access to personal financial data. Were this to happen, banking across borders could be paralyzed. Likewise, an airline selling a round-trip ticket between Paris and New York could find itself unable to transmit the itinerary from France to computer systems at Kennedy Airport. A company making personnel decisions or assessments may find that employee records cannot be transmitted from Brussels to Los Angeles. Assuming that the threat is serious—in other words, that the EU actually will implement data flow restrictions against non-complying non-EU nations—the stakes in ignoring the Directive are daunting.

Because the data-flow restrictions are potentially so harmful not only to third-party nation economies, but also to Europe's economy itself, one has to wonder whether the risk of noncompliance is really significant. Had the US ignored the threat, would the EU have carried it out? The costs of doing so to Europe would be so enormous that it is hard to believe Europe would actually exercise the data-flow provisions of Article 25. It is also questionable whether the EU will enforce the threat against other significant trading partners in the future, should those partners fail to develop acceptable Safe Harbor principles.

Whether a true threat or a bluff, the EU's approach in the Directive is one specific example of a more general contemporary problem regarding Internet regulation. Given its unprecedented globe-spanning capabilities, the Internet creates new regulatory challenges for sovereign entities. Technology creates a world where municipalities, states, nations, and even regional affiliations of nations are arguably too small to address contemporary social interaction.

A likely future scenario is as follows: nations will recognize the new challenges of Internet technology, and will search for ways to control new risks, sometimes within the framework of regulation and legislation. To do this effectively, they must acknowledge the degree to which spillover effects can undermine regulatory efforts. Europe certainly did so in the area of privacy, and there is no doubt that the EU was justified in its belief that failure to control the use of data outside Europe would destroy the protections it was creating for its citizens. It is one thing to protect data privacy and integrity within the borders of the fifteen EU nations; it is another thing entirely to control what happens to information after it leaves the jurisdiction of EU nation borders.

What is clear is that nations cannot effectively manage Internet behavior without somehow controlling activities outside their own boundaries. What remains to be answered, however, is how nations, or regions such as the EU, should try to manage spillover effects fairly, effectively, and optimally. Is it appropriate to hold other

17. See Julian Randall and Bridget Treacy, Digital Buccaneers Caught in a Legal Web, Fin Times 2 (May 30, 2000) (discussing a number of areas in which the Internet evokes concerns for businesspersons regarding legal conflicts across countries of the world).
nations and regions hostage to one’s own regulatory scheme, as Europe arguably has done and is doing in regard to its Data Privacy Directive? What will be the possible costs of this method of managing spillover effects? And will this method even be feasible in a pluralistic world with hundreds of nations? What will be the result of this method—is it more likely to spur rapid unification of regulatory schemes, or to spur international disharmony?

The remainder of this article makes the following arguments, in Sections III through VI. First, aggressive management of spillovers will be essential if nations are to pass effective consumer protection laws and regulations, not only in the realm of privacy, but in other areas as well. Second, there may be some advantages in managing spillovers multilaterally, as opposed to unilaterally. Third, the need for effective spillover management in a technologically globalized world may favor unilateralism over multilateralism. Finally, aggressive spillover management, while potentially effective, is also risky. To the extent that sufficient groundwork in the form of aligned values is lacking, aggressive approaches run the risk of encouraging international dissension and tension.

III. THE NECESSITY OF AGGRESSIVE MANAGEMENT OF SPOILLOVERS

The global privacy debate has demonstrated a fundamental problem with Internet regulation and control: the problem of spillovers. I use the term “spillovers” to refer to instances where control of behaviors in one sovereignty is affected by behaviors from outside that sovereignty. This conceptualization comes from Post and Johnson, who define spillovers as “effects of conduct [that] extend beyond pre-established geographical boundaries—or ‘spill over’ into other jurisdictions.”18

In the instance of data privacy protections, the outside activity spills into the controlling state, and affects, often negatively, that state’s ability to achieve its goals. Thus, if control of privacy invasions in the European Union can be undermined by behaviors in the United States, those US behaviors have a spillover effect in Europe. Aggressive management of spillovers will be essential if nations are to pass effective laws and regulations, not only in consumer privacy but in other areas as well.

