

Engel, Christoph

Working Paper

Organising co-existence in cyberspace: Content regulation and privacy compared

Preprints aus der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter, No. 2002/12

Provided in Cooperation with:

Max Planck Institute for Research on Collective Goods

Suggested Citation: Engel, Christoph (2002) : Organising co-existence in cyberspace: Content regulation and privacy compared, Preprints aus der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter, No. 2002/12, Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter, Bonn

This Version is available at:

<https://hdl.handle.net/10419/85151>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



Gemeinschaftsgüter: Recht, Politik und Ökonomie

Preprints
aus der Max-Planck-Projektgruppe
Recht der Gemeinschaftsgüter
Bonn
2002/12

**Organising Co-Existence in Cyberspace
Content Regulation and Privacy Compared**

von
Christoph Engel

Table of Contents

I. From Cyberspace to Choice of Law – The Evolution of the Legal Debate	3
1. First Generation, Fundamentalist Debate	4
2. Second Generation, More Nuanced Debate	6
II. Privacy and Content Regulation – Stories of Precarious Success and of Provisional Failure	10
1. The Safe Harbour Compromise in Privacy	10
2. Provisional Failure in Content Regulation	13
III. A Rational Choice Model of Content Regulation	14
1. The Issue	14
2. Limitations of the Model	15
3. Empirical Validation	17
4. The Core Argument	18
IV. National Preferences Before the Advent of the Internet	18
1. Introduction	18
2. Degree of Protection	19
3. Evaluation	19
4. Opportunity Cost	21
5. Evaluation	22
6. Taxonomy of Values	23
7. Complications	24
V. The Impact of the Internet on National Preferences	26
1. Degree of Protection	27
a) Introduction	27
b) Impact on Old Governmental Protection Technology	27
c) Impact on Problem Solving Capacity of Nation-States	30
d) Impact on Governance Externalities	30
2. Evaluation	31
3. Opportunity Cost	31
a) Higher Opportunity Cost of Old Protection Technology	31
b) Opportunity Cost of New Protection Technologies	33
4. Concomitant Goods	34
VI. Coordination of National Behaviour in General	37
1. Win-Win Situations	37
2. Strategic Interaction Over Agreement	39
a) Nuisance Value	40
b) Multilateral Protection	40

c)	Dynamic Element	41
3.	Strategic Interaction over Implementation	42
VII.	Organizing Co-Existence in Particular	43
1.	Defining Co-Existence	43
2.	Protection Technologies	44
a)	Introduction	44
b)	Re-Introducing Nationality Barriers	44
c)	Mutual Enforcement	45
d)	Re-Inventing the Nation-State	46
3.	Win-Win Solutions	46
4.	Strategic Interaction over Agreement	48
5.	Strategic Interaction over Implementation	48
VIII.	How is Privacy Different?	49
1.	The Issue	49
2.	National Preferences before the Advent of the Internet	49
3.	Impact of the Internet on National Preferences	50
4.	Coordination of National Behaviour in General	51
5.	Organizing Co-Existence in Particular	52
IX.	Conclusions	53
	References	55

* Henry Farrell and myself originally planned a joint paper. It turned out that our convictions about the appropriate explanation for the differences between content regulation and data protection fell too far apart. Henry Farrell, however, had already written section I of this paper, which he generously agreed to leave as part of what now is my individual paper. I also am grateful to Adrienne Héritier and Katharina Holzinger for their helpful comments on an earlier version.

The Americans praised the advent of the automobile as a major breakthrough for a serious social problem – horse manure in the streets.¹ This is how well society is able to understand the social impact of a technological revolution when it happens. Many of the early legal reactions to the Internet demonstrate that the example is able to be generalized. Even the brightest minds are unable to fully grasp the social potential of a new technology at the moment of its introduction. To put it differently: forging such an understanding is itself a social exercise that many people are engaged in over a considerable period of time. Today the Internet is still an adolescent phenomenon at best. Yet the legal discourse has already matured considerably. The *basso continuo* no longer sounds “Leviathan or Behemoth.”² Rather, a multitude of legal voices are engaged, sometimes dissonantly, in a piece entitled “Organizing Co-Existence in Cyber Space”.

It has been no mean feat for the legal discourse to reach this point (as shall be discussed in section I), and not all fields of law have been equally successful in adopting the approach. Privacy provides a story of precarious success, while attempts to organize co-existence in the area of content regulation have failed thus far (section II). I offer a rational choice model to explain the difference, and to help those grappling with the impacts of the Internet better understand the stakes (section III). The model starts with content regulation, looking at national preferences before the advent of the Internet (section IV), and how the Internet changes national preferences (section V). This makes it possible to determine the opportunities for coordinating national behaviour in general (section VI), and for jointly organising co-existence in particular (section VII). Against this background, I can explain why practise was more successful in the area of privacy regulation (section VIII).

I. From Cyberspace to Choice of Law — The Evolution of the Legal Debate

Debates over the implications of the Internet¹ and related technologies for law have undergone an important shift in the very recent past. Initial discussions focused on how or whether the Internet undermined the ability of legal authorities to enforce the law, and whether “cyberspace” was indeed amenable to traditional forms of law at all (part 1). More recently, legal scholarship has begun to engage in a more complex — and potentially fruitful — set of debates. Few now believe that cyberspace will radically undermine conventional forms of law, as was predicted by some scholars in early debates. Instead, scholars are beginning to discuss the implications of the Internet for the interdependence between different jurisdictions.² Insofar as the Internet creates new forms of communication and interaction across borders, it may lead to uncertainties and ambiguities where it is unclear whether the law of one, or the law of another, jurisdiction should govern a particular transaction. This may lead to conflict between jurisdictions, and potentially to

1 I owe the graphic parallel to KENNETH KENISTON.

2 HOBBS *Leviathan* (1651)

1 The Internet, strictly speaking, refers only to the packet switching protocols underlying the World Wide Web and other forms of communication. In this paper, I use the term Internet not only to refer to these protocols, but also to the various kinds of communication and interaction that they permit.

2 FARRELL in *Zeitschrift für Rechtssoziologie* (2002).

new kinds of institutions designed to resolve these jurisdictional questions.³ However, the novelty of the solution should not distract us from the fact that these issues involve relatively well-established problems for lawyers, in particular the problems known from old debates over “choice of law” or “conflict of law,” which now reappear under a new guise (part 2).

1. First Generation, Fundamentalist Debate

In early discussions about the consequences of the Internet for law, these problems were typically only implied. The initial agenda of these debates was set by libertarians and some legal scholars who argued that cyberspace was by its nature ungovernable by traditional means and, furthermore, that traditional state regulation was normatively inappropriate.⁴ These scholars suggested that traditional forms of law relied on the territorial segmentation of physical space, which was the basis of the current system of legal sovereignty.⁵ However, they went on to argue that territorially based law was being undermined by developments in communication technology. While “location” remained important in cyberspace, it was a virtual location, which bore no necessary relation to physical geography.⁶ This meant, in these scholars’ view, that no single territorially based sovereign actor was capable of effectively asserting jurisdiction over the Internet, and thus that considerable legal perplexities were immanent. Furthermore, any attempts by sovereign authorities to claim jurisdiction were likely to fail, given the ability of actors in cyberspace to “route around” physical jurisdictions and easily relocate their activities to jurisdictions where the power of the authority in question did not apply.⁷ This ability to easily relocate activities also enhanced the power of private actors vis-à-vis states by creating opportunities for “regulatory arbitrage.”⁸

The solution, advanced on both normative and technical grounds, proposed treating the Internet as a social and legal space in its own right, not subject to the jurisdiction of traditional law.⁹ Instead, it was predicted that self-regulatory solutions, along the lines employed by the Internet Engineering Task Force (IETF) or the mediaeval Law Merchant, would arise in cyberspace to regulate behaviour and provide some level of legal certainty to transactions. Given the inability of sovereign authorities to enforce their laws, private actors would have to create their own.¹⁰

3 FARRELL in Héritier (2002) 116-118.

4 See JOHN PERRY BARLOW, A Declaration of the Independence of Cyberspace, <http://www.eff.org/~barlow/Declaration-Final.html> (3/5/2002); JOHNSON and POST in Stanford Law Review (1996); although see also POST in Stanford Law Review (2000) for a more nuanced consideration of the role of government.

5 JOHNSON and POST in Stanford Law Review (1996).

6 Ibid.in .

7 Cf. JOHN GILMORE’s famous dictum that “the Net interprets censorship as damage, and routes around it”, quoted in BOYLE in University of Cincinnati Law Review (1997).

8 FROMKIN in Kahin und Nesson (1997) ; see also KOBRIN in Dunning (1997) .

9 JOHNSON and POST in Stanford Law Review (1996).

10 SIMON NetPolicy (2000) ; for a corrective see the sophisticated reassessment of the relationship between sovereign authorities in SPAR Ruling the Waves (2001) .

Furthermore, many argued that even if government could intervene, it should not; private actors should be left to their own devices as much as possible.¹¹

These claims and pronouncements came under criticism from a variety of perspectives. Lawrence Lessig, in a widely debated monograph, argued that the libertarian position on the Internet rested on dubious empirical claims and was normatively inappropriate.¹² Lessig pointed to how the Internet — and the forms of communication that it allowed — were fundamentally dependent on the underlying technical architecture, which shaped possibilities for communication and action in a quite fundamental way. If architecture shaped possibilities, then the freedom of possibility espoused by libertarians was by no means a given; for if the architecture were reshaped, these possibilities might also disappear.¹³ Two sets of actors were particularly well-placed to reshape these architectures: Governments, now that they had come to realize the importance of the Internet, might mandate changes in underlying communication technologies that would allow them to reassert control over private actors. More insidiously, as the Internet became more and more commercialized, firms would have an incentive to create architectures that limited the power of private citizens in areas such as content control, copyright and privacy. Thus, the originally freewheeling Internet might come to be replaced by a social space which was dominated by architectures of control. Furthermore, Lessig argued that these architectures of control might effectively vitiate the rights of individuals, thus that it was necessary to reassert *collective* control of the Internet, and to seek to protect fundamental constitutional values.¹⁴

A second line of critique was offered by Jack Goldsmith, who argued that the effects of the Internet on state sovereignty were greatly exaggerated.¹⁵ States and courts still maintained their traditional means of enforcing law, especially in situations where actors maintain assets in the jurisdiction in question. Furthermore, Goldsmith, like Lessig, pointed to the possibility of new technical architectures, and in particular filtering technologies, which allow the geographical location of users to be identified, and thus might permit the partial re-imposition of “borders in cyberspace.” States might act unilaterally to prevent harm within their own borders, as for example in the EU’s Data Protection Directive, which sought to protect the data of European citizens.¹⁶ Furthermore, Goldsmith argued that not only was it possible for states to unilaterally regulate transnational relations on the Internet, but that it was normatively appropriate for them so to do under many circumstances.¹⁷

11 White House, A Framework for Global Electronic Commerce, <http://www.whitehouse.gov/WH/New/Commerce/read.html> (10/10/2000); LITAN in Duke Law Journal (2001).

12 LESSIG Code (1999) .

13 On this point, see also BOYLE in University of Cincinnati Law Review (1997).

14 Specifically, American values; one of the limitations of Lessig’s approach has been its almost exclusive concern with domestic US issues.

15 GOLDSMITH in Engel und Keller (2000) .

16 See below II 1.

17 GOLDSMITH in European Journal of International Law (2000).

2. Second Generation, More Nuanced Debate

This first generation of debate has given rise to a second one, as scholars have increasingly come to realize that the problems posed by e-commerce do not involve the weakening of law in any simple or obvious sense so much as the increasing problem of reconciling different laws and different national approaches, which are brought into conflict because of the new forms of transnational action enabled by the Internet. If the libertarian thesis that cyberspace is effectively ungovernable by states does not hold, as it apparently does not, then a two-fold problem arises. On the one hand, if, because of the Internet, activities which are permitted in one jurisdiction have negative repercussions for another jurisdiction, in which they are not permitted, then there is clearly a problem of negative spillover. On the other hand, the efforts of the second state to regulate behaviour within its own jurisdiction may (under certain circumstances) have negative consequences for the first state, insofar as the regulations may restrict the freedom of agents within the first state's jurisdiction. More succinctly put, not only may the transnational effects of the Internet give rise to harmful varieties of interdependence, the unilateral efforts of states to mitigate these problems may also give rise to second-order negative spillovers.¹⁸

Spillovers of this sort occur in different policy areas. The collection of taxes,¹⁹ copyright control,²⁰ consumer protection,²¹ and international rules governing trade²² are among the areas directly affected by e-commerce. Perhaps of most interest are those areas where interdependence has direct implications for the basic social values that are expressed in legislation, which may differ substantially across countries: most prominently in the cases of privacy and content control.²³ At the same time, clashes over fundamental values have potentially more worrying effects, and they are more intractable to potential solutions. These problems — and others — are clearly identifiable as variants of a more general set of issues, namely those issues subsumed under the heading of choice of law and more particularly under the heading of conflict of law.²⁴ However, to identify the problem is not to solve it: There is considerable controversy among legal scholars about how choice of law or conflict of law problems might best be solved, and there is no general agreement on a set of principles for addressing or even mitigating these problems.²⁵ These disagreements point to deeper theoretical issues of concern both to political scientists and to lawyers. Both choice of law problems and conflict of law problems stem from fundamental problems involved in resolving state claims to sovereignty in an international system in which some transactions cross state borders. As Joel Trachtman observes, “the durable technical legal ques-

18 FARRELL in *Zeitschrift für Rechtssoziologie* (2002).

19 MANN, ECKERT and KNIGHT *Global Electronic Commerce* (2000); COCKFIELD in *Minnesota Law Review* (2001); LITAN in *Duke Law Journal* (2001).

20 JOHNSON and POST in *Stanford Law Review* (1996); GINSBURG in *Columbia Journal of Law and the Arts* (2000).

21 WILHELMSSON, TUOMINEN and TUOMOLA *Consumer Law* (2000).

22 MANN, ECKERT and KNIGHT *Global Electronic Commerce* (2000).

23 See below II 2 and III - VII. See also ENGEL in *Engel und Keller* (2000); REIDENBERG in *Jurimetrics* (2002).

24 GOLDSMITH in *European Journal of International Law* (2000).

25 OSTHAUS in *Engel und Keller* (2000).

tions of choice of law and prescriptive jurisdiction resolve into a core normative public policy issue: how should authority be allocated within an interstate or international system.”²⁶

There are a variety of possible solutions to these profound problems, some involving the re-organization of sovereignty and/or judicial competences, others the application of rules within the pre-existing set of differing national legal systems. None of these solutions is universally satisfactory. Discussions in the literature suggest five approaches to problems of clashing jurisdictions. First, some authors – most particularly Jack Goldsmith – have argued that unilateral regulation provides a solution in and of itself to transnational problems.²⁷ Second, under some circumstances, the harmonization of national laws may provide a solution.²⁸ Third, it may be that some rule can be identified regarding the choice of forums by which transactions may be identified as falling under one jurisdiction or another.²⁹ Fourth, recourse may be made to private international law, through specifically tailored contracts.³⁰ Fifth, perhaps disputes can be resolved outside the legal system, through private systems of ordering (alternative dispute resolution).³¹

One possible solution to the problem is to proceed on the basis of traditional sovereign authority; that is, states are to take unilateral action to defend their values. This action may then be upheld by national court systems, even in situations where this action has implications for actors external to the system in question. In a series of important articles, Jack Goldsmith has explicitly defended this position.³² In his argument, not only are states, *contra* some libertarian arguments, capable of taking unilateral action to defend their domestic values and laws, they are normatively justified in doing so. Furthermore, technologies exist which may permit service providers on the Internet to identify which country their customer lives in, and thus to tailor their provision of services accordingly. However, Goldsmith’s argument has serious limitations.³³ As Yochai Benkler points out, these kinds of technology may themselves have repercussions for the fundamental values of third countries, especially those third countries that value privacy and anonymity in communications. To the extent that an information provider requires all users everywhere to identify themselves, these values are abrogated in a manner which may have substantial repercussions. Furthermore, such segregation may impose a high – and perhaps unsustainable – burden on firms that have to maintain firewalls between customers from differing jurisdictions, even when these customers have purchased identical goods or services. Finally, as Goldsmith acknowledges, unilateral action is only practicable when the firm or actor in question has assets that can be affected by the jurisdiction in question. It is by no means certain that they do; this especially applies to small, mobile firms, which can easily escape through the wainscoting of the

26 TRACHTMAN Choice of Law (2001) 1.

27 GOLDSMITH in Engel und Keller (2000); GOLDSMITH in European Journal of International Law (2000) For a defence of the right of states to take unilateral legal action with extraterritorial implications in order to defend their basic social values, see REIDENBERG in Stanford Law Review (2000).

28 GOLDSMITH in European Journal of International Law (2000).

29 GEIST in Berkeley Technology Law Journal (2001).

30 SWIRE in International Lawyer (1998).

31 SCHWARCZ Private Ordering (2002) .

32 See especially, GOLDSMITH in Engel und Keller (2000); GOLDSMITH in European Journal of International Law (2000).

33 See in particular, BENKLER in European Journal of International Law (2000).

international system.³⁴ Thus, limited unilateral action may not prove effective against certain kinds of content provision and certain kinds of privacy abuse (as, for example, email spamming). Efforts to resolve these problems, insofar as they are likely to be effective, are also likely to involve the extraterritorial application of law in a manner which may be offensive to advocates of strict state sovereignty.

A second possibility, also canvassed briefly by Goldsmith,³⁵ is to harmonize the approach among states. Clearly, this may offer a solution to some of the problems of regulatory interdependence posed by the Internet. As Goldsmith acknowledges, harmonization is likely to be difficult, and may often trample over local values. It is likely only to be practicable where there is a substantial degree of pre-existing consensus among states about how a specific area of activity ought to be regulated; and even there, reaching agreement may be very difficult.³⁶ For more controversial issues involving basic social values, harmonization is unlikely, even in the very long run. This also probably holds for other areas of regulation that reflect hard-fought social bargains at the national level, such as core issues of taxation.

