Henry Farrell
Max Planck Project Group
Bonn

HYBRID INSTITUTIONS AND THE LAW: OUTLAW ARRANGEMENTS OR INTERFACE SOLUTIONS?

Comments welcome: farrell@mpp-rdg.mpg.de

Much recent discussion of electronic commerce (e-commerce) policy focuses on forms of hybrid regulation which involve both state and private actors. John Dryden of the OECD describes such institutions as the coming wave, allowing states to set broad principles, and thus to protect the general interest, while delegating the specifics of enforcement to private actors, who may be able to address policy concerns in a more flexible and effective manner (Dryden 2000). This approach, however, has its critics. Some scholars see the new reliance on private actors as symptomatic of the state's abdication of general social responsibilities, in the face of pressure from private forms of governance which reflect commercial, rather than public, interests (Cutler 2000). Others, while less critical in principle, point to the many ambiguities in these new forms of relationship between state and private actors. Many of these criticisms turn more generally on the relationship between the law and private governance. In contrast to existing forms of co-regulation or private interest government at the national level (Streeck and Schmitter 1985, Mayntz and Scharpf 1995), international forms of hybrid regulation are not bedded down in a strong legal order. Not only has the status of international law always been a subject of contention among legal scholars (Beck 1996), but many forms of hybrid regulation, including the Safe Harbor arrangement discussed in this article, have their basis in quasi-formal or informal agreements among states rather than treaties or other binding international instruments. Thus, the relationship between these forms of regulation and more conventional legal instruments remains uncertain.

This article sets out to study one such hybrid institution, the EU-US Safe Harbor arrangement on privacy and data protection, in order to arrive at some preliminary conclusions about how such institutions may relate to the kinds of law and formal regulation more usually studied by political scientists and legal scholars. Broadly speaking, lawyerswho have engaged with this set of topics have usually asked whether law is being replaced by new modes of governance, or whether traditional forms of law, on the contrary, are re-asserting themselves. Johnson and Post (1996), for example, in a widely cited article, contend that new communications technologies are creating spaces of social interaction which are beyond the reach of law as it is commonly understood. Jack Goldsmith (2000), in reply, points to the success

of national legal systems in reasserting control, in areas such as privacy and content regulation. As I have argued elsewhere at greater length, debates about whether new communications technologies are strengthening or weakening states are not very well suited to providing insights about new forms of hybrid regulation. Hybrid regulation is difficult to understand as a strengthening or a weakening of state authority; instead, it is a modest but real transformation of this authority (Farrell 2001a).

In this article, I suggest a new and different perspective about the sources and nature of hybrid regulation. Hybrid institutions do not reflect either the weakening of the state (and its consequent need to rely on private actors), or the fundamentally new policy problems posed by e-commerce. Instead, I argue that these hybrid solutionsrespond to the increase in interdependence resulting from globalization and the spread of new communication technologies. I then seek to document this with reference to a specific case study; the Safe Harbor arrangement reached between the European Union and United States in the area of privacy protection. I conclude by discussing the implications of my perspective for studies of the relationship between law and new communications technologies.

Globalization, Technology and Institutional Change

Hybrid institutions are central to current debates about the governance of e-commerce. Both scholars and policy makers are interested in the circumstances under which public and private actors can come together in order to solve public policy problems at a global, as opposed to merely national level. These proposed solutions may be understood in two, quite different lights, according to one's theoretical perspective on the problems that they are supposed to be addressing in the first place.

On the one hand, the new reliance of state actors on private actors may be seen as a response to the weakening of the law in the face of globalization and new communications technologies. The argument goes that these forces have led to the creation of new social spaces, where sovereign actors have only limited power to underpin their claims to legitimate authority. "Cyberspace," that much over-used term, is understood by some legal scholars not only to be a

new social realm which is largely free-standing of the law,[5] but also to undermine the law in many of the areas of social life where it has traditionally held sway.[6] To the extent that the power of states to govern has been eroded, they may naturally be forced into new alliances with private actors. Under this interpretation, the emergence of hybrid forms of regulation may be seen as a symptom of a broader crisis in in states' ability effectively to exercise their traditional sovereignty. States have little choice but to hand over important governance functions to private actors.