While this problem certainly is not new, it takes on unprecedented importance in the era of high technology. Spillovers threaten regulatory effectiveness so forcefully in a wired world because wiring facilitates cross-border activities and cross-border effects of conduct. For example, five hundred years ago, activities in Spain certainly affected people who had their own governance structures in the Americas, but those activities were highly constrained—indeed, interaction occurred only via transatlantic ship travel. By the nineteenth century, technologies like telegraphy and telephony fostered increased interaction among physically distant parties, so that spillover effects

became more common. Nations had to be more concerned about whether extraterritorial activity would undermine the control mechanisms adopted through their legal systems.

This trend continued into the twentieth century as new technologies continued to shrink the world. Airplanes, cheaper international telephone technologies, overnight mail, and other innovations made the corners of the globe more accessible, permitting more transnational interaction, hence creating more spillover effects. No previous innovation, however, has come close to interactive computer technology in terms of its exponential magnification of spillover threats.

Clearly, the EU’s efforts to limit the use of personal information would be seriously undermined if they were to disappear at the fifteen member nations’ borders. Without effective controls of personal data use abroad, all the abuses that the EU seeks to avert simply would be shifted. Whatever one ultimately thinks of the EU’s aggressive approach, one must at least understand its motivation and sympathize with the difficulties of achieving effective Internet governance in today’s global arena.

Moreover, at first blush, the EU’s approach to privacy protection appears to be at least somewhat effective. By being an early and aggressive entrant, Europe has set the terms of the debate and, in the process, has identified itself as exercising leadership in the area of data privacy protection. Other countries indeed appear to be moving toward Europe’s groundbreaking model for privacy protection.19

Still, despite its unquestionable influence, the Directive will impose major costs around the world. These costs come in numerous forms. Relatively pedestrian are the localized costs to third-nation governments and businesses in forging Safe Harbor compliance systems and the organizational changes that will be necessary to implement them. Of greater concern are the potential costs in international goodwill, should non-EU nations resent the domineering approach taken under the Directive.

Barbara Crutchfield George and others have observed that the EU’s approach has been “unsettling,” noting that “the EU in effect is dictating to [businesses]... how to run their companies.”20 Some politicians apparently agree with this assessment. In March 2001, Representative Billy Tauzin of Louisiana, House Energy and Commerce Committee Chairman, joined other members of the House in attacking the Privacy Directive.21 He suggested that Europe is foisting a global privacy standard on the rest of the world, erroneously assuming that, where privacy is concerned, one size fits all.22

22. Id.
The level of discomfort in the US may be exacerbated by the difficulty we may have in accepting the EU/US role reversal inherent in the Safe Harbor Provisions of the Directive. This change reflects a broader shift in the balance of power between Europe and the US, as a function of increased contemporary European unity.

The US has taken seriously the Directive's threat to transnational information flows. The Directive certainly did engender heated debate and protest by US companies. One reporter described the reaction in early 1999 as a "furious counterattack from American companies that fear the EU measure could slow the transatlantic growth of electronic commerce." Yet while the Directive's aggressive management of externalities seems to be working, at least on paper, there may be costs in terms of international dissension and friction. These will be addressed in more detail later.

IV. MULTILATERAL ALTERNATIVES

Some suggest that unilateral action is not the best approach to the development of a unified, global policy for the management of global technology issues. Julia Fromholz contends, for example, that

[u]nilateral action, such as the implementation of the EU Directive, will only stir international resentment. Only if a wide array of nations, possibly acting through a body such as the WTO or the United Nations, arrives at an agreement on the appropriate level of data protection will a truly global solution be possible.

Fromholz's concern about the impact of unilateral regulatory solutions on international relations certainly is legitimate. Any time one nation or group of nations tries to impose its own rules and order on others, disagreements can ensue, tensions can mount, and resentments can develop and grow. A question that remains is

24. Id at 782–783. The authors state, Without a united European contingent of fifteen Member States, it was much easier for the United States to use its strength with individual nation-states. Any attempt of one of the European nations to impose an extraterritorial effect on data transfers would either never have occurred or, if it did, would not have been considered a serious threat. The overall lesson that multinational employers and those engaged in international business transactions may learn from the current data protection controversy with the EU is that an increasingly integrated Europe brings with it the specter of an increasing intrusion in U.S. business policies.
25. See, for example, Brandon Mitchener and Julie Wolf, EU Notebook: A Special Background Report on European Union Business and Politics, Wall St J Eur 1 (Jan 28, 1999) (quoting David Aaron, US Undersecretary of Commerce, as saying that the Directive "is an important priority for the Administration and the U.S. business community, and high stakes are involved").
whether Frohmolz's alternative—multilateral negotiation of, forging of, and agreement on appropriate solutions to global privacy challenges—will work.