A third possibility would be to identify a clearer set of rules on the choice of forum and the choice of law. Under such a rule, it might be possible to identify both the set of laws relevant to a particular transaction, and the judicial forum in which disagreements over that transaction might be litigated. However, there is little consensus on what such a set of rules might involve. In the U.S. and Canada, the traditional approach to the question of the conflict of law and the choice of jurisdiction has been to determine whether it was foreseeable that parties might find themselves litigating matters in a particular legal system. However, this metric (unless it is properly specified) does not work especially well in Internet transactions, where it is much more difficult to gauge what is foreseeable, and what is not, and where local courts may often wish to provide protection to local individuals and values.³⁷ Another approach, currently under discussion in the European Union, seeks to resolve consumer disputes in the jurisdiction of the consumer in question. This provides greater certainty and protection for the consumer – but also generates quite substantial costs for the actors selling or otherwise providing the service, who have to ensure that they comply with fifteen different bodies of consumer protection law. Understandably, firms have protested against this proposal and have sought to have draft legislation changed so that the consumer law of the country in which the provider is located applies. This may, however, impose an undue burden on the consumer, who has to litigate in a foreign system, with associated information asymmetries and increased costs. The problem is obviously multiplied if one seeks to impose the approach, either of the jurisdiction of the producer or of the jurisdiction of con-

34 SWIRE in *International Lawyer* (1998).

35 GOLDSMITH in *European Journal of International Law* (2000).

36 For example, even though a privacy regime was constructed in the 1970's and 1980's in the OECD and other international organization, which saw nominal agreement on common principles, in practice the US continued to pursue a very different approach to privacy regulation. See BENNETT *Privacy* (1992); BENNETT and GRANT *Visions of Privacy* (1999) . The regime was thus not sufficient to prevent clashes over privacy between the US and other states after the advent of e-commerce. see FARRELL in *Zeitschrift für Rechtssoziologie* (2002).

37 GEIST in *Berkeley Technology Law Journal* (2001).

sumer, internationally rather than merely within Europe. Another approach, which has in part been adopted by U.S. courts, is to seek to determine whether information was passively supplied on the Internet, or actively targeted towards individuals. Early cases in the U.S. and Canada (the *Inset* case, *Maritz Inc. v. Cybergold Inc.*, and *Alteen v. Informix Corp.*) adopted the principle that transmitting information on the Web involved a conscious decision to target all users on the Internet, and thus made it possible to assert local jurisdiction.³⁸ However, with the *Bensusan* case, an alternative line of interpretation began to develop, which sought to determine whether or not a website *actively* sought to target consumers, rather than passively provided information to all comers. This approach reached its culmination in the Pennsylvania court's decision in *Zippo Manufacturing Co. v. Zippo.Com Inc.* The court found that "jurisdictional analysis in Internet cases should be based on ... the nature and quality of the commercial activity conducted on the Internet",³⁹ rather than on the simple use of the Internet itself. This is grounded in traditional jurisdictional principles – owners of passive websites may reasonably expect not to be taken to court in jurisdictions that they do not specifically target – but most importantly, it makes "it explicit that local law still applies to the Internet."⁴⁰ More recently, the *Zippo* principle has been eroded to some extent in the U.S. as courts have begun to apply an effects doctrine, which "holds that personal jurisdiction over a defendant is proper when a) the defendant's intentional tortious actions b) expressly aimed at the forum state c) causes harm to the plaintiff in the forum state, ... which the defendant knows is likely to be suffered."⁴¹ This requires evidence that individuals within a specific state have been targeted. However, both of these rules pose problems. The *Zippo* case creates perverse incentives for actors by discouraging them from developing active websites. Geist suggests that an effects-based targeting approach provides a superior alternative, especially given the availability of technology that allows firms and others to determine the geographical location of their customers. However, this approach also falls victim to Benkler's criticism that it requires the Net to be "re-territorialized" in a manner that may have negative consequences for jurisdictions that privilege the right to privacy and anonymity.

A fourth approach might be to rely on private law and contractual arrangements in which providers and users of Internet services agree to the laws and venues governing a specific transaction beforehand. This approach may provide increased certainty in many situations. Yet, there are situations in which it is not very helpful. Choice of law and venue clauses do not always create certainty, especially in the context of the Internet.⁴² Furthermore, different jurisdictions take different approaches to the rights which individuals may or may not voluntarily relinquish through contractual arrangements: Some jurisdictions substantially restrict the ability of individuals to "sign away" their rights, and thus foresee a far more limited role for contracts, substantially restricting their degree of legal certainty. In other instances, such as privacy protection in relations between the EU and third countries, contractual clauses may only satisfy legal authorities if they provide adequate protection for the privacy of individuals, essentially reproducing many of the

38 This and the following discussion summarizes the excellent account provided in *Ibid.in*

39 *Ibid.in* 21.

40 *Ibid.in* 26.

41 *Ibid.in* 27.

42 See *Ibid.in* for more detailed discussion.

formal obligations of one jurisdiction in the language of private law, and potentially subjecting parties to such a contractual arrangement to litigation in the courts of EU member states.

Finally, some scholars and policy-makers have suggested that purely private ordering – systems of alternative dispute resolution – may provide a solution to transnational disputes involved in e-commerce. Again, such systems of ordering may have their uses, as is historically demonstrated by the considerable expansion of the private arbitration of commercial disputes, in large part motivated by choice of law problems (Stone Sweet 1999). However, they also involve important problems, especially when fundamental social rights are involved. Many who study private ordering neglect the important – and complex – relationship between arbitration and national courts, which typically serves to enforce arbitration decisions under relevant international conventions (Lehmkuhl 2001). Private ordering works best when it is embedded in an appropriate system of formal law. Furthermore, choice of forum problems may arise, in which dominant partners in a relationship (typically service suppliers) may seek to force others to accept forums of dispute resolution which tend to find solutions in a manner favourable to the domestic partner.⁴³ Finally, and perhaps most importantly, where fundamental disagreements over rights and values are concerned, private systems of ordering by no means necessarily provide a solution. However, by providing one component of an “interface” between different legal systems, they may provide part of the solution. Again, this is only possible through a direct linkage between the private system of ordering and the formal jurisdictions that it seeks to mediate.

II. Privacy and Content Regulation – Stories of Precarious Success and of Provisional Failure

1. The Safe Harbour Compromise in Privacy

Privacy regulation in the EU and in the United States differ markedly, both with respect to substance and to form.⁴⁶ It is true that at the level of very general principles, both legal orders tend to agree. But once these principles are broken down into concrete legal rules, the different approaches become visible.⁴⁷ U.S. data protection legislation is confined to isolated reactions to scandal, as in the case of video rental data. The EU data protection directive, by contrast, is a piece of omnibus legislation.⁴⁸ The divergence over procedure is even more pronounced. Europe has entrusted the implementation of data protection legislation to independent data protection officers, who have far reaching powers. Traditionally the U.S. has disliked the legal implementa-

43 Of course, this is also a problem for the choice of forum clauses that specify formal jurisdictions. There is a copious literature on the “Delaware effect” and race to the bottom problems in the protection of consumer rights. See ESTY in *Journal of International Economic Law* (2000). On bias problems and choice of forum in ICANN, see LEHMKUHL in *Zeitschrift für Rechtssoziologie* (2002).

46 For an overview see FARRELL in Héritier (2002) 118-122; NATIONAL RESEARCH COUNCIL *Global Networks and Local Values* (2002) 135-156.

47 For details see REIDENBERG in *Stanford Law Review* (2000) 1326-1336.

48 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. *Official Journal L* 281, 23/11/1995, pp. 31-50.

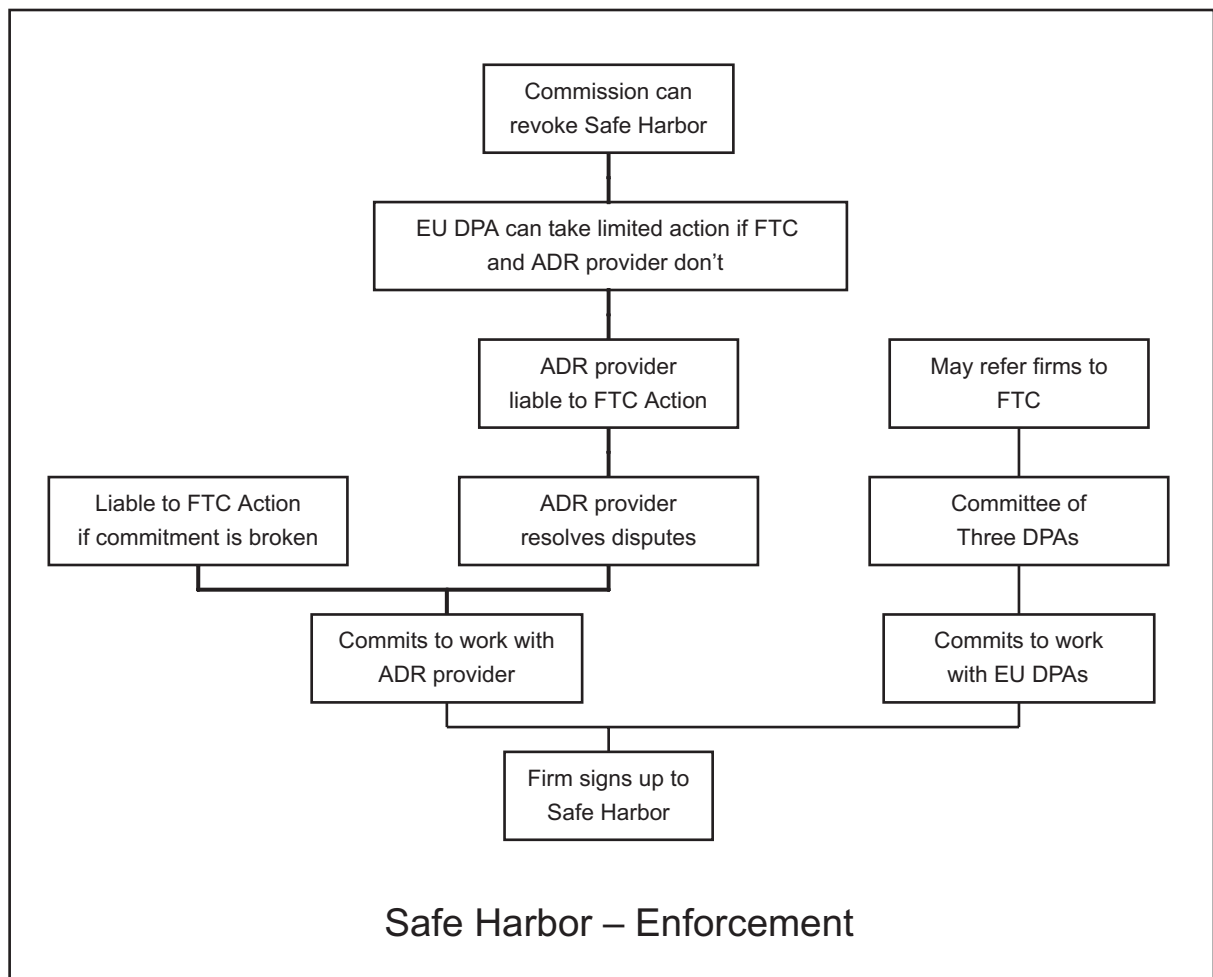
tion of data protection principles altogether. The U.S. government thought this to be best handled by industry self-regulation.⁴⁹

With the advent of the Internet, these different regulatory traditions frequently clashed. The EU directive foresaw the problem and, from its first version on, had a provision making the export of data to third countries conditional upon “adequate” protection.⁵⁰ The breakthrough in protracted transatlantic negotiations came via an American suggestion: the adequacy judgement does not have to apply to the U.S. system as a whole, but could rather be applied to a specific scheme, to which U.S. firms could voluntarily sign up.⁵¹ U.S. firms that committed to adhere to a specific set of privacy principles and to subject themselves to credible enforcement mechanisms would be considered to be in “safe harbour” for the purposes of the directive. Actually, the compromise opens up alternative routes, the details of which are summarized in Fig. 1.

49 More from FARRELL in Hérítier (2002) 118-120.

50 The first draft of the Data Protection Directive had included the even stronger provision that third countries had to provide “equivalent” protection. After furious lobbying by US firms, this requirement was watered down to “adequate” protection.

51 For details see FARRELL in Hérítier (2002) 109-112.



Legend

- EU DPA European Data Protection Authority
- ADR Alternative Dispute Resolution
- FTC (US) Federal Trade Commission

The decisive element in the compromise is the role of the U.S. Federal Trade Commission. Even if a U.S. company opts for a private, alternative dispute resolution mechanism, it cannot entirely forego the involvement of state authority; for the data owner can complain to the FTC, alleging the firm has broken the commitment made with the alternative dispute resolution body. The open flank of this elegant mechanism is participation. It came into effect on November 1, 2000. Up till now, only some 140 firms have signed onto the safe harbour list. Admittedly, these include some major U.S. firms: *Intel*, *Microsoft*, *Hewlett Packard*, *Compact* and *Gateway* in the information technology sector, *Eastman-Kodak* and *Procter and Gamble* in consumer products, and *Dun and Bradstreet* and *Ecxiom* in the information brokerage industry. However, there is little doubt that these figures are disappointing.⁵²

52 More from Ibid.in 112.

2. Provisional Failure in Content Regulation

In practical terms, data protection is a European-American conflict. There is a parallel conflict over content regulation. It also has a substantive and a procedural side. In substantive terms, the European, and especially the German public is primarily concerned with exposure to Nazi content over the Internet. The average American detests nudity and pornography much stronger than the average European does.⁵³ Again, the deeper conflict is over institutions. Even if the overwhelming majority of the public would like to ban a type of content, the American constitution still protects it.⁵⁴ The rationale of this constitutional position is uncertainty. It is never easy to discern whether some type of expression is still within or beyond the legal limits. When regulating content, the legal order therefore has to choose between two potential errors. Is it worse to tolerate speech, although it might have been forbidden? Or is it worse to forbid speech, although it should have been tolerated?⁵⁵ The American Constitution clearly considers the second error to be graver. It opts for the first and thereby against a potential chilling effect.⁵⁶

For Europe and the United States, organizing the co-existence of their content regulation would therefore be attractive. But despite the burgeoning literature,⁵⁷ there is little, if any, practical action. The European countries occasionally resort to unilateral strikes. A Bavarian lower penal court convicted the national manager of *CompuServe* for not having prevented access to indecent material.⁵⁸ A French court obliged *Yahoo* to take all reasonable technical steps to prevent access

53 The findings of a study commissioned by the Bertelsmann Foundation are telling: Jens Waltermann and Marcel Machill (eds.): *Protecting our Children on the Internet. Towards a New Culture of Responsibility*, Gütersloh (Bertelsmann Foundation Publishers) 2000. The study asked people 18 years and older in the two countries two The first concerned risks that they associate with the Internet? Each interviewee could name as many risks as he or she wanted. The responses were as follows:

Risk	USA	Germany
Data protection	22%	24%
Pornography	13%	17%
Protection of Minors	21%	6%
Fraud, Manipulation	8%	3%
Presentation of violence	2%	3%

The second question addressed attitudes toward censorship. Each interviewee was allowed to name the kinds of content that he or she would like to see banned from the Internet. This yielded the following:

Content type	USA	Germany
Racist speech	63%	79%
Violence	39%	61%
Pornography	59%	60%
Politically radical speech	26%	58%
Nudity	43%	13%

54 More from NATIONAL RESEARCH COUNCIL *Global Networks and Local Values* (2002) 106-132.

55 This inescapable choice is an old philosophical problem, see e.g. LÜBBE in Engel, Halfmann und Schulte (2002) .

56 Leading case *Reno, Attorney General of the United States et al. v. American Civil Liberties Union et al.* June 26, 1997, 117 S.Ct.2329, 138. Online version available at <http://supct.law.cornell.edu/supct/html/96-511.ZS.html> (4/15/2002).

57 For an overview see ENGEL in Engel and Keller (2000); BERMAN *Internet and Nation State* (2002) .

58 Amtsgericht München 8340 Ds 465, Js 172158/95, 28.5.1998, *Multimedia und Recht* 1998, 429 = *Neue Juristische Wochenschrift Computer Report* 1998, 356; see also BENKLER in *Colorado Law Review* (1999),

from France to websites selling Nazi memorabilia. Actually, *Yahoo* preferred to ban access to these sites for all its customers.⁵⁹ Northrhine-Westphalian officials recently issued an administrative act against all Internet service providers present in the country, obliging them to ban access to two U.S. sites of Nazi groups.⁶⁰ The U.S. Children Online Protection Act would have also been applied extraterritorially, had it not been struck down by the courts.⁶¹

III. A Rational Choice Model of Content Regulation

Applying national laws extraterritorially is the opposite of organizing co-existence; it is open international conflict. Why did the nations not know better? The remainder of this article purports to explain the different outcomes in the areas of privacy and content regulation by way of a rational choice model. It should also allow policy-makers to assess the opportunities for improvement. Modelling pre-supposes a precise definition of the issue (part 1 below). Any model has limitations, which should be apparent at the outset (part 2). Finally, a model can do no more than generate hypotheses. Before taking action, they would have to be verified empirically (part 3).

1. The Issue

Nazi speech and pornography epitomize international conflict about Internet content. But they are not the only contentious issues. Other examples include tobacco advertising, gun sales, gambling and the sale of prescription drugs.⁶² All of them are covered by the following model. They center around a national intention to protect a defined group from being exposed to harmful content. One typical goal is to protect adolescents from content that is potentially unhealthy for their development. In such cases, the disputed content can remain on the Net. But effectively prevent-

electronically available at http://www.digital-law.net/IJCLP/1_1998/ijclp_webdoc_14_1_1998.html (4/16/2002); MAYER in *European Journal of International Law* (2000) 151-153.

- 59 Tribunal de Grande Instance de Paris, ordonnance de référé, 11/20/2000, <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm> (4/16/2002) ; id. Document de travail sur le rapport d'expertise, 11/6/2000, <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001106-rp.htm> (4/16/2002) ; id. Ordonnance de référé, 8/11/2000, http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord_tgi-paris_110800.htm (4/16/2002) ; Ordonnance de référé, 5/22/2000, <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm#texte> (4/16/2002). See also United States District Court for the Northern District of California San Jose Division, 11/7/2001, *Yahoo! Inc. v. La Ligue contre le racisme et l'antisémitisme*, <http://www.juriscom.net/en/txt/jurisus/ic/dccalifornia20011107.htm> (4/16/2002) ; FOWLER, FRANKLIN and HYDE in *Duke Law and Technology Review* (2001); GEIST in *Berkeley Technology Law Journal* (2001) at note 16 ss; GEIST in *Juriscom* (2001); BERMAN *Internet and Nation State* (2002) 24 s., 27 s., 64-66; REIDENBERG in *Jurimetrics* (2002).
- 60 Bezirksregierung Düsseldorf, 2/6/2002, Az.21.50.30, Sperrungsverfügung gegen *Oberon.net GmbH*, electronically available at <http://www.odem.org/material/verfuegung/> (4/16/2002). Australian and Italian cases are reported by GEIST in *Juriscom* (2001); BERMAN *Internet and Nation State* (2002) 25 s. A further German case is reported by FOWLER, FRANKLIN and HYDE in *Duke Law and Technology Review* (2001) 5.
- 61 GEIST in *Juriscom* (2001); see also DERTOUZOS *What Will Be* (1997) 289 on extraterritorial effects among states of the United States of America.
- 62 U.S. Congress bills on all these issues are reported by BENKLER in *Colorado Law Review* (1999) 12 and 18.

ing minors from gaining access to it essentially requires organizing co-existence among governments.