On the other hand, one may interpret the emergence of hybrid institutions as a response not to the weakening of the effective grasp of the law, but of increasing interdependence among different systems of law. This second interpretation points to a different set of factors bound up in globalization and technological change (Berger 2000); the way in which they create new cross-national flows, which bring previously isolated forms of social regulation into contact, and potentially into conflict, with each other. Under this interpretation, hybrid solutions play a rather different role. They are not responses to the weakness of states, so much as they are efforts by states to create modes of international regulation that allow previously existing domestic systems of order to co-exist together in relative peace, while allowing increased interchange between them. There is precedent for such arrangements within the European Union's regulatory policy, as documented by Fritz Scharpf (1994). The 1985 White Paper on the Internal Market led to a substantial change in the style of regulation within the European Union, which sought to move away from previous lengthy and difficult efforts to harmonize the regulation of all member states. Instead, under the new approach, the Council of Ministers decided on legally binding "principles" but left the detailed specification of these principles to non-governmental committees on standards. This made it easier to reach agreement in the Council of Ministers, and also left it up to firms whether they wished to conform to the final technical norms or not.

---

[5] I wish to bracket the underlying question of whether "code" may be understood as a form of "law" while acknowledging the invaluable contribution of Lessig (1999) to this important theoretic issue.

[6] The literature on this subject is vast; Johnson and Post (1996), and Froomkin (1997) are among the more sophisticated and interesting legal scholars adopting this perspective.

Scharpf describes this as an "interface solution" - it allows for some degree of coordination across quite different national systems, without either requiring these national systems to introduce new formal rules, or necessitating hierarchical enforcement. Under this explanation, hybrid institutions represent an effort to create interfaces between different legal systems which are becoming increasingly interconnected due to globalization.Hybrid institutions should seek to allow the necessary minimum of coordination to prevent forms of regulation in one system from having negative repercussion in another, without at the same time imposing a "one size fits all" hierarchical solution.

These two logics not only suggest quite different origins for hybrid institutions; they also lead to different predictions about their consequences. Under the first interpretation, hybrid institutions mark an uneasy point of transition between traditional formal modes of regulation, and the new private modes of regulation which are becoming increasingly dominant in those policy areas touched upon by e-commerce, new communications technologies and globalization. Hybrid institutions here are attempts by sovereign authorities to co-opt the outlaws, the private actors who are creating their own social spaces, compromises which dilute the legal order in order to maintain some control over social processes. Under the second interpretation, their significance and consequences are quite different; they are interfacesin which different legal orders seek to create institutions that will minimize the downside of interdependence.

In the next two sections I will seek to examine the origins of one, quite prominent hybrid institution, the so-called "Safe Harbor arrangement," in greater detail. I will begin by examining the origins of Safe Harbor in the European Union's Data Protection Directive, and efforts to implement those requirements of the Directive that had external implications. I then go on to examine the Safe Harbor itself, and its enforcement characteristics. I conclude by arguing that Safe Harbor represents a relatively pure example of a hybrid institution which has emerged from the need to create an interface between two rather different systems of legal order. I show that Safe Harbor enforcement not only seeks to fulfil the objectives of law, but also rests on assumptions about the existence of a legal order within the United States. Thus if Safe Harbor is any guide, while hybrid institutions represent an important challenge for the study of law, they do not imply the obviation of law in its traditional sense. Instead, they not only seek to sustain

pre-existing legal orders, but actually depend on these orders if they are to function properly.

The EU Data Protection Directive and Its Requirements

The Safe Harbor has its origins in the European Union's so-called "Data Protection Directive," or, to give it its full title, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.[9] This directive had its origins in the intersection between data-protection, which had become a concern for many European states, especially France and Germany, during the 1970's and 1980's, and the single market process.[10] The efforts of individual states to protect the data of their citizens was increasingly coming into conflict with the creation of the single market, as data protection officials in member states acted to forbid the export of data to other member states which did not provide similar legal protections (Regan 1999). Accordingly, a Directive was introduced which was intended to bring coherence to data protection practices across the European Union, and thus prevent privacy issues from impeding market integration. The Directive provided rights to "data subjects," individuals on whom data had been gathered, and who could be identified directly or indirectly from this data. It also mandated responsibilities for "data controllers," those persons or entities which had control over the processing of personal data, as well as recipients of such data. Furthermore, the Directive required member states to have public authorities monitoring the application of provisions on data protection, and endowed with investigative powers and the power to engage in legal proceedings when the provisions relating to data protection had been violated, or to bring the violation to the attention of judicial authorities.