The growing influence of non-governmental organizations ("NGOs") in the global arena suggests that multilateral negotiation has a potential role to play in the process of managing international spillover effects associated with technological global integration. Whether this growing role of NGOs and intergovernmental organizations ("IGOs") turns out to be a positive or negative force, the phenomenon is a present reality, and likely will continue to develop along with contemporary information technologies. Jessica Mathews goes so far as to call the telecommunications revolution "[t]he most powerful engine of change in the relative decline of states and the rise of non-state actors." Diffusion of information technology has eroded governmental power bases, as the ability to collect and manage information has spread to ordinary people and less established institutions and organizations. This in turn "multiplies the number of players who matter and reduces the number who command great authority." In this information age, it is hardly surprising then that NGOs and IGOs have made substantial gains in influence.

Of course, while the EU itself can be seen as one kind of IGO and therefore multilateral, Frohmolz's characterization of both the EU and its Data Privacy Directive as essentially unilateral is accurate. There are broader, more inclusive, less regionally defined alternatives that are truly multilateral. These are likely to provide some advantages over IGOs that are defined geographically, and therefore are subject to some of the same limitations as geographically defined traditional sovereign nations. In other words, even if we technically consider the EU to be an IGO, it is hardly one that embodies the spirit of multilateralism. It is more accurate to cast the EU as a regional alliance intended to create benefits for its members, in part by increasing Europe's relative global power. While the EU is not one nation, it serves some of the unabashedly self-interested goals that are traditionally sought by single nations.

Potential alternative examples that are not so regionally constrained, and therefore are potentially more multilateral in scope, are the Organization for Economic Cooperation and Development ("OECD"), the World Trade Organization ("WTO"), and the United Nations. Of course, just as regional governmental alliances, such as the EU, are imperfect providers of global policy, so too do these alternative alliances have advantages and disadvantages. One possible benefit of such

31. See id at 51.
32. Id.
NGOs and IGOs as international policy forgers is the role they can play as accumulators and managers of knowledge and information. Ryan and others posit this role as follows:

Building upon the functional theory of international governmental organizations ("IGOs") and drawing from the organizational theory of knowledge management, we conceptualize IGOs as knowledge managers, organizations with the capabilities to support multilateral trade and economic lawmaking processes. States create IGOs to further their wealth of knowledge; IGOs transfer information better than global markets. Moreover, states create IGOs to accumulate and disseminate knowledge, and thereby reduce international transaction costs.

IGOs are essentially "learners," as they acquire new information in order to be disseminators of knowledge. Each IGO possesses distinctive domains of knowledge, including strengths and weaknesses with respect to institutional capabilities. The knowledge accumulation and management of the IGO is central to the shared-knowledge of an international regime, thereby making the IGO the crucial cooperation-facilitating institution in a given area of international relations. We present an analytic framework for the investigation of IGO capabilities and capacities as knowledge managers in future international trade and trade-related law-making negotiations.

Again, while NGOs and IGOs have a potential role to play, they also have potential limitations. For example, while the OECD is an influential organization with the power and resources to champion global policy, in some ways it is no less parochial than the EU. Whereas the EU's limited purview is a function of its regionalism, the OECD's limitations derive from its status as what James Salzman calls a "Rich Man's Club." This label refers to the fact that the members of the OECD are wealthy, industrialized nations whose perspective is limited. Potential flaws are exacerbated by what some purport to be a lack of openness and transparency of OECD meetings, which raises potential questions regarding accountability. The WTO recently has been subject to similar criticism, in some ways more severe than challenges lodged against the OECD. Demonstrations at the 1999 Third Ministerial Meeting in Seattle reflected beliefs that WTO decisionmaking on trade and environmental policy is non-democratic, lacking both legitimacy and accountability.

35. See id at 776.
36. See id at 776-77.
37. See Gregory C. Shaffer, The World Trade Organization Under Challenge: Democracy and the Law and Politics of the WTO's Treatment of Trade and Environment Matters, 25 Harv Envir L Rev 1, 1-2 (2001) (noting that the central claim of the US environmental groups which formed "a core part of the protests" was that "WTO decisions on trade and environment issues are anti-democratic and thus lack legitimacy").
The United Nations arguably brings a converse bias to its proceedings, under perceptions that the organization is “developing country dominated and politicized.” Prominent alliances that are not dominated by either developed or developing nations appear to be in short supply. Moreover, NGOs and IGOs tend to be bifurcated into another set of constraining classes—political versus economic. Whereas the United Nations tends to focus on “the politics of peace,” the World Bank focuses on macroeconomic dynamics. Although both organizations work toward global coordination and conflict resolution, each tends to do so from a specialized vantage. While specialization by two of the world’s most powerful alliances may bear benefits of expertise and focus, they also bear potential costs, in the form of limited scope. Globalized challenges like world privacy demand attention to all pertinent dimensions—political, social, and economic.