Not so rarely, the protectee is neither government nor society at large, but a precisely defined small number of individuals. This is typical in libel and slander cases, or in cases of copyright infringement. The ensuing conflicts are basically the same as in privacy. Not surprisingly, these issues have been much easier to resolve internationally.⁶³

International conflict over Internet content can also be framed as a clash of national values. In that perspective, it becomes apparent that values do not stand in isolation, neither analytically nor normatively. Rather each culture is characterized by a specific mix of conflicting, often even incompatible values. National differences are much more pronounced with respect to the composition of the specific basket of values than with respect to single values contained in it.⁶⁴ Yet, analytically, the metaphor of a basket of values, being a highly aggregate concept, is hard to handle. For simplicity, the model therefore narrows the issue down to single values.

2. Limitations of the Model

The model takes the advent of the Internet to be exogenous. In other words, it does not reflect the impact of national values on the design and evolution of the Internet. Obviously, in reality this impact has been profound.⁶⁵

The second qualification is shared by all rational choice models. Preferences are assumed to be exogenous and stable. This assumption is necessary, since rational choice models rest on the distinction between stable preferences and variable restrictions.⁶⁶ In the long run, this is certainly not a realistic assumption. In the area of privacy regulation, there is even empirical evidence that the Internet has already changed the perception of which activities and environments are considered private.⁶⁷ More generally speaking, psychologists point to the fact that it is not so rare for individuals to adapt their attitudes to newly introduced restrictions in the environment. In psychological terminology, the basic mechanism is called the reduction of cognitive dissonance.⁶⁸ It is therefore more than likely that the more the Internet penetrates the world, the more individuals and society will change. But in all likelihood, these changes will not occur ad hoc. Normally, the model will therefore properly capture the attitude of an individual nation, reflecting upon its present attitude vis-à-vis the impact of the Internet on the values it cherishes.

63 For a comprehensive treatment of copyright NATIONAL RESEARCH COUNCIL Digital Dilemma (2000) .

64 More from NATIONAL RESEARCH COUNCIL Global Networks and Local Values (2002) 46-73.

65 On the evolution of the Internet see Ibid.Global Networks and Local Values 23-45; on the interrelationship between the Internet and culture see NATIONAL RESEARCH COUNCIL Global Networks and Local Values (2002) 205-223; that Internet technology might ossify national (in particular American) values is the basic tenet of LESSIG Code (1999) .

66 For a succinct (formal) introduction to rational choice modelling see FELDMAN Welfare Economics (1980) chapter 1.

67 BELLMAN, JOHNSON, KOBRIN and LOHSE Privacy Preferences (2002) 6 with references.

68 Basic FESTINGER Cognitive Dissonance (1957) ; for a more recent survey see FREY and GASKA in Frey und Irle (1993) .

Ordinary rational choice models, like the one employed here, are static. The inherent limitation should, however, not be overstated. The model can handle any new step of Internet evolution. Within the model, this is just an alteration of the restrictions. Likewise, the model can be applied to any new set of state preferences. It is also open to the national preference to keep evolutionary paths open. What the model does not do is two things: It does not itself explain how changes in restrictions or preferences come about. It is thus not an evolutionary model, organized in terms of variation, selection and retention.⁶⁹ Moreover, this is not a model of negotiation dynamics. This is not a severe limitation, however, since the model explicitly captures strategic interaction. In game theoretic terms, the only limitation is therefore the restriction to one shot games.⁷⁰

Rational choice models imply a specific definition of the social problem. In short, they view it as a conflict of interests. Two or more actors autonomously strive to maximize their individual utility. This is not the only possible definition. Alternative views might stress the role of ideas⁷¹ or of shared mental models.⁷² They might point to the possibility that negotiators collectively construct a joint definition of the problem.⁷³ Negotiators might even generate a sense of joint responsibility.⁷⁴ While this may be quite realistic in other international negotiations, such a beneficial development is not very likely in the case of Internet content regulation; for nations want to combat Internet content precisely because the population finds it shocking, disgusting or frightening. If at all, deviations from rational choice predictions may therefore be expected in the opposite direction. Nation-states might be unwilling to compromise, even if that were the best way to serve their interest.⁷⁵

The last limitation is not inherent in any rational choice model. It hinges upon the definition of actors used here. The model exclusively looks at nation-states' actions. This makes the model state-centric. Of course, there are other important actors out there. Along the vertical axis, there are supranational entities like the European Union, international organisations, but also regional and local entities. Along the horizontal axis, government input is supplemented by pure private governance and by a rich variety of hybrid mixes of governmental and private input.⁷⁶ Moreover, only legally are nation-states truly units. In reality, legal entities are composed of many actors pursuing their individual aims. More importantly, the internal struggles translate themselves into changes in the international position of the nation-state. Realistically speaking, it is not so rare that states do not do the negotiating, but that governmental units from one state negotiate with

69 For rational evolutionary theorizing see NELSON in *Journal of Economic Literature* (1995); for evolutionary game theory as the most rigorous way of modelling evolution see BINMORE *Social Contract* (1994) .

70 On the distinction between one-shot and repeated or nested games see (in easily accessible language) BAIRD, GERTNER and PICKER *Game theory* (1994) 159-218.

71 The distinction of interests and ideas has been offered by YEE in *International Organization* (1996); see also VANBERG and BUCHANAN in *Journal of Theoretical Politics* (1989) and ENGEL in *Rechtstheorie* (2001).

72 More from MANTZAVINOS *Individuals, Institutions, and Markets* (2001) .

73 On the interface of individualistic and constructivist positions see BÖRZEL and RISSE *Internationale Institutionen* (2001) .

74 For a graphic illustration see VERWEIJ *Rhine and Great Lakes* (2000) .

75 More on irrational unwillingness to trade in negotiations from FARNSWORTH in Sunstein (2000) .

76 For an overview see NATIONAL RESEARCH COUNCIL *Global Networks and Local Values* (2002) 190-204.

their counterparts of other states.⁷⁷ Yet the state-centric model still captures the essence of the problem studied here. Put differently, the idea of organizing international co-existence is itself state-centric. It presupposes that governments keep at least the power to substantially slow down the emergence of forms of Internet governance that exclude state intervention. Realistically, bringing about proper co-existence on issues of Internet content regulation seems hard to do without active state involvement. And for the purposes of this problem, it does not matter whether the views of governmental agencies are properly coordinated inside of nation-states. It suffices that the negotiating agencies can credibly claim to engage the state for which they are speaking.

3. Empirical Validation

Models put a general epistemic problem into relief: perceiving reality presupposes narrowing down one's view. He who tries to see everything at once will see nothing at all.⁷⁸ But reality remains as complex as it is. Since all models have to exclude many elements of the events they observe, they necessarily can do no more than generate hypotheses. Before policy-makers base action on the predictions of a model, they are therefore well-advised to test the hypotheses empirically.⁷⁹ This paper fully accepts this view, but it does not do the empirical testing itself.

Put differently, despite the apparatus of rational choice theory used here, the paper in essence is inductive, not deductive. It does not start from a hypothesis, derived from a rational choice model, and uses the two cases of content regulation versus data protection to test them empirically. The underlying conviction is the following: it is hardly disputed that states are (also) driven by interest in their interaction. If interests matter, the character of the game must play itself out. What may be interesting, to a degree even surprising, is that and how the inability to organise co-existence in the area of content regulation, as opposed to data protection, can be traced back to such a parsimonious rational choice explanation. Despite methodology borrowed from the rational choice theory, the paper thus remains a lawyer's contribution. It does not want to add a piece of evidence to a discourse in the social sciences. It instead wants to teach policy makers what are the foreseeable obstacles in an attempt to organise co-existence in the area of content regulation. Or more modestly: it wants to tell them that they will have to look out attentively for the alternative causal factors stressed in Henry Farrell's comment.

77 Lucid SLAUGHTER in *Foreign Affairs* (1997) 184: states are gradually desegregating into separate, functionally distinct parts.

78 Basic ALBERT *Kritische Praxis* (1978) .

79 In order not to be misunderstood: the fundamental epistemic problem does not disappear in empirical testing, see KING, KEOHANE and VERBA *Designing Social Inquiry* (1994) . But the empirical methods are different from the theoretical tools. This explains why empirical tests can generate surprises, i.e. findings that question the tested theoretical hypotheses.

4. The Core Argument

Even if this paper is not written in the tradition of testing a theory guided hypothesis empirically, it may help the reader to know the core argument at the outset. The ability of states to organise co-existence in the area of data protection, and their inability to do so in the area of content-regulation, is traced back to strategic interaction. National preferences also differ significantly, but to all likelihood not to a degree that would exclude agreement altogether. The crucial difference seems to be the character of the conflict. Data protection typically is a one-to-one conflict. One nation wants to protect its nationals against intrusion by actors under the control of another nation into privacy. Content regulation, however, typically is a one-to-many conflict. One nation wants to protect its nationals, or its value system at large, against intrusion from anywhere in the world. Provided nation states have any hold on the issue at all, the willingness of all, or at least of very many, nation states to contribute is necessary in order for protection to be effective.

IV. National Preferences Before the Advent of the Internet

1. Introduction

This paper wants to explain why organizing co-existence has proved possible in the area of privacy regulation, but impossible in the area of content regulation. The explanation comes in three steps. Step 1 looks back into a past without Internet. A more rigorous, but less evocative way of making the same point is that step 1 is a thought experiment. It models the preferences nation-states would have today if there were no Internet. Step 2 adds the Internet to the picture. More rigorously: it models how states' preferences change as the Internet alters the opportunities for realizing their attitudes. Step 2 assumes that nation-states do not coordinate. Step 3 drops this assumption.

Formal modelling is not popular in either of the two fields that are relied upon for this paper. It nonetheless uses the following, primitive equation

$$U = \alpha(v) - \beta(c) \tag{1}$$

All of the elements of this formula will be explored in detail. Suffice it at this point to explain the notation; U stands for utility; v for the degree of protection of a specific national value; α for the evaluation of this protection by the nation-state; c stands for the opportunity cost involved in reaching a certain degree of protection; β stands for the evaluation of this cost.

This section is also organized in accord with the structures of this formula. It starts by explaining the concept of degree of protection (part 2 below) and of its evaluation by nation states (part 3). It goes on, explaining the concept of opportunity cost (part 4) and its evaluation (part 5). From this, a taxonomy of values can be derived (part 6). The section concludes, pointing to a number of complications (part 7).

2. Degree of Protection

The first element of the equation is straightforward: v is the good nation-states are seeking. This may be whatever value the state embraces. But v does not measure how strongly the state feels about that value. It measures how well the value is protected within the state's area of influence. If v is 0, a value has disappeared from a population. For instance, in Western countries, nowadays nobody would find it offensive for a man and a woman to kiss in public, whereas quite a number of Japanese seem to feel differently. If v is 1, in this population the value is safe. In reality, v will normally lie somewhere in between. If, for instance, occasional violations occur, but almost everybody considers the value to be legitimate, this might correspond to $v = 0.9$.

V looks at the outcome, not at what one might call the protection technology. Put differently, v measures the efficacy of the specific mix of protection technologies. A characteristic mix is composed of enculturation,⁸⁰ social norms and formal legal institutions, e.g. penal law.⁸¹

Values are not ironclad. They change over time. Since this model exclusively looks at single values, this observation translates itself into uncertainty about the degree of protection. Moreover, the model is meant to help states in deciding whether they want to engage in extra protection efforts. That is a forward-looking decision. What they need is an assessment of the degree of protection in the future. The character of the decision therefore increases the degree of uncertainty. When they take that decision, states do not know the degree of protection for sure. They must base their decisions on their subjective beliefs about the increase in protection originating from employing a certain, additional protection technology.⁸²

At closer sight, v turns out not to be an undisputed assessment, but the subjective valuation of each country. The privacy example from the introduction illustrates the point. As mentioned, Europeans and Americans are divided over their willingness to rely on industry self-regulation. One interpretation of this fact is that Americans expect this protection technology to be significantly more powerful than Europeans do and, hence, expect self-regulation to generate a significantly higher degree of protection for the value of privacy.

3. Evaluation

Not everybody likes everything. This is also true for values. Some Arabic countries consider it good for women to hide themselves under a burqu^c in public. Western countries consider the wearing of a burqu^c to be an outrageous offence to the dignity of women. The protection of one and the same value can therefore be a good for one country and a bad for another. This is due to the fundamental relativity of normative judgement. There is no last, undisputed norm from which

80 More from DONALD in Renfrew und Scarre (1999).

81 On the interaction of formal and informal institutions see EISENBERG *Informelle Institutionen* (2001).

82 More on rational choice models of expected outcomes from BAIRD, GERTNER and PICKER *Game theory* (1994) 79-89.

any more specific normative judgement could be logically derived.⁸³ α in equation 1 can thus be negative.

Even if two countries agree on whether they adhere to a given value, they may not deem it equally important for their national basket of values. To take the example from the introduction: The majority of Germans would not positively want easy access to pornography. But in comparison with the majority of Americans, they do not seem to think such access to be a very serious problem. This difference translates itself into the model in the following way: pornography has never been extinguished. At most, a country might enforce $v = 0.9$. With less effort, something like $v = 0.6$ is still feasible. Access to pornography is possible, but one does not come across it inadvertently, and one has to overcome natural or artificial access barriers. This was basically the state of affairs before the advent of the Internet. Pornography was only sold in sex shops. Not everybody wanted to be seen there. The shop personnel did not allow the access of minors. If a country feels strongly about pornography, it will value $v = 0.9$ highly. Within the formal language of the model, α is high, say 0.9. The lower level of protection characteristic for liberal countries before the advent of the Internet might appear very unattractive for such a strong-minded country. Therefore, for them α (0.6) would be much lower than 0.6, say 0.2. This would mean: the strong-minded country still considers some protection better than none. But the evaluation quickly drops once v falls below the practical maximum. The example demonstrates why the model writes $\alpha(v)$ and not simply αv . For the relationship between a certain degree of protection and its evaluation is not necessarily linear. The example points to the possibility of an exponential relationship. Another way of interpreting the example might be to introduce a threshold degree of protection. In that case, a country would accept a protection technology only if it offers a minimum degree of protection.

Obviously, the model can also capture how much a country dislikes the protection of a certain value. Again the burqu^c might serve as an illustration. Some Western countries, out of their belief in religious tolerance, would not oppose the wearing of a burqu^c. Some Muslim women would do so, since formal and informal religious institutions are imposed on them. But as long as the religion is not aggressive in its guest country, the government would not try to impose its will on women with such religious beliefs. The model could, admittedly somehow artificially, capture the case by setting $v = 0.1$ and $\alpha = -0.2$. This would read: the guest country weakly dislikes that Muslim women have to wear a burqu^c when on their streets. But it will not do a lot to prevent this from happening. If religious tolerance is stronger, α might even be 0. That would mean: the country would not itself want Muslim women to wear a burqu^c. But neither would it be opposed. It would be indifferent.

Thus far it has been assumed that the protection effort is real. Applying a certain protection technology does indeed make the value safer. Given uncertainty, the model admits that v usually denotes national beliefs. They may or may not turn out to be true after the fact. But when engag-

83 Out of the rich literature see only THOMPSON, ELLIS and WILDAVSKY Cultural Theory (1990); KERSTING in Kersting (1997); ENGEL in Rechtstheorie (2001).

ing in protection efforts, the state sincerely believes the effort to be useful. This assumption is not always realistic. States may deliberately engage in symbolic action.⁸⁴ They employ a protection technology, although the additional protective effect is minimal. Despite state activity, the value is still not effectively protected. Or the institution creates what one might call symbolic overkill, in that the value had already been protected effectively anyhow. Such symbolic action can make sense. A government may want to send a signal that it still stands behind a value, although it currently is not able to enforce it. The government may hope that addressees keep an earlier attitude. Symbolic action may be interpreted as the promise to take effective action once the opportunity structure changes, or technical and institutional creativity find more powerful protection techniques. Moreover, social actors might interpret symbolic governmental action as an invitation to step in with informal protective institutions. Within the model, symbolic action means $\alpha(v) > v$. The borderline case is pure symbolic action, with $v = 0$, but $\alpha(v) > 0$. But the model also captures cases where government values the symbolic effect of a protection technology separately. Formally then $\alpha(v) > v$.

4. Opportunity Cost

The model interprets values as goods. This interpretation engenders a follow up question: Is the good a free one? Economists consider a good to be free if demand is smaller than natural supply. An example is sunlight. If one narrows the assessment down to government itself, the protection of quite a number of values actually is a free good. Culture, religion or social groups do the job. But government might care about the effort of social actors involved. And frequently, a sufficient degree of protection implies some governmental activity too. The core of penal law is a case in point. People do not respect others' property solely because infractions are penalized. But occasional penal sanctions help uphold the cultural commitment to the protection of property. This is all the more true, if one goes back to the actor modelled here, the state. For as a collectivity, the state should care for efforts in society as well.

The protection of values thus normally entails an opportunity cost. It can be borne by government, by the addressees of an institution or by outsiders. It can be pecuniary, but it also can consist of the total or partial sacrifice of a competing regulatory goal. Two classically conflicting goals are the rule of law and democracy. Traditional command and control regulation is a fine-tuned compromise between effective governance and the demands of the rule of law and democracy.⁸⁵ But many think that command and control regulation is particularly inappropriate for Internet governance.⁸⁶ If that were true, governments would have to trade more effective governance against inroads into the rule of law and democracy.

84 REIDENBERG in *Jurimetrics* (2002) at note 72 alludes to the possibility: "Instead, democratic states frequently rely on law to shape social expectations and behavior rather than implement police state enforcement mechanisms"; a classic on symbolic politics is EDELMAN *Symbolic Politics* (1964) ; see also HANSJÜRGENS and LÜBBE-WOLFF *Symbolische Umweltpolitik* (2000) .