Most pertinently for the later history of Safe Harbor, the Directive placed restrictive

---

[9] Official Journal L281, 23/11/1995, pp. 31-50.

[10] See Bennett (1992), Mayer-Schönberger (1997) on the policy processes through which Western European states came to introduce formal legislation to protect the data of their citizens.

conditions on the export of data to third countries which did not provide "adequate" protection for it.[12] The reason for this was clear; European policy makers were worried that new communication technologies made it possible for private actors, especially firms, to evade the Directive by transplanting their operations offshore. Thus, the Directive sought to limit data flows so as to make this option unattractive. Adequacy was to be considered in light of the circumstances surrounding a data transfer, the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the 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"(Art. 25, Data Protection Directive). When the Commission found, under the strictures of a comitology procedure, that a third country did not provide an adequate level of protection, Member States were to prevent any transfer of data of the same type to the third country in question. Simultaneously, the Commission was to enter into negotiations with the third country with a view to remedying the situation. Alternatively, the Commission could find that a third country provided an adequate level of protection, "by reason of its domestic law, or of the international commitments it has entered into, particularly upon conclusion of [negotiations with the Commission]"(Ibid.).

A number of derogations were possible from the adequacy requirement. However, these derogations were intended to be interpreted narrowly; in the words of a Commission official, the exceptions were "tightly worded and unlikely to be applicable to the majority of situations."[15] Thus, the Data Protection Directive potentially imposed a quite substantial burden on exporters from third countries which did not have adequacy judgements, or which had been found to be inadequate.[16]

---

[12] The first draft of the Data Protection Directive had included the stronger provision that third countries had to provide "equivalent" protection. After furious lobbying by US firms, this requirement was watered down to "adequate." See Regan (1999).

[15] Ulf Brühan, quoted p.46, Swire and Litan (1998).

[16] In the event, the Commission has not to date formally judged any regime to be inadequate, instead preferring to engage in negotiations with third countries before making an

In short, the issue of data transfers to third countries remained a thorny one; these countries either had to meet the standard of adequacy, or else potentially suffer data blockages. Firms within countries that did not meet the adequacy requirement and were unlikely to make the required reforms had few ways to protect themselves from EU action. These problems were especially marked in the EU-US relationship; while the US was the EU's largest trading partner, it also had adopted a relatively *laissez-faire* approach to privacy protection. Some policy makers and analysts advocated the development of model contracts, with clauses aimed to protect the privacy of EU citizens. The Directive provided in principle for contractual solutions that would allow the data of European citizens to be exported; such contracts would in principle bind the exporting firms, and give legal recourse to citizens whose privacy had been violated. The Commission could approve a set of model contract clauses which could then be inserted as boilerplate into contractual agreements which involved the export of personal data. While some European data protection officials had originally been uncertain about the virtues of model contracts, as their thinking evolved, they began to acknowledge that such contracts could serve in many situations (DPWP 1998, Swire and Litan 1998). Indeed, there was an important precedent for the use of such contracts from the era before the Directive, the *Citibank-Bahncard* controversy, where a German data protection commissioner had only allowed the export of data to the US after contractual safeguards had been put in place.

Contracts potentially offered a solution to the clash of regulatory cultures between the EU and US. However, EU and US officials, for different reasons, were unwilling to place too much reliance on model contracts. First, such contracts were clearly more suitable to some kinds of data than others; most particularly, they were suited to data which was transferred in a repetitive fashion by large firms which had to operate in a relatively transparent manner, most prominently personnel data.[17] Second, there was some reluctance among some EU data protection officials, which lessened over time, to give too important a role to contracts, which were seen as being a stop-gap and partial arrangement, much inferior to the kinds of wide-sweeping changes which

---

adequacy judgement, rather than on the basis of an unfavourable judgement as the Directive seems to intend.

[17] Interview with European Commission negotiator, June 2000.

they wished the US to make.[18] Third, US negotiators for their part were reluctant to accept contracts as a solution insofar as they imposed an additional administrative burden on firms, were unsuitable to many kinds of data, and strongly implied that the US system of privacy protection was flawed and inadequate. Thus, while the European Commission began to discuss model contracts with the International Chamber of Commerce, culminating in a set of model contract clauses issued by the Commission in June 2001, few believed on either side of the Atlantic that contracts could offer a general solution to EU-US disagreements on data protection. Attention began to focus once more on adequacy, and the circumstances under which the US could receive an adequacy judgement.