To address Internet challenges like privacy, with their substantial spillover effects, we may need more overarching NGO or IGO activity. This could be in the form of extant organizations expanding their focus, or the creation of new organizations having broader focus, or the collaboration of existing organizations to cover all relevant dimensions. An advantage of the third option is that collaboration would allow the participating organizations to maintain the benefits of their own specializations, while overcoming parochialism through the joining of forces.

These observations suggest that there presently is no ideal (or even close to ideal) organization with which to entrust multilateral negotiation of global high-tech privacy issues. This dearth is likely to apply to NGOs and IGOs alike. Within this reality, and given the exigency of political, social, and economic challenges arising from the ever-changing Internet, unilateralism has a substantial appeal. Whatever its downside, the Directive has moved relatively quickly, reducing the risk that deliberations will outlast the poignancy of the issues they are intended to address.

V. HOW THE NEED FOR EFFECTIVE SPILLOVER MANAGEMENT IN A TECHNOLOGICALLY GLOBALIZED WORLD MAY FAVOR UNILATERALISM OVER MULTILATERALISM

Spillover management is more than an assurance of legal efficacy; it is also a driving force that presses regulation to catch up with technological globalization. This pressure is likely to favor unilateral approaches, such as the EU Data Privacy Directive, over more multilateral efforts.

To understand this proposition, it helps to begin by defining globalization, and then explaining the phrase “technological globalization.” These definitions are especially important because they often mean different things to different people.  

“Globalization” is a term fraught with the potential for creating conflict partly because different groups perceive it so differently. Western businesspersons may not see globalization in the same way as environmentalists or developing nation activists, for example. Duffield succinctly captures what he calls “the paradox of globalization”:

The term globalization has a number of different and even conflicting meanings. Within the international financial institutions (IFIs) and among free-market economists, for example, globalization is largely understood in terms of a worldwide economic and political convergence around liberal market principles and the increasing real-time integration of business, technological and financial systems. Based on an expansion and deepening of market competition, globalization is synonymous with an irresistible process of economic, political and cultural change that is sweeping all national boundaries and protectionist tendencies before it. Indeed, for a country to remain outside this process is now tantamount to its marginalization and failure. This pervasive neo-liberal assumption has been dubbed “hyperglobalization.”

However, while accepting that the current phase of globalization represents a new departure, there is a political economy position that contradicts the optimism that usually accompanies globalization’s free market interpretation. That is, the forces of globalization often produce unexpected and unwanted outcomes as they encounter other social systems. Rather than the anticipated virtuous circles of growth and prosperity that lead to orderliness, globalization tends to encourage new and durable forms of division, inequality and instability.

As I use the term here, globalization refers to the “inexorable integration of markets, nation-states and technologies driven by free-market capitalism and having a widespread homogenizing effect on cultures.” Modern driving forces of globalization include space exploration, the development of satellites, the development of nuclear energy, borderless environmental influences, and the political and economic hegemony of the multinational corporation.

Globalization today is facilitated by regional economic alliances like the North American Free Trade Agreement and the European Union. Globalization increases the number of relationships among nation-states and people the world over, as well as

43. See Bruce Mazlish, A Tour of Globalization, 7 Ind J Global Legal Stud 5, 5-6 (1999).
the degree of connectedness that characterizes these relationships. These phenomena spur a concomitant demand for global integration of laws capable of maintaining order in this rapidly changing global environment.

I use the term "technological globalization" to refer to a subclass of globalization that is important not only because it can be analyzed as a refined category, but also because this aspect of globalization is the driving force behind the unprecedented speed of globalization in general. Modern media that support the storage and exchange of information are having a profound effect on global society and politics. A good metaphor to distinguish technological globalization from the broader category of generic globalization is the Internet phenomenon of e-mail. International snail mail certainly has enhanced generic globalization by serving as one of numerous ways in which people can interact and communicate across the globe. Recently, e-mail has enhanced the more specific end of technological globalization by supporting such interaction and communication in a manner that is virtually instantaneous. This temporal leap is also a quantum leap in its social and economic effects, and therefore in the challenges posed to legal systems aimed at monitoring and controlling such effects.