85 More from ENGEL in *Rengeling* (2001) .

86 For a critical view see ENGEL *The Role of Law in the Governance of the Internet* (2002) .

5. Evaluation

The model does not write c , but $\beta(c)$. This has a number of implications. First of all, nations do not necessarily evaluate the opportunity cost of a certain protection technology in the same way. To take up the example again: in the light of its Roman law and French administrative law origins, German law might evaluate rule of law higher than, say, the English law does; for their administrative culture does not rest on formal, litigable acts, but on the informal cooperation between individual administrators and a set of firms.⁸⁷ If one wishes, one may call this national preferences for institutions.⁸⁸

A second implication runs parallel to the distinction between v and $\alpha(v)$. There is no common normative currency for evaluating the opportunity cost involved in a certain protection technology. Fundamental normative relativity thus carries over to the assessment of the cost of protection. Likewise, the problem of uncertainty is present. Assessing the cost of a protection technology is no less a prognostic endeavour than assessing its governance effects. Therefore governments can have different beliefs about this cost.

Thirdly the model deliberately writes

$$U = \alpha(v) - \beta(c) \quad (1)$$

and not

$$U = \alpha(v - c) \quad (2)$$

For the latter would only be sufficient if governments had just one normative currency for measuring protection effects and protection costs. Sometimes the institutional framework forces actors to express their preferences in such a single currency. The most important institution having that effect is the market, at least if barter trade is excluded. Traders then must translate their desires and their dislikes into a sum of money. Votes in elections or in Parliament have the same effect. But neither public international law nor the mores of international comity impose similar currencies on states when negotiating Internet contents. It is therefore fully conceivable that a state likes a protection technology for one reason, but dislikes it for another reason fully inconsistent with the first.

It is only a logical step from this insight to the next. States can have several reasons for disliking a certain protection technology. They may think it uses up too much of the state's budget, and it weakens democratic control. In that case, the original equation must be written

$$U = \alpha(v) - \beta_1(c_1) - \beta_2(c_2) \quad (3),$$

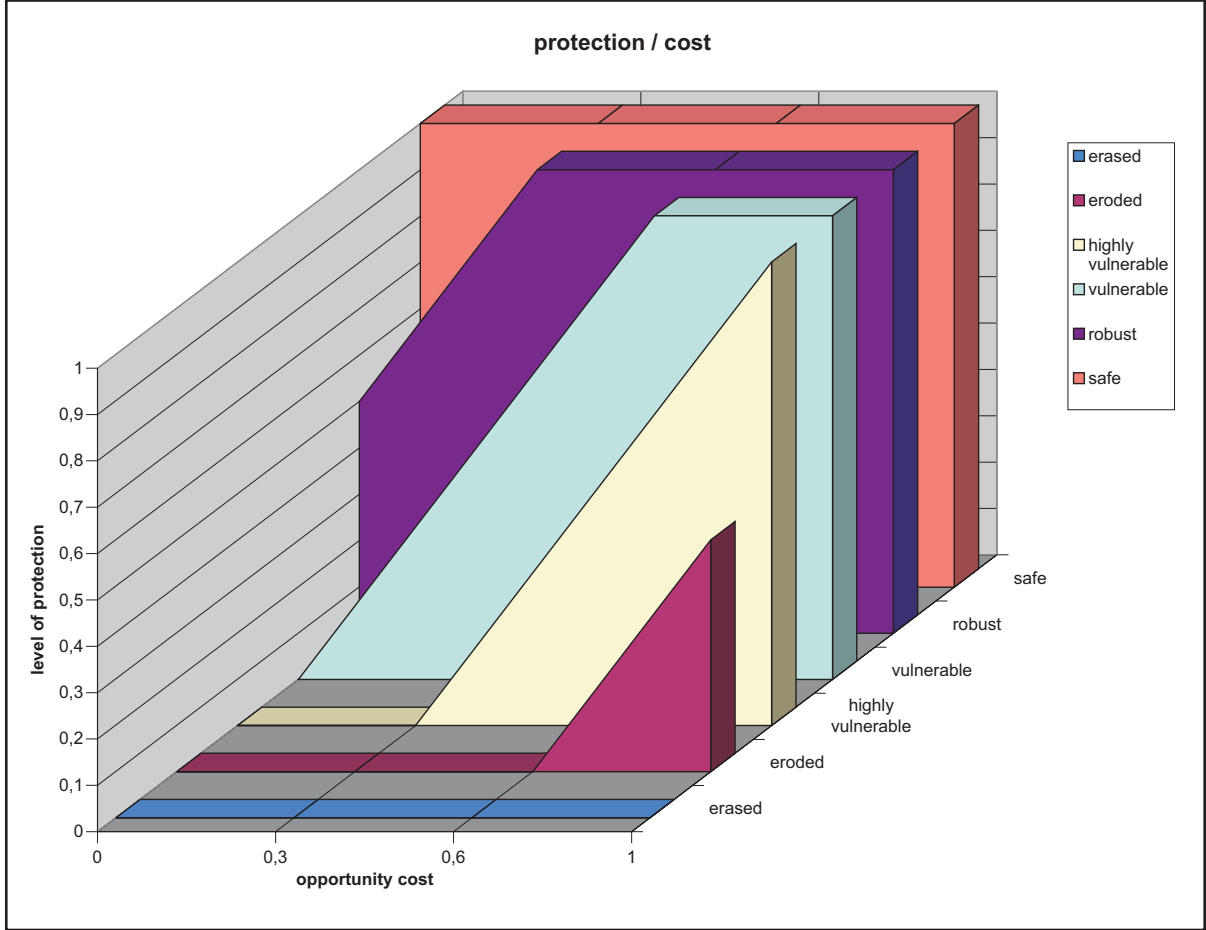
87 A comparison of the two administrative cultures is to be found at HÉRITIER, KNILL and MINGERS Ringing the Changes (1996) .

88 These preferences can be strong, graphic FREY and OBERHOLZER-GEE in Frey (1999) .

where c_1 and c_2 respectively are the two costs, each of them evaluated individually. Logically, the difference between β_1 and β_2 can also mean that government has different beliefs about the likelihood of the unwanted side effect of a protection technology.

6. Taxonomy of Values

Although the formula is primitive, it captures what tends to be overlooked in political discourse. It is not enough to find out how strongly a nation feels about a certain value. The nation must also determine its willingness to accept the opportunity costs involved in improving protection. There are thus three factors to be taken into account: the desirable level of protection, the opportunity costs involved in improving it and the ex-ante level of protection without state intervention. These three parameters yield the following graph:



In ideal types, six classes of values can be distinguished. A value is safe if additional intervention is not able to increase the level of protection; the value has the fullest protection anyhow. A value is robust if even with no additional intervention it will be protected to a certain degree. At a small opportunity cost, full protection can be restored. A value is vulnerable, if no additional action means that the value is no longer protected. But a small effort is enough to generate some protection. Considerable effort will yield full protection. In principle, the same holds for highly

vulnerable values. With no action they are not protected. It is possible to generate full protection. The difference lies in the opportunity cost involved. Small efforts are useless. Considerable efforts do only yield partial protection. Full protection is only possible with maximum effort. If a value is already eroded, the latter is no longer possible. Even if a country is willing to do all it can, it can at best generate partial protection. Anything short of maximum effort is useless. Things are even worse, once a value is eradicated. By definition, nothing is to be done about it. Even full effort would be useless.

These ideal types help understand borderline cases. If a country has made the violation of a value a taboo, it has set the level of protection to the maximum.⁸⁹ The same can be the case if exposure to a type of content is able to generate a trauma in spectators.⁹⁰ Although the result is often the same for fundamentalist countries, the analytical background differs. Characteristic for fundamentalism is not the high valuation of a value, but the almost entire disregard of the opportunity costs. Fundamentalists literally act at whatever cost.⁹¹

7. Complications

Equation 3 has already introduced the possibility of more than one kind of opportunity cost, evaluated separately. The same complication is also conceivable on the value side. The formula then reads:

$$U = \alpha_1(v_1) + \alpha_2(v_2) - \beta(c) \quad (4)$$

However, adding v_2 to the model is only necessary if governments evaluate two values jointly. Say they care for the side effects on freedom of information should they give privacy better protection.⁹² If governments evaluate two values separately, the basic formula suffices for both of them.

Governments do not only provide for the protection of values; they provide for many other goods too. If they evaluate one of these goods in relation to the protection of a certain value, the model captures this by

$$U = \alpha_1(v_1) + \alpha_2(g_2) - \beta(c) \quad (5)$$

This extension of the model will play a large role in explaining governments' attitude towards the effect of the Internet on the protection of values. At this point, one illustration suffices. When they visibly increase the protection of an endangered value, governments also demonstrate their problem-solving capacity.

89 More on taboos from JONES Taboo (1999) ; see also the classic WEBSTER Taboo (1942) .

90 More from BREMNER and MARMAR Trauma, memory, and dissociation (1998) .

91 For a rational choice analysis of fundamentalism see ARCE and SANDLER in Journal of Institutional and Theoretical Economics (2003).

92 More on the (partial) conflict between these two values from NATIONAL RESEARCH COUNCIL Global Networks and Local Values (2002) 133-135.

The first series of complications integrated issue linkages into the model. Another type of linkage is temporal. The protection of a value is normally not an exercise developed from scratch. A rational government should therefore assess the protection across a larger span of time. This can be integrated into the model in the following way:

$$U = \sum [\alpha_{t_0}(v_{t_0}) - \beta_{t_0}(c_{t_0})] \dots [\alpha_{t_n}(v_{t_n}) - \beta_{t_n}(c_{t_n})] \quad (6)$$

The equation looks complicated at first glance, but actually it is very simple. The only thing it adds are several points in time, written as $t_0 \dots t_n$. Moreover, the model assumes that governments do not lump all protection efforts and all the opportunity costs together, but that they assess the cost and benefit for each point in time separately. This seems plausible. States are not likely to be content with average protection in the long run if this means strong protection at one point in history, and neglect at other periods. Likewise they are likely to care about the degree of variation in opportunity costs. The model also captures differently long time horizons, and how political institutions cater for them. One constitution might government allow to be a strict vote maximizer.⁹³ Such a government would predict how far the majority of voters look into the future, and it would customize their protection efforts to that time span. Formally, such a government might only consider $t_0 \dots t_4$. Another government might be basically driven by ideology and plan for a much larger time span.

Finally, rational actors on markets prefer money today to money tomorrow. This is so, since they could re-invest the money once they receive it. In other words, on markets, rational actors discount future benefits.⁹⁴ For sure, this is not a model about markets. There is no such thing as a capital market, giving rational actors a benchmark for discounting. But democratic constitutions do not allow governments to stay in office for a lifetime. Since the constitution wants the government's position to be precarious, it must face that they consequently will have a tendency to discount the future.

Psychological research points to the fact that, in many circumstances, individuals discount the future even beyond what would be rational.⁹⁵ The effect seems, however to hinge upon perception. Discounting results when individuals frame the choice as one between near and remote benefits. The effect reverses if they instead frame it as a choice between different sequences of outcomes. In that scenario, they tend to prefer the best at the end.⁹⁶ It is not likely that these effects directly carry over to governmental choice. For governments are corporate actors, and they choose in a highly institutionalized environment. There is much less psychological evidence on behavioural anomalies in such circumstances. But the psychological observations should serve as a warning. Constitutions, and hence our model, should be open for differences in the evaluation of several points on a time sequence. This is precisely what the present model does in that it al-

93 This is the standard assumption of public choice theory, see e.g. BUCHANAN and TULLOCK *Calculus* (1962) .

94 This is the starting point of intertemporal economic modelling, see e.g. STRÖBELE in Beckenbach (1991) .

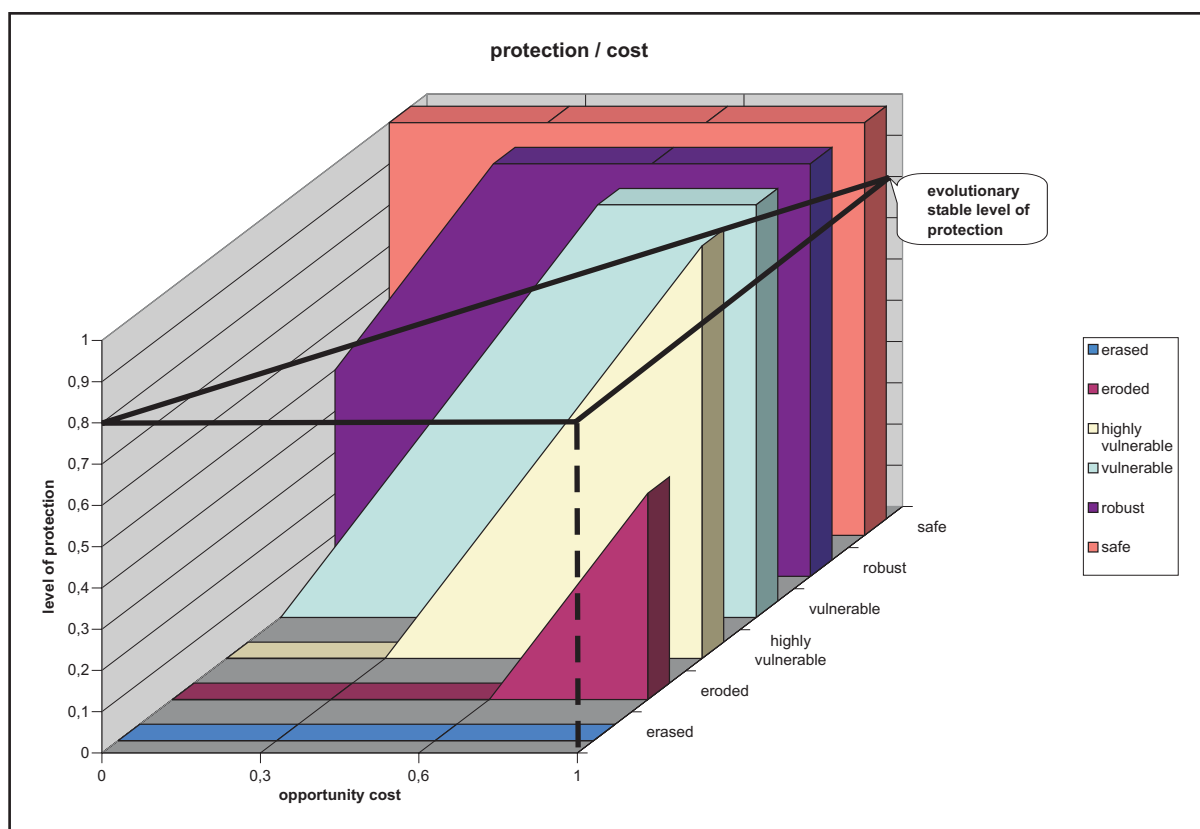
95 AINSLIE *Picoeconomics* (1992); LOEWENSTEIN and PRELEC in *Quarterly Journal of Economics* (1992); LAIBSON in *Quarterly Journal of Economics* (1997).

96 LOEWENSTEIN and PRELEC in Kahneman und Tversky (2000) .

lows for a separate α and β for each point in time. Formally, α_{in} would be considerably smaller than α_{t0} .

One of the most important practical areas of application of intertemporal economics is resource economics. The parallel generates a further insight. One of the problems resource economics has to struggle with is regenerative resources, like crops, cattle or fish. Nature regularly yields a certain outcome. Sometimes it is possible to increase the outcome, say by adding fertilizers. Sometimes other human activities, like air pollution, can diminish the outcome. But typically, the impact of such human input is not linear. Many natural resources tolerate a certain amount of damaging action without any effect. Once the damage goes beyond a certain threshold, however, the regenerative capacity is affected.⁹⁷

All this carries over to values, at least if they are considered from the perspective of governments. As mentioned earlier, values are typically not generated by government from scratch. The basic inputs come from enculturation, and from informal social norms. These inputs are continuous anyhow. Each new individual has to be enculturated anew. Social norms are permanently actualized.⁹⁸ Moreover, values are much easier to destroy than to generate anew. There is thus a considerable threshold involved. Figure 3 illustrates this phenomenon:



97 For an overview see STRÖBELE Rohstoffökonomik (1987); HECHT Stoffpolitik (1999) .

98 More from BOHNET Kooperation (1997) 29-44.

V. The Impact of the Internet on National Preferences

The purpose of the model is to clarify national reactions to the advent of the Internet. The next section will explore opportunities for coordinating the behaviour of several or even all nation-states. Whether individual nations are likely to engage in such coordination depends on what they have to win and lose in the exercise. Breakdown values determine negotiation outcomes.⁹⁹ This section is about breakdown values. It uses the model to determine national preferences after the advent of the Internet. The section is organized to fit to the elements of the model. It looks at the degree of protection (part 1 below), the evaluation of protection (part 2), the opportunity cost (part 3) and the concomitant goods (part 4).

1. Degree of Protection

a) *Introduction*

The model looks at individual values. Of course, the Internet is not only able to affect the degree of protection accorded to values that a country adhered to before there was the Internet. The Internet also brings up new issues, like the electronic manipulation of pictures. It highlights earlier problems and induces countries to take sides. In many countries spamming is a case in point, i.e. unsolicited commercial electronic mail. Finally, the Internet can contribute to policy diffusion. The fairly strong egalitarian culture of those who built the Internet is a case in point. It might change attitudes in countries like Germany, which were traditionally almost untouched by egalitarian thought. If a country does indeed adopt a new value, another issue surges, which can be treated separately by the model.

The following subsection focuses on the case that is more important in practice, i.e. on how the Internet affects the problem pressure to uphold values which a country had already adhered to before the Internet was introduced. The model demonstrates that the advent of the Internet can have two separate effects. It can either affect the degree of protection or the opportunity cost involved in maintaining the earlier degree of protection. This subsection looks at the first possibility. The Internet can affect old governmental protection technologies (part b below). It can have a more general impact on the problem solving capacity of nation-states (part c). Finally, the Internet can alter the contribution of other foreign or non-state actors to the protection of a given value (part d).

b) *Impact on Old Governmental Protection Technology*

In the first scenario, before the advent of the Internet, a value was already protected by governmental action. Given the opportunity cost of this protection technology, the country considers the degree of protection to be adequate. The Internet takes some of the protection power away from the old protection technology. Ultimately this need not lower the degree of protection. External

99 OSBORNE and RUBINSTEIN *Bargaining and Markets* (1990) 70 s.

efforts to protect this value might come into play. The government might be willing and able to bear the opportunity costs of additional protection technologies. But all things being equal, the Internet would then decrease the degree of protection. Figure 1 illustrates this scenario. The value would drop into a less protected class.¹⁰⁰ A highly vulnerable value might be eroded. A vulnerable value might become highly vulnerable. Depending on the weakening effect of the Internet, values could even switch from being highly protected to being protected very little. For instance, a robust value might become highly vulnerable. Should the value have properties of a renewable resource, its regenerative capacity might be damaged. The old value might eventually even be replaced by an entirely different one. Since this is a model about quantitative, not qualitative change, within the model this would mean that the earlier value would be eradicated.