European data protection officials, who played an advisory role in the European Union's decision-making processes on third party adequacy, had already begun to think through some of these questions in a series of documents on the adequacy question, issued through the Data Protection Working Party (DPWP) (see DPWP 1997, 1998). The Data Protection Directive envisaged that adequacy could be established with regard to individual transfers, or categories of transfers. However, data protection commissioners, who were well aware of their own limited resources, perceived that this would be impracticable, and argued the need for rationalizing mechanisms (DPWP 1997). They argued that a "white list" could be drawn up of countries which could be assumed to ensure an adequate level of protection. They acknowledged that this approach had its own problems; specifically, they pointed to the difficulty of handling counties such as the US, which accorded only specific sectoral protections to privacy on this basis. While privacy might be adequately protected in some sectors in the US, it might not be protected at all in others. The Working Party proposed a list of principles on which adequacy could be judged - purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition, and restrictions on onward transfers to third countries (DPWP 1997). Enforcement should provide a good level of compliance with the rules, support and help to data subjects in the exercise of their rights, and appropriate redress to injured parties. These principles and enforcement characteristics could be used by EU authorities to assess adequacy in

[18] Many who were sceptical about contracts turned out to be more sceptical still about the

third countries; data protection commissioners envisaged themselves playing a rather larger role in this process of assessment than the drafters of the Directive had perhaps intended.

In later work, the data protection commissioners considered more closely the circumstances under which industry self-regulation might qualify for adequacy (DPWP 1998). The Directive required that account be taken of non-legal rules that are complied with in a given sector. Important criteria included whether the body which was responsible for the code was representative of the sector, the level of compliance among industry members, the presence of genuinely dissuasive sanctions for non-compliance (or at least a system of rigorous external verification), support for individuals with complaint, and individual redress. These criteria were difficult to meet, especially for self-regulation in the US context, which has provided notoriously weak protection for privacy (Froomkin 2000). Indeed, self-regulatory codes in industries such as direct marketing have not only had weak requirements in and of themselves, but have been honoured more in their breach than their observance (Rotenberg 1998).

Thus, the Data Protection Directive posed serious difficulties for US firms and the US administration. While it required adequacy rather than equivalence, adequacy was defined so that it required quite a high threshold of privacy protection. European data protection commissioners interpreted the Directive in a manner unsympathetic to the US system of self-regulation; while self-regulatory solutions to privacy were permissible under the Directive, they had to reach much higher standards than US self-regulatory schemes had traditionally aspired to, let alone accomplished. Contractual solutions, while possible for certain forms of data transfer, were not suited to provide a general solution to the problems faced by US firms which needed access to the personal data of European citizens.

The Safe Harbor Arrangement

The potential impact of the Directive increasingly became a worry for US firms and policy makers over the course of 1998, the year when the Directive came into effect. It was relatively clear that the US had less stringent protections in many, perhaps most economic

---

Safe Harbor arrangement itself.

sectors, than the European Union (Swire and Litan 1998, Cate 1997). Most pertinently, the US had no equivalent to the cross-sectoral privacy laws and data protection authorities mandated by the Directive (Cate 1997). Finally most US self-regulatory initiatives fell far short of European requirements. Under these circumstances, there was good reason to believe that the US had little chance of receiving an adequacy judgement. The US administration initially sought to persuade the EU to delay the Directive, threatening WTO action, and lobbying individual member states, but had little success in persuading the Europeans to back down. Indeed, given the complex decision making system in the EU, it is difficult to see how US pressures could have had more than a marginal effect in preventing the Directive from coming into force. The EU, for its part, made it clear that the US would only receive an adequacy judgement after making substantial changes to its domestic privacy policy. Specifically, the Europeans wanted the US to introduce a comprehensive privacy law, and independent officials to enforce it.

Under the circumstances, there were no clear solutions that could meet both EU and US objectives. While both sides were willing in principle to find an acceptable compromise, no such compromise was immediately apparent. The breakthrough came through an American suggestion; that the adequacy judgement did not have to apply to the US system as a whole, but could rather be applied to a specific scheme, to which US firms could voluntarily sign up.[26] US firms which committed to adhere to a specific set of privacy principles, and to subject themselves to credible enforcement mechanisms, might be considered to be in "Safe Harbor" for the purposes of the Directive, and thus need not fear summary blockages in their data flows. EU Commission officials were intrigued enough by this proposal to start serious discussions about how it might work in practice. While negotiations lasted far longer than either side originally anticipated, stretching from late 1998 to early/mid 2000, they eventually culminated in agreement on the Safe Harbor arrangement as a means to privacy protection.