Because it is characterized by dramatic acceleration over generic globalization, technological globalization makes daunting demands on legal and regulatory systems. As the Internet magnifies the speed and quantity of potential international transactions exponentially, the stakes in creating a global governance structure likewise increase dramatically. Within this context, aggressive unilateral spillover management drives regulation to catch up with the remarkable pace of technological globalization. The process is cyclical and self-reinforcing. Technological globalization increases the stakes in addressing Internet control issues globally and consistently, and doing so quickly. These increased stakes are the impetus for aggressive spillover management efforts. Because the effects and implications of spillover are greatly magnified by technological globalization, nations and regions have a growing imperative to address them effectively. Because the problems and challenges of the Internet change more rapidly than ever, there is also a growing imperative to address spillover effects quickly, in order to ensure that domestic protections are not lost or damaged abroad. This combined pressure for effective, fast answers confers upon aggressive, unilateral regulatory approaches a serious competitive advantage over more deliberative, time-consuming multilateral processes.

46. See Knowles, 95 Nw U L Rev at 735 (cited in note 42).
47. See generally Ronald J. Deibert, Parchment, Printing, and Hypermedia: Communication in World Order Transformation (Columbia 1997).
If an Internet policy is to have value, it indeed must be both effective and timely. By the time a slow response is created, the challenges of the Internet are likely to have morphed into something new, so that slow responses are unlikely to be effective. The second part of the cycle is fulfilled when timely, effective, unilaterally forged laws meet the social and economic needs of our wired world, thereby supporting both the infrastructure and the transactions that occur within it. A strong, effective technological society then can strive to respond to even more demanding new legal and regulatory challenges, which again will demand even more rapid responses that effectively address a wide array of global issues.

One very important final observation: this reasoning presumes that unilaterally forged laws, regulations, and policies can be effective, and that there are no serious impediments to that effectiveness. This may be far from true. Indeed, multilateral approaches have serious advantages in this regard because they incorporate constituent inputs that may be necessary or helpful in creating effective responses. In other words, the speed that is so crucial in addressing contemporary challenges works against effectiveness in many ways. Speed can come at a price, including insufficient groundwork, careless analysis, and failure to muster necessary consensus. If unilateralism is to achieve its potential advantages in managing global spillover effects, it must be built on some level of fundamental legitimacy, including a foundation of global value consensus. The world might not yet be ready for the unilateral answers that one day could be optimal. This issue and related issues are addressed in more detail in the following final section.

VI. CONCLUSION: THE RISKS OF AGGRESSIVE SPILLOVER MANAGEMENT WHEN VALUE SYSTEMS ARE INSUFFICIENTLY ALIGNED

While potentially effective, aggressive spillover management is also risky. In the absence of sufficient groundwork, in the form of acceptable procedures and sufficiently aligned value systems, aggressive approaches run the risk of increasing international dissension and tension.

This risk is a function of two factors that I will label substantive friction and procedural friction. These are examined individually in the subsections below.

A. SUBSTANTIVE FRICTION

The term “substantive friction” here refers to difficulties created when the terms of laws or policies are alien to a group upon whom they are imposed. In the case of data privacy, the more Europe’s values differ from the values of other regions, the more the Directive’s threat to data flows will be resented in those regions. Conversely, the greater the global concurrence regarding fundamental privacy rights, the less officious one region’s efforts to organize common beliefs into law and public policy will seem. In terms of international relations, the Directive is likely to be well
received, and to appear as a form of leadership, if it builds on a solid foundation of preexisting community values. This perception of leadership gradually deteriorates into perceptions of overreaching, bullying, and aggression the more third-party nations disagree with the fundamental philosophy behind the Directive.

This is certainly a real risk in regard to the EU’s data-flow restrictions. At first glance, data privacy seems fairly straightforward and not very controversial. But consider just one of many possible objections, rooted in fundamental cultural differences: that aggressive data privacy protections undermine a countervailing “right to know.” Nowhere is this latter right taken more seriously than in the United States. Our First Amendment speech protections reflect the very strong values we place on discourse, knowledge, and exchange of ideas. Central to these objects is a profound belief in the value of information—a belief that, if anything, has grown rather than diminished in the age of the computer. One person’s privacy diminishes another person’s right to know, and vice versa. Neither right would ever be considered absolute by anyone save extremists. Nonetheless, the US and Europe are quite far apart in the relative weights they assign to these two conflicting rights. Not surprisingly, Americans often shrug away suggestions that they should be concerned about marketers’ use of data—indeed, how many of us even bother to opt out of such processes? This scenario is very dissimilar to Directive opt-in provisions for European consumers. US business interests have a lot to lose when the EU Data Privacy Directive asks for fundamental changes in the ease with which marketing data can be garnered, sold, and used. Substantive friction is likely to be considerable in this context.