There are several ways of explaining why the Internet could weaken earlier protection technologies. Many have observed the globalizing effect of the Internet.¹⁰¹ This may result from what economists call systems competition.¹⁰² Economically speaking, governments switch from a situation in which there is a monopoly to one in which there is monopolistic competition. That is, the substitution gaps between the bundles of public goods offered by governments remain large. But those addressed by regulation are no longer captive customers. If they are willing to bear the switching cost, they can exchange one provider for another.¹⁰³

Another conceptual language for making the point is taken from Albert O. Hirschman's work. He distinguishes exit and voice as two techniques with which members can control the management of an organization.¹⁰⁴ In accord with that perspective, the Internet gives those who dislike the earlier protection efforts of government new exit options. In other words, they can engage in regulatory arbitrage.¹⁰⁵ There are many ways to do so. The effect is obvious for situations in which earlier barriers to accessing unwanted content were media specific. This is true for many mechanisms that impeded access to pornography. It could only be broadcast late at night. Printed material was sold only in sex shops. Now though, via the Internet, pornographic material can be accessed from any computer at any time. If users fear governmental intervention, they can even access pornographic sites anonymously. If the content provider cooperates, traffic can be encrypted.¹⁰⁶

100 Another way of putting the effect is: the Internet results in a mismatch between law and reality, DELLAPENNA *Law in a Shrinking World. The Interaction of Science and Technology with International Law* (2000) 7-11, with a graphic example from admiralty law.

101 See only the following two quotes: "In Cyberspace, the First Amendment is a local ordinance", BARLOW *Leaving the Physical World* (1997) electronically available at http://www.eff.org/Publications/John_Perry_Barlow/HTML/leaving_the_physical_world.html (4/18/2002); the US Constitution is just "a speed bump on the Information Superhighway", REIDENBERG in *Texas Law Review* (1998) 586.

102 Again, a small choice of voices must suffice: GERKEN *Competition Among Institutions* (1995); MONOPOLKOMMISSION *Systemwettbewerb* (1998); MÜLLER *Systemwettbewerb* (2000) .

103 More from KERBER in *Ordo* (1998) 254-257; SCHÄFER in *Berg* (1999) .

104 HIRSCHMAN *Exit voice* (1970) .

105 FROMKIN in *Kahin und Nesson* (1997) .

106 More from HETCHER in *Vanderbilt Law Review* (2000).

A credible threat of exit gives an actor more voice internally. Internal actors can also forge coalitions with foreign governments. U.S. privacy regulation illustrates the point. Traditionally, U.S. privacy advocates had a hard time, given the characteristic reluctance of the U.S. public to elicit state regulation. But these privacy advocates forged an advocacy coalition with the European Union. The U.S. Federal Trade Commission also joined in and thereby enlarged its own domain of influence.¹⁰⁷

Why does the Internet put old governmental protection technologies under pressure? Why do political actors gain extra leverage? The basic point is: communications technology in general, and the Internet in particular, dramatically decrease transaction costs. Distance costs drops to nearly zero.¹⁰⁸ Moreover, the Internet weakens traditional regulatory targets.¹⁰⁹ There are many reasons for this effect: the decentralized architecture of the network,¹¹⁰ packet switching,¹¹¹ anonymity,¹¹² encryption,¹¹³ and disintermediation are among the most important.¹¹⁴

All these have been rational choice arguments. They are supplemented by effects that can better be understood with other conceptual tools. Rational choice theory assumes actors to be optimizers. Whenever restrictions change, they recalculate their best response. Actually, reactions tend to be much slower, since actors organize their behaviour by routines.¹¹⁵ Given that, behaviour only changes if actors are faced with a surprise. For those interested in locally unwanted content, however, the Internet is likely to be perceived as such a surprise. There are two ways of explaining why. The Internet is qualitatively new and thereby allows many to get access to content that would have been entirely inaccessible to them earlier. Moreover, quantitatively speaking, the opportunity costs dramatically drop, since earlier barriers fall.

Finally, old barriers to accessing pornographic material are weakened, since they are adapted to a commercial supply. On the Internet, posting pornographic material is so cheap and easy that many do it with no commercial interest. Since they do not want to make money, governance technologies that rely on reducing profit fail. In order to be effective, they would have to address what is most difficult to do: the isolated individual and his pastime.

107 More from Ibid.in .

108 Of the many voices see only PERRITT in *Villanova Law Review* (1996) 1: “lack of localisation”; TRACHTMAN in *Indiana Journal of Global Legal Studies* (1998) at note 12 and passim: for these actors, the Internet shifts the “technical production frontier”.

109 PRICE and VERHULST In *Search of the Self. Charting the Course of Self-Regulation on the Internet in a Global Environment* (2000) 16.

110 BOYLE in *University of Cincinnati Law Review* (1997) 179: a censor therefore has no central exchange to access.

111 This makes it almost impossible to interrupt traffic; government can at best observe it.

112 On techniques for safeguarding anonymity of electronic traffic see FROMKIN in *University of Pittsburgh Journal of Law and Commerce* (1996) at note 72 ss.

113 For a basic treatment see NATIONAL RESEARCH COUNCIL *Cryptography* (1996) .

114 BENKLER in *Colorado Law Review* (1999) 32, for other effects of the Internet on governance see ENGEL in Engel und Keller (2000) 220-232.

115 Basic GIGERENZER, TODD and ABC RESEARCH GROUP *Simple Heuristics* (1999) .

c) *Impact on Problem Solving Capacity of Nation-States*

If the Internet weakens an old governmental protection technology, governments could still switch to new technologies. If they do, the impact of the Internet can simply amount to an additional switching cost. The Internet can even provide government with new, more powerful or less costly governance tools.¹¹⁶ For instance, packet switching presupposes that the sender and receiver are clearly identified. This is done by what are known as IP addresses. Log files document to which IP address the computer has been linked. This makes it much easier for the government to track access to unwanted content.¹¹⁷ Government can even use its influence on standardizing bodies in the interest of making the Internet more regulable.¹¹⁸ It can switch to other regulatory targets. Governments seem particularly attracted by the idea of imposing content regulation on hosts and Internet service providers.¹¹⁹

All this notwithstanding, it still does not seem exaggerated to maintain that the problem-solving capacity of the national governments has decreased in the area of content regulation. National borders have become highly permeable.¹²⁰ Potentially, any other country becomes a neighbour. These and many other effects of the Internet make sovereignty a much weaker concept for content regulation.¹²¹

d) *Impact on Governance Externalities*

Protecting national values is not only the government's concern. Rather, governmental input supports and supplements the input from other domestic or foreign, formal or informal actors. Economically speaking, government thus profits from considerable positive regulatory externalities.¹²² The Internet changes this regulatory environment fundamentally. Before the Internet, the strongest positive input came from natural and artificial borders. Going abroad or trading with foreign suppliers was not impossible, but it was costly and often not very practical. As mentioned, due to the Internet, the physical border of territorial distance almost fades away. And artificial borderlines among states are easy to surmount electronically.

116 The point has often been made, see e.g. TRACHTMAN in *Indiana Journal of Global Legal Studies* (1998) at note 12 and passim: the Internet extends governments' structural production frontier; GOLDSMITH in *University of Chicago Law Review* (1998); PERRITT in *Indiana Journal of Global Legal Studies* (1998); KAHLER in Engel und Keller (2000) .

117 Admittedly, this is not a watertight technology. For instance, individual users can hide behind a firewall.

118 This point has been stressed by LESSIG *Code* (1999) 43 and passim; LESSIG and RESNICK in *Michigan Law Review* (1999) 404-411.

119 This is what the cases reported in the introduction are about, see notes 58, 59, 60.

120 REIDENBERG in *Emory Law Journal* (1996) at note 5; see also POST in *Wayne Law Review* (1997) at note 15: "Cyberspace [...] does not merely weaken the significance of physical location, it destroys it".

121 The impact of the Internet on sovereignty is the object of a rich literature, see only SASSEN *Losing Control? Sovereignty in an Age of Globalization* (1996); SASSEN in *Indiana Journal of Global Legal Studies* (1998); TRACHTMAN in *Indiana Journal of Global Legal Studies* (1998); ENGEL in Engel und Keller (2000) 233-240.

122 More on the concept of regulatory externalities from ENGEL *Abfallrecht* (2002) 307-313.

Within the international environment created by the Internet, new regulators surge, and they muster considerable power.¹²³ From the traditional egalitarian culture of the Internet, forces like the CyberAngels originate. Like a private police, they look for gross moral offences, and sanction electronically those who they consider to be intruders.¹²⁴ Supported by computer technology, users can engage in self-help,¹²⁵ e.g. by using filters.¹²⁶

2. Evaluation

The advent of the Internet may not only affect the degree of protection, it may also alter how it is evaluated. Within the formal language of the model, the impact is potentially not restricted to v ; it can also affect α . The most likely practical effect is cognitive. As mentioned, governments act under considerable uncertainty when they decide upon protection activities. In other words, they have to rely on their beliefs. The stronger a country feels about a value, the more likely it is that the Internet will be socially perceived as an unwelcome surprise. This may induce governments to overemphasise the risk involved. Within the language of the model, they would evaluate the marginal increase in risk more than linearly. Such a reaction would at least be consistent with research on social risk perception. As a rule, the general public's perception of risks differs significantly from the experts' perception.¹²⁷ Since politicians are re-elected by the general public, they are likely to orient themselves towards public risk perception, much rather than expert judgement.

3. Opportunity Cost

The Internet does not only affect the degree of protection, it also alters the opportunity costs involved in applying the old governmental protection technology (part a below). If government gains new regulatory options, they are not free of charge either (part b).

a) *Higher Opportunity Cost of Old Protection Technology*

If the Internet destroys old governmental protection technologies altogether, there is no need for government to assess the opportunity cost of this tool under changed circumstances. Normally, however, the effect of the Internet is smaller. It only weakens the old tools, or it doesn't affect their power at all. But the opportunity costs change. There are several reasons for this.

123 For an overview see ENGEL in Engel und Keller (2000) 245-258; NATIONAL RESEARCH COUNCIL Global Networks and Local Values (2002) 123-132 and 190-204.

124 See <http://www.wiredpatrol.org/>.

125 Programmatic DAM in Journal of Legal Studies (1999), more critical RADIN and WAGNER in Chicago Kent Law Review (1998) at note 60, but see at note 41.

126 An excellent, albeit dated, overview of available filter technology is provided by WEINBERG in Hastings Communications and Entertainment Law Journal (1997) see also NATIONAL RESEARCH COUNCIL Pornography (2002).

127 Graphic PILDES and SUNSTEIN in University of Chicago Law Review (1995); see also SUNSTEIN in Stanford Law Review (1996) 264, 267, 293 and critical VISCUSI Risk Equity (2000) 32.

The first effect can best be illustrated with command and control regulation – say the prohibition to sell child pornography. Since the advent of the Internet, suppliers have been able to move abroad and serve their customers electronically. Even if the Attorney General successfully traces the foreign server, it is difficult for one country to enforce its rules on child pornography abroad. The country may feel obliged to switch to more costly enforcement options, and prosecute users instead of suppliers.¹²⁸

Regulatory addressees are not the *homines oeconomici* of the economic model. Their reactions to regulatory intervention are not confined to optimization. They can react creatively instead, and find ways to mute regulatory action altogether.¹²⁹ Since governmental intervention clashes with the egalitarian Internet culture, such reactions are particularly likely. The now classic statement reads: “The Net interpretes censorship as damage at roots around it.”¹³⁰ The decentral architecture of the Internet provides regulatory addressees with many opportunities for creative reactions. It is particularly likely that they will dislodge activities to parts of the Internet that are strongly protected from central intervention.¹³¹ It is next to impossible to control the material exchanged via e-mail, in news groups or chatrooms.¹³² If senders cooperate, both parties can even use strong encryption, or they can wrap the provocative content into forms that look entirely innocent to control officials.¹³³

A second additional opportunity cost is neither technical nor monetary, but legal. As mentioned, content control the Internet makes every nation a neighbour. Put differently, if one nation-state tries to impose its own content standards on the Internet, it almost inevitably impinges upon other nation-states' freedom to decide upon which expressions they prefer to tolerate. Regulating Internet content is what public international law calls the extraterritorial application of laws. This is an old issue of international economic law. Some 20 years ago, transatlantic conflict originated from different attitudes towards antitrust and tax. Protracted legal discourse resulted in a set of rules that limited nation-states' abilities to impose their will on other nations. The basic rule is that, for applying its own rules extraterritorially, the case must have a genuine link to the regulating country.¹³⁴ Adapting these rules to Internet cases is a hot issue among public international lawyers.¹³⁵

128 This is what German law has done, see sec. 184 (3) Nr. 3 penal code.

129 Basic WEGNER Wirtschaftspolitik (1996) ; see also WEGNER in Journal of Institutional and Theoretical Economics (1997).

130 JOHN GILMORE, cited to BOYLE in University of Cincinnati Law Review (1997) 178.

131 PRICE and VERHULST In Search of the Self. Charting the Course of Self-Regulation on the Internet in a Global Environment (2000) 13.

132 NACHBAR in Minnesota Law Review (2000) 256.

133 This technique is called tunnelling; more from LESSIG and RESNICK in Michigan Law Review (1999) 414.

134 Basic MENG Extraterritoriale Jurisdiktion (1994) ; see also ENGEL in RabelsZ (1988).

135 Out of the rich literature see PERRITT in Villanova Law Review (1996); GOLDSMITH in University of Chicago Law Review (1998); NACHBAR in Minnesota Law Review (2000) 312-316; GEIST in Berkeley Technology Law Journal (2001); BERMAN Internet and Nation State (2002) 17-20.

b) *Opportunity Cost of New Protection Technologies*

Typically, the Internet does not disempower governments altogether. Governments retain the ability to impose values on their constituency. But they may not be willing to do so, given the opportunity costs of the available protection technologies. There are many reasons for such hesitance.

Some 45 countries restrict Internet access altogether. Most of them also employ some mechanism of censorship.¹³⁶ China has created a national sub-network to monitor international Internet traffic. It has also imposed a licensing regime on Internet service providers. That provides government with direct control over domestic Internet use.¹³⁷ Governments could even resort to electronic aggression against countries that tolerate unwanted Internet content. Aggression could come as a virus or as a denial of service attack.¹³⁸ But Western democracies are unlikely to use any of these tools. They are obviously at variance with other constitutional values to which they adhere.

Other mechanisms may not appear outrageous, but may still be too costly. This is basically what the struggle over imposing content control on technical intermediaries is about. As the *Yahoo*, *CompuServe* and *North Rhine Westphalia* cases demonstrate, this is a practical option. It does not yield absolute protection.¹³⁹ But it makes exposure of the population to the unwanted content considerably less likely. The strongest drawback of such action is, however, its indivisibility. More precisely, the cost of customizing the intervention is considerable. Customizing can fail in two ways. If governments do not succeed in confining the effect of their intervention to their territory, they are likely to run into international conflict. And if they are unable to confine the intervention to narrowly defined types of content, they are likely to violate their own commitment to free speech. Both failures are practical. In the *Yahoo* case, the French Court purposely did not order a ban on the sale of Nazi memorabilia altogether. All it asked was that reasonable technical steps be taken to make access to the websites difficult for French users. Apparently, however, shielding one country from access to defined websites in this manner entailed considerable costs for *Yahoo*. At any rate, the firm preferred to ban these sites for all its customers.¹⁴⁰ Likewise, imposing technical safeguards on Internet service providers may well help a government ban access to some particularly off-setting websites. But once these technologies are in place, any other or later government can easily abuse them to turn the Internet into a tightly controlled forum.¹⁴¹

136 MAYER in *European Journal of International Law* (2000) 161.

137 REIDENBERG in *Jurimetrics* (2002) at note 73.

138 *Ibid.* in note 70.

139 The realistically feasible degree of protection played a major role in the *Yahoo* case, see the references above note 59 and the statement of JEAN-RAYMOND LEMAIRE to the Paris Court, unpublished document.

140 See refs. above note 59.

141 This is the basic tenet of LESSIG and RESNICK in *Michigan Law Review* (1999).

4. Concomitant Goods

Governments do not decide on the protection of endangered values in isolation. This issue is embedded in a much larger Internet policy. Before deciding to take action, governments consider what that means for related political goals. In the formal language of the model: $\alpha_1(v_1)$ is considered along with $\alpha_2(g_2)$.

A country does not lose its identity if a single value is eroded or replaced by a new one. It is a long way from Victorian attitudes to women's lib. But nobody would pretend that England is no longer England because of the changes in attitudes. But cultural identities can get lost. Nation-building has been precisely such an exercise in relegating regional cultures to reservates, and replacing them with a joint national culture. The Internet could contribute to a similar phenomenon on a larger scale. It might also contribute to gradually replacing territorial ties and making personal ties the basis of culture. Even now, the technical elites might already be culturally remote from many of those surrounding them physically.¹⁴² Not all governments will dislike such developments. But some might. If they do, preserving cultural identity is an additional good that is being sought.

Cultural diversity presupposes the cultural identity of a considerable number of individual cultures. But the normative perspective differs. Cultural identity looks at individual cultures. Cultural diversity looks at the benefit that all arguably have from the co-existence of a multitude of cultures. The parallel to bio-diversity is telling. It is protected by international treaties, since the nations are convinced that a large genetic pool makes nature more robust to change and accident. The idea can be transposed to culture, calling for the maintenance of social variety.¹⁴³

While the former two policy goals might corroborate a national wish to regulate Internet content, the next policy goal largely points in the opposite direction. Governments rightly care about the benefits their country can gain from the Internet. They are economic, political and cultural.¹⁴⁴ Many unilateral protection technologies make it more difficult for the population to exploit this potential. This is obvious if a country cuts its population off from parts of the Internet.¹⁴⁵ Even if, at closer sight, the restrictions imposed on Internet use are small, the public may still perceive them as much graver.¹⁴⁶ Or regulatees may be uncertain about what intervention actually means. This is what the U.S. courts have in mind when they try to prevent a chilling effect.¹⁴⁷

142 More on the impact of the Internet on culture from NATIONAL RESEARCH COUNCIL Global Networks and Local Values (2002) 205-223.