Safe Harbor in its final form, consists of seven principles.[27] These are (in summarized

---

[26] I discuss the genesis of the Safe Harbor arrangement at greater length in Farrell (2001a, 2001b).

[27] The Safe Harbor Principles, as all other official Safe Harbor documents discussed in

form)

(1) Notice - An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization, the types of third parties to which it discloses information and the choices and means the organization offers individuals for limiting use and disclosure.

(2) Choice - An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party, or (b) whether it is used for a purpose incompatible with the purpose for which it was originally collected or authorized. For certain kinds of sensitive information, individuals must be given opt-in choice.

(3) Onward transfer - Organizations must apply the notice and choice principles if they disclose information to a third party. It may transfer information to a third party when that party subscribes to the Principles, is subject to the Directive, or enters into a written agreement to provide at least the same level of privacy protection required by the Principles.

(4) Security - Organizations must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration and destruction.

(5) Data integrity - Personal information must be relevant for the purposes for which it is to be used, and organizations must take reasonable steps to ensure that data is reliable for intended use, accurate, complete and current.

(6) Access - Individuals must have access to personal information about them that an organization holds, and be able to correct, amend or delete that information where it is inaccurate.

---

this section, are available at www.export.gov/safeharbor (checked Dec 6, 2001).

(7) Enforcement - Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals affected by non-compliance, and consequences for the organization where the Principles are not followed. Such mechanisms at a minimum must include readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved. Sanctions must be sufficiently rigorous to ensure compliance.

Safe Harbor has a quite complex enforcement system. It relies on a mixture of self-regulation and legal enforcement. On the one hand, Safe Harbor is itself a voluntary arrangement. It also (as described below) provides firms with the option to sign up to private dispute resolution bodies rather than state authorities, to provide enforcement. On the other hand, Safe Harbor is firmly embedded in the US legal framework. Furthermore, insofar as it seeks to meet the requirements of the Data Protection Directive, it is responsive to the strictures of that legal instrument.

<Fig 1. about here>
Figure One.

As figure 1 shows, Safe Harbor provides two possible enforcement options for firms which sign up to it.[29] On the one hand, they may elect to cooperate with European Data Protection Authorities (DPAs) in the investigation and resolution of complaints brought under Safe Harbor. On the other, they may elect to cooperate with independent alternative dispute resolution providers, specialized self-regulatory organizations.

If firms commit to cooperate with DPAs, they must agree to comply with any advice given by the DPAs, where the DPAs take the view that the organization must take action to

[29] A third possible option is mentioned in the Safe Harbor documents; committing to cooperate with an appropriate US regulatory authority. However, there is no such authority; EU negotiators included this option against the day when the US would introduce more extensive formal protections for privacy.

comply with the Safe Harbor principles, including remedial or compensatory measures for individuals affected by non-compliance. The DPAs deliver their advice through an informal panel of DPAs established at the European Union level. While there is little official information available on the specific form that this panel will take, interviews suggest that it will involve three national DPA's; the DPA of the country of citizenship of the individual complaining of non-compliance, and two others. Advice will only be delivered after both sides in a dispute have had a reasonable opportunity to comment and provide evidence; as a rule, the panel will aim to provide advice within 60 days of receiving a referral, and more quickly where possible. If an organization fails to comply with DPA advice within 25 days of its delivery, and has offered no satisfactory explanation, the panel will either give notice of its intention to submit the matter to the Federal Trade Commission (FTC) or another relevant federal or state body, or will conclude that the agreement to cooperate has been seriously breached, informing the Department of Commerce so that the Safe Harbor list can be amended, and leaving the organization open to further FTC action.