B. PROCEDURAL FRICTION

Even when substantive friction is minimal, the procedures through which an otherwise acceptable law or policy is created and imposed can cause conflict. I use the term “procedural friction” to refer to this form of conflict. Of course, both forms of friction can exist simultaneously as well, and the values of two cultures would have to be remarkably well aligned for procedural friction to exist entirely in the absence of substantive friction.

Nonetheless, let us assume for a moment an instance where that is precisely the case: an external sovereign authority is imposing its will on actors in other sovereignties, but the provisions and terms of the imposed will are perfectly compatible with the cultures upon which they are imposed. There is nonetheless a problem: potential resentment, even hostility, over presumptions, attitudes, and power relations.

Some may see aggressive national or regional stances as presumptuous. They may then interpret the perceived overstepping as anything from a breach of etiquette to a serious absence of protocol. Where in this spectrum a particular aggressive act falls can be a function of things like prior general relations between two countries or
regional alliances, and specific antecedents in the form of previous presumptive stances related to other international policy issues.

An aggressive international policy stance also can communicate attitudes, both toward the rest of the world generally, and toward regions or nations specifically. For example, a domineering leadership position can suggest attitudes of superiority. The subtext in this instance is, “We are better than you, therefore our solution to this policy problem will be superior to any that you might devise.” Likewise, forceful initiative can suggest attitudes of patronization, where the message perceived is, “Someone needs to take care of the rest of the world, or particular nations or regions specifically, and we must step up to the challenge in your own best interests.” Needless to say, these two examples of superiority and patronization would likely engender resentment from those on the receiving end. It bears reiterating here that the issue of attitude communication in regard to international relations concerns the perceptions of the receiver of the message, even if the sender of the message is entirely innocent of received slights or offenses. Even the most innocent of policy leaders can find its policies a source of hostility if the message received is not the one they intended to convey.

Finally, aggressive leadership in setting global policies is likely to carry messages regarding power relations. In one sense, a nation’s or region’s mere decision to take such a leadership role is tantamount to the unilateral accession of authority, and the unilateral pronouncement that the nation or region believes it has the force to carry out its mission. Otherwise, the mission would be a fool’s errand, and even if a nation or region does not have the power implicit in the move it is taking, it probably believes it has the power and is not reticent to announce to the world that it has the power. The receiving end of one region’s power is other regions’ submission—this is a scenario custom-made to engender fear, suspicion, and attempts to rectify the power imbalance.

Do these risks then mean that a regional alliance like the EU should not act as it has in taking a leadership position in the area of data privacy protection? Not necessarily. I have used the phrase “aggressive leadership” in this article. I chose a term intentionally ambiguous in that it doesn’t clearly suggest a posture that is good or bad. Leadership is generally viewed as a positive quality; aggression, at least in the context of international relations, is generally considered a negative one. Whether the good associated with leadership trumps the bad associated with aggression will be a function of context. And assessing context will be a delicate matter.

I have already suggested that one critical variable is the degree to which global participants have already converged onto an arena of common ground. The stronger the foundation of globally shared norms, values, and beliefs, the more likely the posture will be viewed predominantly for its leadership attributes instead of its aggressive approach. This makes sense intuitively, and it can also be explained in terms of community.
One way a well functioning community can be defined is in terms of shared norms, values, and beliefs. The greater the global convergence in these areas, the stronger the sense that a world community exists. In this context, the nation or region that takes a leadership position is seen less as an outsider, and more as a community member that has undertaken a difficult task in the interest of that community.

Where does this leave us? We already have seen that technology demands fast, effective spillover management, which certainly can be provided by an effective (and implicitly unilateral) leader. Extant multilateral entities such as the WTO and United Nations may be both too parochial and too unwieldy to meet these speed requirements. Indeed, this may explain why the EU has taken a leadership role in addressing data privacy around the world. However, the risks of unilateralism, including global friction, resentment, and hostility will only begin to decrease as we move closer to building a true global village.