143 The parallel is drawn by DAVID in Engel und Keller (2000) 69 s.; see also the parallel DAWKINS The Blind Watchmaker (1986) draws between genes and "memes"; critical DONALD in Renfrew und Scarre (1999) 186 s.

144 For an overview see LITAN in Duke Law Journal (2001) 1047-1055.

145 Graphic REIDENBERG in Jurimetrics (2002) at note 68: "To the extent that societies are censor-happy, they will be marginalized on the Internet. The potential risk to doing business in oppressive societies will serve to discourage companies from supporting those repressive regimes through commercial activities".

146 In greater detail NACHBAR in Minnesota Law Review (2000) 247-259.

147 More from LESSIG and RESNICK in Michigan Law Review (1999) 402, 416, 423 and passim. RIBSTEIN and KOBAYASHI State Regulation of Electronic Commerce (2001) 72 argue that divergent national (U.S. state) regulation might be a valuable regulatory laboratory. While it is a pertinent evolutionary argument in general,

As demonstrated earlier, values can be modelled as goods. But they are goods of a very special kind. If a society adheres to a certain value, it might not be very willing to trade the diminished protection of the value for some other commodity. In other words, struggling over values generates a particularly severe type of conflict. It engenders conflicts of identity, not conflicts of distribution.¹⁴⁸ Countries might want to tame the ensuing potential for violence, or at least for a disruption of good international relations.

Self-esteem is a powerful motivator, not only for individuals, but also for corporate actors.¹⁴⁹ If a government is perceived as a loser internationally, this may put it at risk in the next election. Both elements explain why governments tend to care about saving face.¹⁵⁰ They often therefore try to avoid the impression that they are plainly and simply unable to protect local values.

The medal has the reverse side. Governments are concerned about demonstrating their problem-solving capacity.¹⁵¹ In the area of Internet content regulation, this is particularly attractive; for in the public perception, the Internet is easily equated with anarchy. Even if the additional protection resulting from governmental action is small, governments might still opt for it. Singling out the demonstration of problem-solving capacity as a separate good is another way of modelling the symbolic value of governmental action.¹⁵²

Individuals do not only care about their own utility, they also care about the utility of others. In reality, preferences are thus inter-related.¹⁵³ States, as corporate actors, are no exception. Democratic countries tend to be missionary with respect to freedom of expression and human rights more generally. As such, they dislike protection technologies that make authoritarian rule more powerful elsewhere in the world.¹⁵⁴ Conversely, belligerent regimes might have an additional interest in impeding Internet access if this also makes it more difficult for the population of their adversaries to profit from the Internet. They will dislike it even more if the open character of the Internet makes it easier for their adversaries to predict their future action.¹⁵⁵

If governments prove unable to protect local values, other regulators are likely to step in. These actors may not define the regulatory goal precisely as government would. They may pick other values, or they may opt for a different level of protection. They may also employ protection technologies with opportunity costs that the government considers prohibitive. In any of these

it does not seem to fit well to Internet content regulation, at least as long as the co-existence of different national Internet content policies is not effectively organised.

148 HUNTINGTON *Clash of Civilizations* (1996) .

149 TESSER, STAPEL and WOOD *Self* (2002) .

150 MUELLER in *info* (1999) 504 s. und passim offers this as an explanation for the design of ICANN.

151 On that category see MITROFF and KILMANN in *Research in Sociology of Knowledge, Sciences & Art* (1978); SCHARPF in *Journal of European Public Policy* (1997).

152 On modelling the symbolic value as a factor increasing α see above note 84 and accompanying text.

153 Of the rich literature on modelling interrelated preferences see only STARK *Altruism* (1995); BOSI in *Rivista Internazionale di Scienze Sociali* (1998); LEVINE in *Review of Economic Dynamics* (1998).

154 Illustrative on this KALATHIL and BOAS *Internet and Authoritarian Regimes* (2001) .

155 Cf. the following speculation of LESSIG and RESNICK in *Michigan Law Review* (1999) 424: "For example, some Serbs and Croats might refuse to allow each other access to their web pages".

scenarios, the outside protection efforts do not (only) entail positive regulatory externalities, but also negative ones.¹⁵⁶ In public awareness, two types of opportunity costs stand out.

Many are concerned with the anarchic element of foreign, private or hybrid regulatory activities.¹⁵⁷ Such regulators are likely to use excessive sanctions, particularly the banishment of some users.¹⁵⁸ They may go far beyond what is necessary to reach the regulatory goal, since they do not care about the opportunity costs. This is a typical effect of filtering technology.¹⁵⁹ Such regulators tend to define the regulatory goal in very broad terms, giving short shrift to competing values like free speech or tolerance.¹⁶⁰ The mere risk that a website will "hassle" customers suffices to ban access to it.¹⁶¹

Private regulatory activity is not controlled by democratic forces. But often it also escapes effective control by competition.¹⁶² Some private regulators even guard their selection policy as a trade secret.¹⁶³ When deciding about the design of a control mechanism, private regulators are driven by commercial or ideological intentions, not by a balanced view of social betterment. It is not so rare that part of the hidden agenda is to further empower business interests¹⁶⁴ or ideological minorities.¹⁶⁵

The second concern with negative regulatory externalities is evolutionary. In evolutionary theory it usually is called over-fitting.¹⁶⁶ Behaviour, or an institution, is fine-tuned to a narrowly specified, historically contingent problem definition. Once the environment or the way it is perceived changes, the institution is no longer adaptive. Things are even worse if the old institution generates path dependence.¹⁶⁷ For Internet content regulation, the danger looms large, since regulation

156 On the concept of regulatory externalities see above at note 122 and accompanying text.

157 Out of the many voices see only RADIN and WAGNER in *Chicago Kent Law Review* (1998) at notes 4, 63 and passim.

158 REIDENBERG in *Emory Law Journal* (1996) at note 34; RADIN and WAGNER in *Chicago Kent Law Review* (1998) at note 46; NACHBAR in *Minnesota Law Review* (2000) 265.

159 Details from WEINBERG in *Hastings Communications and Entertainment Law Journal* (1997); see also LESSIG and RESNICK in *Michigan Law Review* (1999) 425.

160 NACHBAR in *Minnesota Law Review* (2000) 266 s. reports RSACi using a taxonomy of hate speech much stricter than US constitutional jurisprudence.

161 RADIN and WAGNER in *Chicago Kent Law Review* (1998) at note 58.

162 More from NACHBAR in *Minnesota Law Review* (2000) 270-280.

163 This is, e.g., the policy of CYBERSitter, *Ibid.* in 268.

164 REIDENBERG in *Jurimetrics* (2002) at note 78: "Geographic determinacy would enable US intellectual property rights holders to distribute their content on the Internet and engage in self-help by blocking access to those rogue countries that do not adequately protect American rights"; BENKLER in *European Journal of International Law* (2000) 182.

165 This is how BENKLER in *European Journal of International Law* (2000) 176 interprets the story of the US Communications Decency and the Children Online Protection Acts: a Senator representing a radical minority forced Congress to adopt a statute that predictably was unconstitutional. As expected the courts struck it down. But engineers were effectively triggered to develop powerful filtering technologies.

166 WEIGEND in *Mozer* (1994) .

167 More from WITT in *Dopfer* (1996) .

can literally be hard-wired.¹⁶⁸ As one observer puts it: "We might make the net safe for kids, but in consequence make it a fundamentally regulable space."¹⁶⁹

VI. Coordination of National Behaviour in General

A rational actor is not likely to coordinate his behaviour with others if he has nothing to gain from cooperation. Such a win-win situation is not easy to bring about in Internet content regulation (part 1 below). But even if it were, this would not guarantee effective coordination; for Internet regulation requires that a relatively small number of actors agree to solutions. Even if the solution serves their interest, they still might not rationally agree to it; for this is a situation of strategic interaction (part 2). Finally, even if they do agree, it is not self-evident that they will implement the compromise. For at the stage of implementation, the problem of strategic interaction repeats itself (part 3).

1. Win-Win Situations

A catchy phrase, which has even made it into practical politics, is the "search for win-win solutions."¹⁷⁰ An equivalent phrase is the "no regret space," which negotiators often use.¹⁷¹ Game theorists call it the core. They stress that it can be empty.¹⁷² It is the breakdown values that decide whether negotiators stand to gain from cooperation.¹⁷³ This section analyses why the breakdown values of negotiating states could be larger or at least equal to the utility they expect from cooperation.

Normally, negotiation is about gains from exchange. This situation is different. Individual countries are not reciprocally selling some protection of the other's local values; neither are they buying a protection service and paying for the service with some other good. In economic terms, agreeing on Internet content regulation amounts to jointly producing a good.¹⁷⁴ When they agree on protective efforts, nation-states get access to an additional protection technology. They may add it to earlier unilateral efforts or supplement those earlier efforts with the new technology. If they intend to add it to earlier unilateral efforts, their interest must derive from the possibility of increasing the degree of protection. They may have the same reason for replacing national by international efforts. They might also be motivated by the expected savings in opportunity costs.

168 This is the basic tenet of LESSIG Code (1999) 15-17 and passim; see also REIDENBERG in *Emory Law Journal* (1996) at note 61; REIDENBERG in *Texas Law Review* (1998) 587.

169 LESSIG and RESNICK in *Michigan Law Review* (1999) 423; see also LESSIG and RESNICK in *Michigan Law Review* (1999) 398: "Long after the "problem" of "indecent speech" is solved, the consequences of our choices to deal with indecent speech — these secondary effects — will continue to influence the culture of the Net".

170 Programmatic BRAMS and TAYLOR *Win-Win* (1999) .

171 The term was popular during the – failed – negotiations over climate protection.

172 More from FELDMAN *Welfare Economics* (1980) 23-38.

173 See already above at note 99 and accompanying text.

174 Cf. the metaphor of technical vs. structural production frontier used by TRACHTMAN in *Indiana Journal of Global Legal Studies* (1998) at note 31 and passim.

National interests can differ on any of the four elements of the model. Differences over v mean that one and the same protection technology does not generate the same marginal increase in utility in all countries. There may be two reasons for this. On the one hand, one and the same value may be less at risk in one country, and more in another one. The Internet exposure may be larger in one country and smaller in another. Positive regulatory externalities may be stronger in one country than in another. On the other hand, one country may have more effective unilateral protection technologies at its disposal than another country.

A difference in α means that countries evaluate the increase in protection brought about by the joint protection technology differently. This is obvious if one country considers something to be a bad that another considers to be a good. There are many such cases. "What constitutes 'political speech' in the United States (Nazi speech) is banned in Germany; what constitutes 'obscene' speech in Tennessee is permitted in Holland; what constitutes porn in Japan is child porn in the United States; what is 'harmful to minors' in Bavaria is Disney in New York."¹⁷⁵ Even if countries agree in principle, they may not feel equally strongly about a value. For instance, the American public seems to be much more concerned about nudity, whereas the German public seems to be much more concerned about hate speech.¹⁷⁶ Negotiations become particularly thorny in borderline cases. If countries start negotiating on a taboo, they have already given it up. The very fact that negotiations are taking place means that it has been degraded to an ordinary local value. Likewise, fundamentalist countries are already partially tamed if they are willing to negotiate over levels of protection. If they fear the traumatic experiences of users, countries might also find it hard to compromise.

One and the same international protection technology may hit one country much harder than another. Some types of opportunity costs may not even exist in some countries. This is obvious for authoritarian governments. They do not care about free speech, rule of law or democracy anyhow. And even if the types of opportunity costs coincide, they may not have the same dimensions. To use the same example evoked above, in a newly constitutionalized country, the advent of the Internet may put free speech, rule of law and democracy at a much larger risk than in old democratic countries.

If a country does not believe in democracy, the model could also judge β to be 0 or even a negative value. But countries can also differ over the evaluation of opportunity costs that are felt in all participating countries. A case in point is the strong U.S. commitment to free speech. Countries like Germany or France also have protected free speech constitutionally. But they do not grant free speech absolute protection. The government may interfere with this constitutional right if this is justified by a sufficiently important competing policy goal.¹⁷⁷

175 LESSIG and RESNICK in Michigan Law Review (1999) 395, see also LESSIG and RESNICK in Michigan Law Review (1999) 396.

176 See again note 53.

177 More from NATIONAL RESEARCH COUNCIL Global Networks and Local Values (2002) 106-132.

Cooperative efforts are not the only technology available for protecting local values. Whether a country is going to benefit from cooperation thus depends on how powerful unilateral protection technologies might be. In other words, the more asymmetric the gains from trade are, the less likely agreement is. In the area of Internet content regulation, this asymmetry is pronounced. There are many reasons why the U.S. has more powerful unilateral protection technologies at its disposal than many other nations. Unilateralism is thus a very powerful option for the U.S. The Internet not only originated in the U.S., its technical backbone is basically U.S. based. The U.S. has a dominant influence on Internet standardization bodies, including the domain name system. The *lingua franca* of the Internet is English. The net mores are deeply rooted in the egalitarian culture of U.S. technicians.

The complications of the model presented above can all contribute to compounding the problem. Even if two states evaluate a certain degree of protection of one value along the same lines, compromise can be impossible, since one of them evaluates v_1 along with v_2 . In that case, coordination cannot be a win-win solution, for both countries disagree over $\alpha_2(v_2)$. Likewise, disagreement can be rooted in a mere difference of $\alpha_2(g_2)$; that is, both countries can agree on the value, but disagree in their evaluation of a concomitant good. Finally, agreement can be confined to single moments in time, be they today or in the somewhat more remote future. In other words, governments can disagree, since their time horizons are not the same, or since they evaluate future protection or future opportunity costs differently.

2. Strategic Interaction Over Agreement

The metaphor of the invisible hand made *Adam Smith* a world famous author. In the economy, it is not a mistake for buyers and sellers to pursue their respective interests. Precisely by doing so they contribute to the common cause as much as they can.¹⁷⁸ It took almost two centuries before economics started focussing on the limitations of the metaphor. It presupposes what is far from self-evident: workable competition.¹⁷⁹ It was game theory which taught economists that rational actors act strategically. When deciding on individual action, they anticipate the simultaneous or sequential action by their negotiating partners. If they can, they even damage their negotiation partners – if that helps them attain their own ends.¹⁸⁰ The effect is not able to be perceived under workable competition, since, in game theoretic terms, this environment forces actors to play a game against nature.¹⁸¹ But there is no such thing as competition when states negotiate over Internet content regulation. This is obvious, since joint protection efforts are, economically speaking, joint production, not exchange. Hence, negotiations over Internet content regulation can fail, even if cooperation is a win-win solution. There are three additional reasons for failure: Governments can try to impose their will on others by threatening them with additional damage

178 SMITH *Wealth of Nations* (1776) IV.ii.9.

179 Basic CLARK *Competition* (1961) .

180 Basic VON NEUMANN and MORGENSTERN *Games* (1944) ; for an overview of the impact of game theory on economic theory see MYERSON in *Journal of Economic Literature* (1999).

181 SCHARPF *Games* (1997) 5.

(part a below). Even if some nations are willing to agree on a common project, the endeavour can fail due to the role of outsiders (part b). Finally, in a dynamic perspective, there might be no policy entrepreneur who makes generating sufficient demand his cause (part c).

a) *Nuisance Value*

Workable competition pre-supposes that goods are definitely attributed to actors. Competition theory, in other words, assumes well-defined property rights.¹⁸² Another way of making the same point is: competition theory assumes there is no conflict.¹⁸³ International political reality is different. Even the most optimistic scholars do not pretend that public international law is a complete legal order.¹⁸⁴ Dispute prevention and settlement remain central tasks of public international law. At least practically, if not legally, nation-states have a rich array of means for damaging other states at their disposal. And it is hard to overlook that they are willing to play this card.

All this plays itself out when nations consider coordinating their Internet content policies. As demonstrated by the *CompuServe* and the *Yahoo* cases, other nations do have power to impose their will on individual U.S. Internet firms. The U.S. is vulnerable, precisely because industry is far ahead in running and exploiting the Internet. And the cases also demonstrate that other nations are not faced with an all or nothing choice. They can pick specific actors, without running a serious risk of being cut off from the Internet, as a nation.

Technically it might be feasible for the U.S. to cut off other nations from the Internet. But given its commercial interest, and to quite an extent its ideological interest, in Internet proliferation, the U.S. is not likely to take this option. To unilaterally change the structure of the Internet, it might, however, use its power as a threat in negotiations. Faced with a choice between pure American rule and some compromise, other nations might prefer the latter. This is how some observers interpret the worldwide acceptance of the U.S. dominated ICANN.¹⁸⁵

b) *Multilateral Protection*

When two businessmen set up a firm, this is joint venture. But the firm sells its products on a market. Consumption is thus individual. Protecting local values from erosion via the Internet is not a good for sale. At best, nations might jointly protect their own values. In that scenario, they would not only be their own consumers. All effort would serve all participating nations, irrespective of how much they contributed. Economists call such a good a club good. By this they mean that there is no rivalry of consumption. The good cannot be split into units that disappear once used.¹⁸⁶ The more nations participate, the more difficult it becomes to make sure that no one is

182 A classic of property rights theory is EGGERTSSON Institutions (1990) .

183 For a comprehensive account of the rational choice theory of conflict ARROW Conflict Resolution (1995) .

184 The optimistic line is the hallmark of the Heidelberg Max Planck Institute, see recently FROWEIN in *Berichte der Deutschen Gesellschaft für Völkerrecht* (2000).

185 MUELLER in *info* (1999) is outspoken on this.

186 For a classic treatment see BUCHANAN in *Economica* (1965) for a modern treatment see CORNES and SANDLER *Externalities* (1996) 347-482.

free riding on others' efforts. Rational nations will anticipate the opportunity for free riding and hesitate to participate.