Firms may also opt to meet the enforcement principle's requirements through cooperation with independent recourse mechanisms. The Safe Harbor arrangement does not provide a list of acceptable recourse mechanisms, or a formal process of review for such mechanisms.[30] Instead, in a list of Frequently Asked Questions it inter alia sets out basic requirements which such recourse mechanisms should fulfil. They should be independent, and provide readily available recourse and information to individuals about how the procedures work. In the event that a dispute resolution provider manifestly fails to meet these requirements, the European Union reserves the right to announce that an agreement to comply with this provider is not considered sufficient for Safe Harbor membership. There are already a small number of specialized privacy dispute resolution providers, most prominently TrustE, and the BBBOnline privacy seal programme. In addition, some self-regulatory organizations, such as the Direct Marketing Association, have set up Safe Harbor dispute resolution mechanisms for their members. In the

[30] European negotiators pressed hard for such measures, but faced obduracy on the part of US negotiators, who refused to commit the administration to engage in the formal review of self-regulatory organizations.

event that a firm fails to comply with a dispute resolution provider's judgement, it may be liable not only to the specific penalties exacted by this provider, but to wider legal action in the law courts, or through the FTC.

Thus, even when the firm commits to comply with a self-regulatory dispute resolution organization, rather than European Data Protection Authorities, it is still subject to legal sanctions if it breaks its Safe Harbor commitments. Here, the FTC plays a key role. Section 5 of the FTC Act prohibits "unfair or deceptive practices" affecting commerce. This does not allow the FTC to police privacy in a prescriptive manner; the FTC cannot tell firms that they must adhere to a specific privacy policy. What the FTC can do, is to police the privacy commitments that firms have made. In other words, if a firm publicly commits to adhere to a specific privacy policy, and then fails to live up to this commitment, it may be considered to be engaging in unfair and deceptive practices, and thus be liable to FTC sanctions. The FTC has made it clear in side-letters to the Safe Harbor arrangement that firms' commitments to Safe Harbor may be considered to be public commitments in the relevant sense. Thus, firms which sign up to the Safe Harbor commitments, and commit to cooperate with dispute resolution providers, or with European DPA's, and then fail to live up to their commitments, will be liable to FTC action.[31] The FTC may also have jurisdiction over alternative dispute resolution providers. FTC action may include "cease and desist" orders, the seeking of temporary or permanent injunctions, or, in especially egregious cases, administrative rules proscribing practices.

The FTC has committed to give priority to complaints from alternative dispute resolution organizations such as BBBOnline and TrustE, regarding possible violations of Safe Harbor commitments. Further, it has committed to give priority to complaints from European data protection authorities. Thus, FTC enforcement is intended to provide a crucial "backstop" for self regulation in the Safe Harbor arrangement, and to ensure that firms and live up to their stated commitments.

The Safe Harbor arrangement also provides for a limited role for direct action by European data protection authorities. If there is a substantial likelihood that the Principles are

---

[31]However, Joel Reidenberg (2001) suggests that the FTC would be going beyond its

being violated, there is an imminent risk of grave harm, the company in question has had a chance to respond, and US authorities have not taken action, it remains possible for DPAs to block data flows to Safe Harbor members. These conditionsare quite stringent, at the insistence of US negotiators.

Safe Harbor came into effect on November 1, 2000. So far, it has failed to attract the large number of firms that were predicted. Over twelve months, only some 140 firms have signed onto the Safe Harbor list. These include some major US firms; Intel, Microsoft, Hewlett-Packard, Compaq and Gateway in the information technology sector, Eastman-Kodak and Procter and Gamble in consumer products, and Dun & Bradstreet and Acxiom in the information brokerage industry. However, there is little doubt that these figures are disappointing. Interviews suggest that the low sign-up rate stems from three factors. First, the EU still has in place an informal standstill, whereby it will seek to avoid taking action against US firms when at all possible, in order to allow them decide whether to sign up to Safe Harbor. As long as this standstill holds, US firms have no immediate reason to sign onto the arrangement. Second, ambiguities in the details of enforcement persist; many firms prefer not to sign up to Safe Harbor until they are sure precisely what it is that they are signing up to. Third, some firms, especially multinationals whose primary concern was employee data, have been unwilling to sign up to Safe Harbor until they could fully evaluate their main alternative; model contracts. Now that the contracts have been issued, and are relatively unattractive from the point of view of US firms,[32] some doubters may be expected to sign on.

Conclusions - Safe Harbor and the Law

In the beginning of this article, I suggested that there were two ways in which one could understand the origin and effects of hybrid institutions. On the one hand, one could see them as attempts to come to terms with the new power of private actors which involved the watering

---

jurisdiction in enforcing the privacy rights of European citizens.

[32] The model contract clauses have been described as "Safe Harbor plus," and present greater restrictions on firms than the Safe Harbor arrangement.

down of the law, in favour of new, self-regulatory arrangements. On the other, one could see them as efforts to create interfaces between different regulatory systems which were coming to interfere with each other in a context of increased cross-border contacts and communication.