Designing a protection technology that limits benefits to participating nations is not easy. If nations do not succeed, the character of the good switches to what economists call a public good. In this scenario, free riding becomes an even more serious problem. Not only might those who contribute consume more than their legitimate share, non-contributors are even more likely to consume. Again, rational actors perceive the problem in advance and do not contribute.¹⁸⁷

At closer sight, the problem with Internet content regulation is even more profound. Even if negotiating states design the protection technology cleverly enough to control consumption, the protection technology must match the risk to the value. As mentioned, individual Internet users have plenty of opportunities to circumvent content regulation. Full protection therefore presupposes the almost unanimous participation of nation-states. Public goods theory calls this a weakest link good. The graphic term means that the good is of no use for all contributors unless everybody participates.¹⁸⁸ Since the Internet also weakens national sovereignty, even the unanimous participation of nation-states might not be sufficient; for individuals and organized social actors might have power to circumvent even joint national action.

c) Dynamic Element

Club goods and public goods theory are static. They might not offer the best ways to model the multilateral element of Internet content regulation. A low initial degree of participation might be acceptable for the forerunners if they see a realistic chance of attracting the others soon enough. In this dynamic perspective, cooperative Internet regulation is interpreted as what economists call a network good. They use this term to characterize goods with economies of scale on the demand side. The good becomes more and more valuable for those already using it if new users join in.¹⁸⁹

Although the hope for future benefits somewhat eases the incentive problem, it does not make it disappear. As the network industries demonstrate, there are quite a few institutional solutions to network problems. But none of them easily carry over to Internet content regulation. There is no world government to step in. No nation other than the U.S. seems powerful enough to act as a

187 For a classic treatment see SAMUELSON in Review of Economics and Statistics (1954); SAMUELSON in Review of Economics and Statistics (1955) for a modern treatment see CORNES and SANDLER Externalities (1996) 143-346.

188 CORNES and SANDLER Externalities (1996) 184-190. A qualification is warranted, to which KATHARINA HOLZINGER has pointed me. In the logical extreme, a true weakest link good cannot be a public good. For if, for the good to be produced altogether, truly every individual must contribute, and must contribute a defined share, free riding is impossible. But apart from this extreme case, the deficiency problem persists.

189 From the rich literature see only KATZ and SHAPIRO in American Economic Review (1985); LIEBOWITZ and MARGOLIS in Research in Law and Economics (1995); SHAPIRO and VARIAN Information Rules. A Strategic Guide to the Network Economy (1998) ; NACHBAR in Minnesota Law Review (2000) 271-276 draws the parallel to Internet content regulation.

network entrepreneur. But given its constitution, the U.S. is the least likely to do so. And the cooperation of all interested nations is, as demonstrated, difficult to bring about.

3. Strategic Interaction over Implementation

Even if proactive states succeed in winning the consensus of their counterparts, this is not the end of the story. If states behave like rational utility maximizers, they also rationally calculate whether it is worthwhile to fulfil their contractual obligations. They keep their promises only if this is their best response, given that the environment is changed by the contractual obligations of the others.¹⁹⁰ Again, rational actors anticipate the post-contractual problem and do not agree to the contract if it is not self-enforcing.¹⁹¹ In game theoretic terms, abiding by the contractual obligations must be either a dominant strategy¹⁹² or a Nash equilibrium.¹⁹³ By this latter term, game theorists mean that no actor can do better, given the other players' action. Whether the post contractual cooperation is indeed rational depends on the protection technology. If governments mutually promised to sanction private actors who jeopardize the local values of other states, this would not be the case; for each country would do best if all others played by the rules while the mentioned country cheated. Happily enough, in reality states do not behave like pure rational actors. Not even powerful states are light about breaching their international obligations.¹⁹⁴ But there is ample evidence in international relations that countries do indeed breach their contractual obligations if this is in their interest. If the contract is not self-enforcing, implementation is therefore at least uncertain.

As always, however, good modelling should not divert attention away from problems that loom larger in practice. The instability of contractual arrangements among states should be a serious concern. But it is not the most serious problem; for states do not actively endanger the local values of their counterparts. It is private parties who do. And given the limitations of internal sovereignty brought about by the Internet, states cannot credibly promise each other that they will prevent private actors from doing so. The true problem is therefore not implementation among states, but implementation within states.

190 If the original situation is a prisoner's dilemma, political scientists speak of a second order prisoner's dilemma at the implementation stage, see OSTROM in *American Political Science Review* (1998).

191 More from RICHTER and FURUBOTN *Institutionenökonomik* (1999) 171-173.

192 On dominance as a solution concept see BAIRD, GERTNER and PICKER *Game theory* (1994) 11-18.

193 On Nash equilibriae *Ibid.* 19-23.

194 There are many ways to explain this observation, see OSTROM in *American Political Science Review* (1998); SCHLICHT *Custom* (1998); ENGEL *Vertrauen* (1999) .

VII. Organizing Co-Existence in Particular

What does all this mean for the topic of this paper, for the organization of co-existence among nations? An answer to this question requires that co-existence be defined (part 1 below). A number of protection technologies can be brought under this definition (part 2). But it is already difficult to make one of them a win-win situation (part 3). Moreover, negotiations (part 4) and implementation are plagued by the problem of strategic interaction (part 5).

1. Defining Co-Existence

At first glance, the concept of co-existence seems straightforward: All partners guarantee each other mutual regulatory autonomy. But logically, full autonomy is only conceivable if governments forgo any policy with a spill-over to other governments' domains. Since internationally governments represent their population, they will also have to guarantee that no national or national inhabitant engages in activities that prevent another nation from freely choosing a policy. The only conceivable technology for organizing co-existence would thus be universal autarky. Put differently, organizing co-existence would be an oxymoron; for autarkic nations have no interest in organizing co-existence. They want to exist on their own.

Public international law holds a different view. From the very beginning, organizing co-existence among states has been a prime task of this field of law. Although the very idea of public international law rests on the concept of sovereignty, it has never been understood as a synonym for autarky. Sovereignty has three elements: a territory, a people, and institutions.¹⁹⁵ Logically, public international law could therefore not presuppose contact zones among states driven down to zero. On the contrary, developing rules for situations where sovereign states come into contact with each other has always been one of the prime tasks of public international law. Neighbourhood law addresses territorial contact.¹⁹⁶ The law of diplomatic protection determines when nationality is more significant than territory.¹⁹⁷ The rules on diplomatic immunity organize contacts between territory and foreign institutional sovereignty.¹⁹⁸

This observation is generalizable. The very idea of organizing co-existence only makes sense if all those participating are willing to take on a certain risk. When co-existence is organized, conflict is not precluded, it is patterned.¹⁹⁹ Put differently, the idea of organizing co-existence only makes sense if and when political property rights are not fully determined among states.²⁰⁰ Co-existence and cooperation are therefore not opposites: they are elements along a continuum. When they organize co-existence, states also have a joint goal. It is only more limited. All states

195 The concept goes back to JELLINEK and JELLINEK *Allgemeine Staatslehre* (1914) 396 ss.

196 For an overview see KLEIN *Umweltschutz* (1976) .

197 For an overview see JOSEPH *Nationality* (1969) .

198 For an overview see PRZETACZNIK *Protection of Officials* (1983) .

199 EGEBERG *Organisational Approach* (2002) coined the term.

200 Cf. MAJONE in *Journal of Institutional and Theoretical Economics* (2001) for the concept of political property rights.

consider reciprocal contacts to be valuable. And they are willing to pay a price for them. They do not go so far as to harmonize their substantive policies, but they are willing to tolerate and even support foreign policies to the extent necessary to make a contact possible.

2. Protection Technologies

a) Introduction

In the area of Internet content regulation, organizing co-existence means that all participating countries consider the Internet to be valuable. More precisely, in the interest of exploiting the economic, political and cultural potential of the Internet, they are willing to pay some cost. This cost originates from the fact that different nations cherish different values and that all of them have policies to protect them. The cost thus consists of the repercussions of foreign protection technologies. Organizing co-existence means cooperatively diminishing this cost.

For two reasons, this is not an easy task: The first reason becomes apparent when comparing Internet law and traditional public international law. Public international law was able to organize co-existence, since natural barriers were rather high. Territory did only clash with territory close to the border. The worst problems were no graver than transborder oil fields. Territory clashed with nationality only if and when a country let foreigners in. And territory and institutional sovereignty only clashed for a few diplomats, or visiting heads of state. Thus contact was marginal. Since the dawn of the Internet, this is no longer true. Foreign websites are just a click away. Neither geography, technology nor budget any longer provide natural barriers. Language and culture remain. But the more difficult the internal access to some type of content is, the more attractive it becomes to surmount these barriers. Contact is therefore almost ubiquitous.

Moreover, governments have lost at least some of their power to control what happens in their territory, and what their nationals do. Even if governments agree to cooperate, foreign content policies do not therefore necessarily receive effective protection.

In light of these considerations, organizing co-existence in the area of Internet content regulation can mean one of three things, or it can consist of an appropriate combination of these elements. The first approach is structural. It tries to reintroduce nationality barriers (part b below). The second approach is behavioural. Countries promise to mutually enforce their autonomous Internet content regulations (part c). The third approach could emphatically be dubbed re-inventing the nation-state. It purports to strengthen the problem-solving capacity of nation-states with respect to Internet content (part d).

b) Re-Introducing Nationality Barriers

There are several ways of describing the first strategy: re-introducing political property rights, re-inventing the distinction between national and international cases, or re-introducing a substantial cost for exit from national content regulation. All these conceptualizations are gradual. Full

protection is not the issue. That would be tantamount to prohibiting contact altogether. States would have done the job if they had again marginalized transnational cases.

Technically and economically this might be feasible. The most severe intervention would be controlled gateways.²⁰¹ Currently the most popular idea is geographical filtering. To a degree it is already in place. Ironically, it has not been imposed on the Internet by governments. In the interest of better targeting banner advertizing, content providers have pushed the development of the necessary technology.²⁰² It can rely on three types of verification: by the IP address of the computer, by an online statement of the user or by an off-line verification mechanism, like credit cards.²⁰³ Any of these techniques leads to a world of online passports.²⁰⁴ The U.S. has already repeatedly tried to impose this solution on foreign countries. New York disliked online gambling from Antigua.²⁰⁵ U.S. copyright owners disliked the re-transmission of U.S. TV programmes on a Canadian website.²⁰⁶ And *Playboy Enterprises* disliked the violation of their trademark by Italian actors.²⁰⁷

Another option is re-intermediation. Ordinary Internet users would no longer have direct access to all websites posted, but would have to go through the portal of a host. Governments could rely on these hosts to impede access to unwanted content.²⁰⁸ *Yahoo* has demonstrated its ability to impose content restrictions. It has effectively banned the sale of pet hamsters and of used underwear and, under pressure from the U.S. National Football League, also of online gambling.²⁰⁹ There are also more indirect ways to impose re-intermediation. A case in point is the technology for giving users broadband access to the Internet. Telecommunications operators have a choice between a symmetric and an asymmetric solution. If they opt for the latter, the capacity for incoming traffic is much larger than for outgoing traffic. This is quite an effective way of preventing end users from turning their personal computers into web servers.²¹⁰

c) *Mutual Enforcement*

When foreigners travel, settle or trade, the host country could in principle impose any of its domestic rules on them. This would, however, be a heavy burden on transnational contacts. Foreigners might no longer be married, they might no longer be the owners of their goods, and they might no longer be in custody of their children. Ere long almost all states in the world do therefore have an autonomous private international law. These conflict rules call on their courts to

201 LESSIG and RESNICK in *Michigan Law Review* (1999) 415.

202 More from GEIST in *Berkeley Technology Law Journal* (2001) at notes 278 ss; BERMAN *Internet and Nation State* (2002) 66-69; REIDENBERG in *Jurimetrics* (2002) at notes 12 s.

203 More from GEIST in *Berkeley Technology Law Journal* (2001) at notes 278 ss.

204 More from BERMAN *Internet and Nation State* (2002) 64-70.

205 *People v. World Interactive Gaming Company*, 714 N.Y.S. 2d 844 (1999), cited in REIDENBERG in *Jurimetrics* (2002) at note 40.

206 *iCraveTV*, 2000 U.S. Dist. Lexis 11670 (W.D. Pa, 2000), cited to *Ibid.in* at note 41.

207 *Playboy Enterprises, Inc. v. Chuckleberry Pub. Inc.*, 993 F.Supp. 1032 (S.D.N.Y. 1996), cited to *Ibid.in* at note 43.

208 BENKLER in *Colorado Law Review* (1999) 42; LESSIG and RESNICK in *Michigan Law Review* (1999) 415.

209 REIDENBERG in *Jurimetrics* (2002) at note 22.

210 BENKLER in *Colorado Law Review* (1999) 26.

apply foreign instead of domestic private law rules in appropriate cases. States, in other words, mutually enforce their private law if they consider this to be the appropriate way to handle a transnational case. In principle, the idea could be transposed to Internet content regulation.²¹¹ This may well work for content issues like libel and slander. But it is not very likely that nations like the U.S. will willingly enforce strict German rules on Nazi speech, or that Germany will be willing to enforce rules of Arabian countries on the portrayal of women.²¹²

d) *Re-Inventing the Nation-State*

The third strategy strives to strengthen the nation-state. As demonstrated, the Internet reduces its problem-solving capacity in general, and in particular with respect to content issues. But there are also the mentioned offsetting factors. The more governments learn to exploit them, the more valuable they become as transaction partners. This is thus also a way of organizing co-existence.

One way of doing so is precisely by re-introducing nationality barriers. This has a double effect: it directly helps nation-states to protect their local values; and it returns some power back to them to make credible commitments vis-à-vis other nation-states. Apart from this, nation-states can commit themselves internationally to use the technical and economic options of empowerment vis-à-vis Internet users. They can, for instance, switch from governance by law to governance by technical code. Or they can switch from pure governmental governance to hybrid forms, and thus partly rely on private governance input.²¹³

3. Win-Win Solutions

Is organizing co-existence in one of the just mentioned ways a win-win solution? And if so, is it more attractive than the outright harmonization of content standards? The latter question is easier to answer. Organizing co-existence imposes much more moderate demands on participating states. They can continue to adhere to substantially different values. All they have to do is to respect that other countries do the same. Put differently, organizing co-existence is a highly un-specific technology for protecting values. It covers all types of content, the access to which a government might want to ban or impede. Organizing co-existence thus considerably enlarges the negotiation space. States no longer have to struggle over single values. Their general ability to impose national values is the issue. Yet another way of making the point is: organizing co-existence is a highly aggregate solution. It bundles all actual and potential content restrictions into one negotiation issue.

In the language of the model, organizing co-existence does not only increase v ; it can also have a positive effect on g_2 . States thus also stand to gain in the area of concomitant goods. Protecting

211 LESSIG Code (1999) 54-57; LESSIG and RESNICK in Michigan Law Review (1999) 423; SAMUELSON in Marsden (2000) at note 79 calls this “policy interoperability”.

212 BERMAN Internet and Nation State (2002) 72; for a critical account also see OSTHAUS in Engel und Keller (2000)

213 See above V 1 c and d.

cultural identity and diversity becomes easier. Once conflict is patterned, it is less likely to degenerate to the point that it seriously disrupts international relations. States save face and demonstrate their problem-solving capacity. States have less reason to engage in unilateral protection efforts. That makes it less likely that other nations will suffer the ensuing negative externalities.

Not all states will evaluate the increases in v and g_2 equally. Differences in α_1 and α_2 will thus play themselves out. For two classes of countries α might be such that organizing cooperation is not advantageous. The first class of countries is epitomized by the U.S. Their constitution prevents them from proactively protecting local values. It therefore is of little use for them that organized co-existence makes it easier for them to do so. For them, the deal is at best attractive if the increase in one of the concomitant goods is strong enough. Most of the just listed goods, however, are not attractive for the U.S. either. The nation's position is so exceptional that it can provide for these goods unilaterally. The basic exception are the negative externalities from foreign protection efforts. Perhaps it is more important that organized co-existence will probably make it easier for the far-advanced U.S. industry to exploit the full commercial potential of the Internet worldwide. To a lesser degree, U.S. government might also welcome the remaining political potential of the Internet.

The second problematic class of countries is fundamentalist, or it wants to protect a taboo. In both cases, a more-is-better approach might not be acceptable internally. The problem is particularly severe if the cooperative protection technology is by agreement limitational. Precisely because the U.S. has to accept this in order for it to work, this is a likely feature of the compromise. For then the U.S. could at least point to the fact that the agreement prevents other nations from what the U.S. considers to be excessive unilateral protection efforts.

When they decide to contribute to organizing co-existence, governments will not only look at the benefits, they will also look at the opportunity costs; for some nations, the greatest advantage of organizing co-existence will then turn into the greatest disadvantage. For the protection technology is not only unspecific, it is indivisible. The new opportunities for protecting substantial values are indiscriminate. Every nation-state can use them for whatever value it deems fit. The same two classes that already had problems with α might also dislike this. Formally, their β of this c might be high; for the U.S. is not only committed to free speech domestically, but worldwide. And fundamentalist values do not typically stand in isolation. They clash with substantial or formal values to which other countries adhere. Both classes of nations are therefore likely to have interrelated preferences. In the case of the U.S. and other liberal countries, an unspecific protection technology can have another drawback. It can make it easier for internal social and political actors to impose substantial values on a group, or even on society at large. This is at variance with the principle of a free marketplace of ideas. Technologies such as reintermediation or IP address tracing also involve considerable risks that there will be private invasions into privacy.²¹⁴

214 BERMAN Internet and Nation State (2002) 70.

There are other opportunity costs, too. Technologically and economically less advanced countries might consider the technical steps involved in re-nationalizing the Internet to be fairly high. All countries might also hesitate to impose this cost on Internet service or backbone providers.²¹⁵ Even more important than this out of pocket cost is the opportunity cost for the evolution of the Internet.²¹⁶ Any of the protection technologies considered would make the Internet "a fundamentally regulable space."²¹⁷ In the future, as the Internet evolves, the technology for organizing co-existence (and thereby restricting it) would have to be respected. Any of these technologies would make the Internet a much more centrally controlled phenomenon than it has been. It would become less likely for the Internet to generate more fundamentally new forms of communication, economic exchange, and social interaction.²¹⁸

4. Strategic Interaction over Agreement

Even if no strategic interaction occurred, it would thus not be easy to organize co-existence for content regulation. But, as demonstrated, negotiating an agreement on Internet content regulation is an instance of strategic interaction. None of the general problems of strategic interaction described earlier disappear when the negotiating states aim at organizing co-existence. On the contrary: given the fact that organizing co-existence is a highly unspecific protection technology, its public good character increases. Even those countries that are only interested in the protection of a small number of highly specific substantive values are now among those who benefit from the protection efforts of others.

5. Strategic Interaction over Implementation

As in the more general case, the stability of an agreement depends on the character of the protection technology. Some technologies are self-enforcing. This is, in particular, true once states agree to embed traces of the users' nationality into the technical standards underlying the Internet. When that happened, the re-nationalization of the Net became literally hardwired. Obliging intermediaries to check for unwanted content is a different matter. Some countries can implement such an agreement with much greater zeal than others. The same is true for an agreement on the mutual enforcement of content regulation. In these cases, the negotiation problem is compounded by the anticipated strategic interaction over implementation.