It should be quite clear from the foregoing discussion that Safe Harbor more closely fits the second than the first interpretation. I have not, in this article, sought to describe the forms of interaction between public and private actors which Safe Harbor involves in any detail. However, there is little evidence that Safe Harbor had its roots in the burgeoning power of private actors in this sector. Instead, it appears much more closely related to the specific difficulties faced in resolving incompatibilities between a system of governance (the European Union) which relied on the formal, legal governance of privacy, and a second system (the United States) which relied on self-regulation in many sectors of the economy, to the extent that it relied on anything at all (see Farrell 2001a). The European Union, in order to maintain an effective system of domestic privacy legislation in an era of globalization, had to impose conditions on the export of data concerning European citizens, only allowing such export to countries which provided an adequate level of protection. However, this threatened to impose substantial external costs on third countries, which were effectively faced with the choice of either seeking to come into conformity with EU requirements, or facing unpredictable data blockages regarding information on European citizens.

Safe Harbor sought to bridge the conflicting needs of the EU and US through creating a legislative "interface" between the two. Effectively, it sought to address the needs of European authorities in a manner which involved as little indirect change as possible for the US self-regulatory system. Accordingly, it incorporated self-regulation in a manner somewhat akin to that of internal EU regulatory interfaces, in which governments come together to set broad principles, which are then fleshed out and implemented in practice by private bodies, and adhered to (or not) on a voluntary basis by firms who wish to secure themselves from action by legal authorities (Scharpf 1994). If Safe Harbor is at all representative (which can only be established through further comparative study), hybrid institutions seem more a product of increased interdependence (and lawmakers' efforts to come to terms with this interdependence) than with the weakening of the state *per se*.

By more closely examining the origins of hybrid institutions such as Safe Harbor, we may also reach interesting conclusions about their effects. At first, arrangements such as Safe Harbor seem to be "outside" the law. Clearly, they are not formal law in *strictu sensu*. Indeed, they do not even have the ambiguous status of treaties which supposedly bind sovereign entities on the principle of *pacta sunt servanda*. However, on closer examination, their ambiguous status springs not from their extra-legal status, as from their uncertain position mediating *between* different legal systems. Safe Harbor, while not legally binding, is deeply conditioned by the two legal systems that it seeks to bridge.

Safe Harbor, as I have sought to document at length, springs from the specific requirements of the Data Protection Directive. Further, it has legal status under the Directive, at least in the European Union. While it does not provide the same level of privacy protection as the Directive itself, or the formal institutional framework which the Directive lays down as necessary for states within the European Union, it is not intended to do either; the Directive does not seek equivalence, but merely adequacy. In other words, the Directive was deliberately designed so that it could flexibly accommodate a variety of possible ways of achieving privacy protection in data exports outside the European Union, even while it created a broadly coherent set of privacy rules and practices within the EU itself. Safe Harbor's continuing existence is also rooted in the Directive. Should the Commission determine in the future that Safe Harbor fails to meet the requirements of adequacy, it maydeclare that the Safe Harbor arrangement no longer satisfies the adequacy requirement, and effectively render the arrangement null and void.

Further, the Safe Harbor arrangement is anchored within the legal framework of the US. Safe Harbor does not as such have official status, beyond being a general guidance offered by the Department of Commerce. But firms which sign up to Safe Harbor will find themselves potentially liable to legal enforcement should they fail in the future to abide by their commitments. As my discussion of enforcement showed, the role of the Federal Trade Commission is paramount; EU negotiators make it abundantly clear that they would never have accepted the Safe Harbor arrangement in the absence of the FTC's powers of enforcement. [34]

---

[34] Interview with Commission negotiator, September 2001.

.

This has consequences both within and without the US. Because of the crucial role played by FTC enforcement, US firms which are not subject to the jurisdiction of the FTC, or a body with similar regulatory powers such as the Federal Aviation Authority (FAA) are not eligible for Safe Harbor. To the extent that their commitments are not legally binding, and breach of these commitments is not actionable by an enforcement authority, they cannot enjoy the privileges of Safe Harbor from EU enforcement. Most prominently, many US financial firms, which are not subject to FTC jurisdiction, are currently ineligible for Safe Harbor.

Furthermore, EU negotiators have suggested that Safe Harbor type solutions may perhaps be suitable for other third countries than the US.[36] However, they have stated a crucial proviso. Safe Harbor solutions can only provide adequacy in countries where the rule of law is well established and where there is some equivalent of the FTC to provide a formal back up to self-regulation. EU negotiators hold out little prospect of Safe Harbor style solutions for those countries in the developing (or indeed developed) world which do not fulfil these criteria.

Thus, in short, Safe Harbor stands as an example of how hybrid institutions may arise from the need to bridge different systems of law, rather than the need to shore up areas of the law which are coming under threat from alternative forms of social order. As such, it is conditioned both by the European legal requirements which gave rise to it in the first place, and the US legal system on which it relies for back up for its self-regulatory elements. This is not to say that Safe Harbor is fully coherent or devoid from ambiguity; indeed, quite the opposite is true. It is to suggest that the specific ambiguities of Safe Harbor represent similar problems to those confronted by international lawyers in "choice of law," "conflict of law" and other areas where it is necessary to balance the needs of conflicting systems of law and legal interpretation. While Safe Harbor, and similar institutional arrangements, may create new problems for both lawyers and social scientists, these problems are not different *in principle* from those which characterized previous efforts to create interfaces between different systems, nor do they reflect the erosion of the law or of formal regulatory arrangements.

---

[36] Interviews with EU negotiator, September 2000, September 2001.

Figure 1

Bibliography

Beck, Robert J. International Law and International Relations: The Prospects for Interdisciplinary Collaboration. in: Beck, Robert J.; Arend, Antony Clark, and Van der Legt, R. D., eds. International Rules. Oxford: Oxford University Press; 1996.

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

Berger, Suzanne. "Globalization and Politics." *Annual Review of Political Science* 3, no. 43-62 (2000).

Cate, Fred H. *Privacy in the Information Age*. Washington DC: The Brookings Institution, 1997.

Cutler, A. Claire. *Patterns of Public-Private Interaction at the International Level: Global Governance and the Modern Lex Mercatoria*. Presented at the Conference on Common Goods and Governance across Multiple Arenas, Max Planck Project Group - Common Goods: Law, Politics, Economics: 2000.

DPWP, Data Protection Working Party. *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*. Brussels: Data Protection Working Party, 1997.

———. *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*. Brussels: European Commission, Directorate General XV, D/5025/98, 1998.

Dryden, John. "The Work of the OECD on Electronic Commerce." Web page, June 2000 [accessed 10 October 2000]. Available at

http://www.oecd.org/subject/e_commerce/Ottowa_speech.pdf

.

Froomkin, A. Michael. "The Death of Privacy?" *Stanford Law Review* 52 (2000): 1462-543.

———. "The Internet As a Source of Regulatory Arbitrage." in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure.* eds. Brian Kahin, and Charles Nesson. Cambridge, Massachusetts: The MIT Press, 1997.

Goldsmith, Jack. "Unilateral Regulation of the Internet: A Modest Defence." *European Journal of International Law* 11, no. 1 (2000): 135-48.

Johnson, David R., and David Post. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48 (1996): 1367-76.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Mayer-Schönberger, Viktor. "Generational Development of Data Protection in Europe." in *Technology and Privacy: The New Landscape.* eds. Philip E. Agre, and Marc Rotenberg. Cambridge, Massachusetts: The MIT Press, 1997.

Mayntz, Renate and Fritz Scharpf, eds. *Gesellschaftliche Selbstregelung und politische Steuerung*. Frankfurt am Main: Campus Verlag, 1995.

Regan, Priscilla M. "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics." in *Visions of Privacy: Policy Choices for the Digital Age.* eds. Colin Bennett, and Rebecca Grant. Toronto: University of Toronto Press, 1999.

Reidenberg, Joel. "Testimony."Committee on Energy and Commerce: Subcommittee on Commerce, Trade and Consumer Protection, 2001.

Rotenberg, Marc. "Testimony."Committee on International Relations, U.S. House of

Representatives: 1998.

Scharpf, Fritz W. "Community and Autonomy: Multi-Level Policy Making in the European Union." *Journal of European Public Policy* 1, no. 2 (1994): 1350-1763.

Streeck, Wolfgang, and Philippe C. Schmitter. "Community, Market, State - and Associations?: The Prospective Contribution of Interest Governance to Social Order." *European Sociological Review* 1, no. 2 (1985): 119-38.

Swire, Peter P., and Robert E. Litan. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington DC: Brookings, 1998.