215 Cf. BENKLER in *Colorado Law Review* (1999) 28; LESSIG and RESNICK in *Michigan Law Review* (1999) 415.

216 BERMAN *Internet and Nation State* (2002) 95 is outspoken: "the distinctive benefits of the Internet should be jettisoned so that the existing jurisdictional framework can be preserved".

217 LESSIG and RESNICK in *Michigan Law Review* (1999) 423.

218 Cf. *Ibid.* in 415: "innovations that introduce new applications would be stifled, since the application layer gateways would not initially know about the new applications and hence would block them. The Internet's current architecture has enabled experimentation and rapid deployment of new applications"; see also SAMUELSON in Marsden (2000) at note 82.

VIII. How is Privacy Different?

So far, this paper has demonstrated why organizing co-existence in the area of Internet content regulation is hard to bring about. But why have states been able to accomplish it in the area of privacy regulation? And does this success not prove that all the impediments in the area of content regulation are surmountable as well? The answer to these questions comes in the steps already used for content regulation. Step 1 clarifies the issue. Step 2 determines national utility functions before the advent of the Internet. Step 2 assumes that there is no Internet and looks for national preferences. Step 3 drops this assumption. Steps 4 and 5 look for the conditions for coordinating national behaviour in general, and for organizing co-existence in particular.

1. The Issue

The protection of privacy can itself be framed as a value. The evaluation of this value is also contentious internationally. As demonstrated in the introduction, the Europeans in general, and the Germans in particular, value it much more than the Americans.²¹⁹ But this divergence in the evaluation is at most a background issue. The true European-American conflict is not about the erosion of the European commitment to high privacy standards. Nor are American political actors primarily concerned about increasing domestic pressure for stricter privacy standards.²²⁰ The conflict is much more down to earth. Europeans are afraid that the data of their nationals will be exposed to unacceptable risk when stored in the U.S. And U.S. businesses and policy-makers are unwilling to grant European data owners a degree of protection they would not give their domestic customers.²²¹

2. National Preferences before the Advent of the Internet

Governmental preferences vis-à-vis data protection can be analysed with the same conceptual tools as in the area of content regulation. The only small alteration concerns the interpretation of the term v in equation 1. The object is no longer social, but individual. Government no longer cares about the social phenomenon of a value, it cares about for the individual welfare of data owners. In accord with a strict rational choice perspective, the relevant object should be the data protection preferences of the median voter.²²² But the model is open for any other transformation of individual preferences into governmental ones. As with content regulation, v ranges from 0 to 1 as a measure of the degree of protection. Before the advent of the Internet, a country's openness to international interaction had only a small impact on v . Individuals communicated with foreigners; they carried out business or took tourist trips to foreign countries; they used foreign

219 NATIONAL RESEARCH COUNCIL Global Networks and Local Values (2002) 133-135 treats privacy as an internationally contentious value.

220 On this see SHAFFER in Yale Journal of International Law (2000).

221 From the rich literature see only REIDENBERG in Stanford Law Review (2000)

222 More from ROWLEY in Rowley (1993) .

services or bought foreign products. All this happened, and usually some personal data went along with it. But all this was marginal.

In the area of privacy, α varies considerably from country to country. Individuals in some countries value data protection much higher than in others.²²³ This can partly be explained by differences in the cultural backgrounds,²²⁴ partly by the level of the economic development.²²⁵ The differences in attitudes towards institutions for privacy protection are even more pronounced.²²⁶ Europeans in general, and Germans in particular, view privacy as an inalienable right, to be protected by public authority. Americans consider privacy a property right, which can and should be traded if this is efficient.²²⁷

3. Impact of the Internet on National Preferences

The impact of the Internet on national data protection preferences is likely to be profound; for the Internet exposes the privacy of national data owners to a much greater risk than before. The former natural barriers between national privacy legislation diminish considerably. This is due to three combined factors. First of all, because of the Internet, the distance cost of communication virtually disappears. Second, to the extent that products themselves are electronic, the cost of delivery also falls dramatically. Once a larger number of households has broadband access to the Internet, this statement even holds for a whole new range of products, like movies. Third, the Internet makes it possible to assemble huge amounts of personal data in one directory. This makes personality profiling a realistic option.²²⁸

All these developments increase the competitive pressure on national data protection rules. Actors who dislike the stronger European rules can export personal data to the U.S. or to outright data havens. Moreover, the Internet increases the market share of transnational transactions. Such transactions do not clearly and exclusively fall within the jurisdiction of one country. To the extent that these countries have differing philosophies of privacy, determining the applicable privacy standards inevitably becomes a contentious issue. Due to both developments, the problem-solving capacity of nation-states in the area of privacy protection is decreasing. Within the taxonomy of the model, privacy is shifting from being robust to being vulnerable.²²⁹

223 For an impressive treatment see BELLMAN, JOHNSON, KOBRIN and LOHSE Privacy Preferences (2002) .

224 E.g. collectivist cultures tend to value privacy less, Ibid. 6.

225 This may play itself out as a difference in penetration with a technology, or as a different familiarity with certain marketing tools, Ibid. 4.

226 Ibid. 5.

227 For a characteristic view see RIBSTEIN and KOBAYASHI State Regulation of Electronic Commerce (2001) "Informed consumers will give up personal information when its privacy value is less than what someone else is willing to pay for it" (13); "given transaction costs, an efficient default rule would maximize social surplus net of the costs of contracting around the rule" (14).

228 From the rich literature see BENKLER in Colorado Law Review (1999) 43 s; REIDENBERG in Stanford Law Review (2000) 1320-1325; RIBSTEIN and KOBAYASHI State Regulation of Electronic Commerce (2001) 7-9.

229 See again figure 2.

4. Coordination of National Behaviour in General

Is coordinating behaviour in the area of data protection a win-win solution for governments? As mentioned in the introduction, there is broad consensus on a set of fairly general first principles,²³⁰ but divergence on how to interpret them, and on choice of protective tools.²³¹ Among concomitant goods, the demonstration of problem-solving capacity might play a role. But the general interest in exploiting the full potential of the Internet certainly stands out. The intensity of international negotiations over data protection may also serve as evidence for the widespread interest of governments in cooperation.²³²

There may thus be a somewhat stronger convergence of preferences in the area of data protection than in the area of content regulation. But by far the more important difference between these two policy areas is strategic. As demonstrated, in the area of content regulation, cooperation is not only a public good, it is a weakest link good. This is not the case for privacy protection. Here, bilateral cooperation makes sense. There are two combined reasons for this. In content regulation, the protectee is diffuse. It is society at large. More precisely, it is all societies all over the world. In privacy protection, however, the protectee is defined. It is the single data owner. Protection technologies can therefore target a defined class of protectees. The U.S. government might, for instance, promise to impose certain rules on its nationals concerning how they are to deal with personal data that originates in Germany. More importantly even, in data protection the potential intruders are often specific, too. This is clearly the case if data owners have to deliberately give their data away in the first place. They use their credit card number, fill in personal information in an electronic form, or they trade electronically and thereby convey trade-related information.

The latter feature, it is true, is not ubiquitous. Data collection can be hidden, e.g. if the owner of a website extracts the e-mail address of the user from his hard disc. Web bugs are specifically designed such that the user will not realize what they do.²³³ Users may also have programmed their browsers such they accept all cookies, since they are not aware of the privacy risk involved.²³⁴ But even if one of these risks materializes, bilateral cooperation is still not useless; for the typical collector and user of private data is commercial. It is a firm that uses the data for marketing purposes. Of course, theoretically such a firm could move its headquarters to a country that is a data haven. But typically, it maintains a physical commercial presence in its country of origin.

This makes it vulnerable to regulatory activity in its traditional country of origin. Bilateral agreements on data protection do therefore have an open international flank. But the danger from

230 Details from REIDENBERG in *Stanford Law Review* (2000) 1326-1330.

231 *Ibid.* in 1331-1337.

232 *Ibid.* in 1355 he even speaks of a “crowded international space”, see REIDENBERG in *Stanford Law Review* (2000) 1356-1375 for an overview of the negotiation going on.

233 <http://rr.sans.org/covertchannels/bugs.php> (4/23/2002).

234 http://rr.sans.org/covertchannels/Internet_privacy.php; see also <http://rr.sans.org/covertchannels/sniffer.php> (4/23/2002).

this flank is not that bilateral agreements will become void. Realistically, they cannot make data protection watertight. But they can significantly improve it. The possibility of bilateral solutions does not make strategic interaction disappear. In particular, each negotiating partner can still have recourse to his ability to threaten the other with damages. But this is a general problem of public international law, and of bilateral international relations more generally. States do not always overcome it, but more often than not they do.²³⁵

5. Organizing Co-Existence in Particular

In content regulation, the characteristic feature of organizing co-existence is its lack of specificity. Such protection technologies do not distinguish between countries, and they do not discriminate between values. Organizing the co-existence of data protection rules is not as lacking in specificity. It is not so easy to trace it at all. The safe harbour compromise between the U.S. and the EU may serve as an example. In that compromise, the U.S. promises to back up self-regulatory mechanisms of the U.S. data users with FTC oversight. U.S. government or industry may find it advisable to apply this regime to the data of foreign, or even domestic, users. If so, the compromise has a positive regulatory externality. But if the contracting parties want to avoid the effect, they are free to do so. The FTC oversight can easily be tailored to the data of European data owners. Likewise, in the compromise one may detect a lack of specificity. As it stands, it applies to all data exported from Europe to the U.S. But again, this is a mere question of design. If the contracting parties deem fit, they might narrow the field of application down to specific types of data, to the data of a specific class of data owners, or to some protection tools, at the cost of others.

What, then, distinguishes full coordination from the mere organization of co-existence? Again this is not a question of principle, but of degree. In its conflict with the U.S., Europe has not been content with the standards or the processes prevalent in the U.S. What negotiators have achieved is thus a typical half-way solution. The substantive standards are above the general U.S. level, but below the general European level. Rule generation does not take place in parliament, but in self-regulatory negotiations. First order jurisdiction for rule application does not lie with an independent governmental official, but with the self-regulatory mechanism. But the U.S. accepts a policy bringing this mechanism under governmental oversight. Neither side thus retains full regulatory autonomy in the field of data protection. Such autonomy, of course, remains for cases with no transatlantic element. But once the case becomes transnational, each side partially gives in.

235 Explaining this outcome is beyond the purpose of this paper. One option is to switch from a one-shot to a repeated or even nested game, i.e. some form of issue linkage.

IX. Conclusions

This paper has asked a question of positive, not normative, analysis. It has tried to explain why organizing co-existence has proven feasible in the field of data protection, and impossible in the field of content regulation. Roughly, the character of the strategic interaction among states has turned out to be the most important difference between the two cases. In data protection, the typical conflict is of a one-to-one kind. It opposes the state who wants to protect the data of its nationals abroad, and the one state under whose jurisdiction these specific data come under risk. In content regulation, the typical conflict has a one-to-many character. It is not enough for a protecting state to prevent intrusions into locally cherished values originating from a defined second state's territory. Any intrusion of that kind, originating from whatever territory, must be prevented in order for protection to be effective. There are three reasons for this difference. Firstly, the protected good is different. In content regulation, the prevalence of the value in the local community is at stake, not only the value orientation of those individuals who would wish not to come across certain contents when surfing the Net. Secondly, in content regulation the typical intruders are diffuse, whereas in data protection they typically are multinational firms or other large business entities. Thirdly, in data protection a state can credibly threaten a specific foreign country with preventing data export to its territory, since the data importers care. The incentive structure of individual intruders in content regulation is different. They often do not even have an interest at all in reaching the audience in third countries. Even if they do individually, their governments usually do not.

One may ask whether the difference between the two cases is not more radical even. Data protection basically opposes (US) businesses to European individuals. Those who want to exploit European data are a fairly good regulatory target for the US government. And European governments have committed themselves to efficient data protection. Despite the transnational character of the Internet, governments do thus still organise the collectivities tolerably well. This is much more questionable in the area of content regulation. The Internet allows everybody to become a broadcaster at a trivial price, and to choose the technical place of origin almost at will. And those who want to get access to locally disliked contents can, at least for the time being, escape national control quite easily. Both at the senders' and at the receivers' side, sovereignty thus no longer effectively organises collectivities. Put in the language used in the previous paragraph: content regulation is a one-to-many conflict, opposing the protecting state with millions of potential intruders, and billions of potential users.

What are the normative conclusions to be drawn from this? First of all, the message of this paper should not be misunderstood. It does not argue that the protection of local values is impossible. The parallel to the discourse over climate change is telling. Organizing co-existence resembles what in climate change is called mitigation. In both fields it is pretty hard to bring about, and for similar reasons. But in both fields adaptation is also an alternative. This is, admittedly, a less causal therapy. The climate does change. Internet users are indeed exposed to contents at variance with local values. But the countries protect themselves. In the area of content regulation, there are many ways to do so. The technical solution is filtering. If it is to be effective, it is likely

that government will need stiff competition among suppliers of filters, driving quality up and price down. Another option would consist in fostering what is usually called “media competence”. Users learn to tolerate that there are different baskets of values out there in the world. They accept that their own set of values is historically contingent, but nonetheless valuable.

The second normative issue concerns situations where organizing co-existence is a practical option. Should countries go for that option? This paper implicitly gives the answer. The benefit of doing so has to be compared to the additional cost involved, both evaluated subjectively. Equation 1 is thus not only an analytic tool, it is also a normative one. But it would not be enough to apply this equation to one technology for organizing co-existence in isolation; for the object of the evaluation is an institution. And institutions can only be evaluated comparatively. Equation 1 must therefore be applied separately to each institution that might help organize co-existence. And a country’s best choice for organizing co-existence can only be determined in reference to its unilateral options. Were there a uniform normative currency, all this would be no more than an exercise of calculus. But, as demonstrated, the normative criteria for evaluating the benefit of some degree of protection and the several types of opportunity cost are incommensurable. The formal model is thus not able to replace the normative choice of a country. It can only help that country avoid overlooking relevant criteria. And it can help structure the process of deliberate choice.

References

- AINSLIE, GEORGE (1992). *Picoeconomics. The Strategic Interaction of Successive Motivational States Within the Person*. Cambridge England ; New York, NY, Cambridge University Press.
- ALBERT, HANS (1978). *Traktat über rationale Praxis*. Tübingen, Mohr.
- ARCE, DANIEL G. and TODD SANDLER (2003). "An Evolutionary Game Approach to Fundamentalism and Conflict." *Journal of Institutional and Theoretical Economics* **159**: Forthcoming.
- ARROW, KENNETH JOSEPH (1995). *Barriers to Conflict Resolution*. New York, W.W. Norton.
- BAIRD, DOUGLAS G., ROBERT H. GERTNER, et al. (1994). *Game Theory and the Law*. Cambridge, Mass., Harvard University Press.
- BARLOW, JOHN P. (1997). Leaving the Physical World.
http://www.eff.org/Publications/John_Perry_Barlow/HTML/leaving_the_physical_world.html
- BELLMAN, STEVEN, ERIC J. JOHNSON, et al. (2002). Regional Differences in Privacy Preferences. Implications for the Globalization of Electronic Commerce
- BENKLER, YOCHAI (1999). "Net Regulation. Taking Stock and Looking Forward." *Colorado Law Review* **71**: 1203-1261.
- BENKLER, YOCHAI (2000). "Internet Regulation. A Case Study in the Problem of Unilateralism." *European Journal of International Law* **11**: 171-185.
- BENNETT, COLIN J. (1992). *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*. Ithaca, Cornell University Press.
- BENNETT, COLIN J. and REBECCA A. GRANT (1999). *Visions of Privacy. Policy Choices for the Digital Age*. Toronto, University of Toronto Press.
- BERMAN, PAUL SCHIFF (2002). The Internet, the Nation-State, and the Social Meaning of Legal Jurisdiction
- BINMORE, K. G. (1994). *Game Theory and the Social Contract*. Cambridge, Mass., MIT Press.
- BOHNET, IRIS (1997). *Kooperation und Kommunikation. Eine ökonomische Analyse individueller Entscheidungen*. Tübingen.
- BÖRZEL, TANJA A. and THOMAS RISSE (2001). Die Wirkung internationaler Institutionen. Von der Normanerkennung zur Normeinhaltung. Preprints aus der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter Bonn 2001/15

- BOSI, STEFANO (1998). "Altruism and Optimality from a Differentiable Viewpoint." *Rivista Internazionale di Scienze Sociali* **106**: 379-412.
- BOYLE, JAMES (1997). "Foucault in Cyberspace. Surveillance, Sovereignty, and Hardwired Censors." *University of Cincinnati Law Review* **66**: 177-205.
- BRAMS, STEVEN J. and ALAN D. TAYLOR (1999). *The Win-Win solution. Guaranteeing Fair Shares to Everybody*. New York, W.W. Norton.
- BREMNER, J. DOUGLAS and CHARLES R. MARMAR (1998). *Trauma, memory, and dissociation*. Washington, DC, American Psychiatric Press.
- BUCHANAN, JAMES M. (1965). "An Economic Theory of Clubs." *Economica* **32**: 1-14.
- BUCHANAN, JAMES M. and GORDON TULLOCK (1962). *The Calculus of Consent. Logical Foundations of Constitutional Democracy*. Ann Arbor,, University of Michigan Press.
- CLARK, JOHN MAURICE (1961). *Competition as a Dynamic Process*. Washington,, Brookings Institution.
- COCKFIELD, ARTHUR (2001). "Transforming the Internet into a Taxable Forum. A Case Study in E-Commerce Taxation." *Minnesota Law Review* **85**: 1171-1267.
- CORNES, RICHARD and TODD SANDLER (1996). *The Theory of Externalities, Public Goods and Club Goods*. Cambridge, Cambridge University Press.
- DAM, KENNETH W. (1999). "Self-Help in the Digital Jungle." *Journal of Legal Studies* **28**: 393-412.
- DAVID, PAUL A. (2000). The Internet and the Economics of Network Technology Evolution. *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values*. Christoph Engel und Kenneth H. Keller. Baden-Baden, Nomos: 39-71.
- DAWKINS, RICHARD (1986). *The Blind Watchmaker*. New York, W. W. Norton.
- DELLAPENNA, JOSEPH W. (2000). Law in a Shrinking World. The Interaction of Science and Technology with International Law. Villanova Public Law and Legal Theory Research Paper Series
- DERTOUZOS, MICHAEL (1997). *What Will Be. How the New World of Information will Change our Lives*. San Francisco, Harper Edge.
- DONALD, MERLIN (1999). Hominide Enculturation and Cognitive Evolution. *Cognition and Material Culture. The Archeology of Symbolic Storage*. Colin Renfrew und Chris Scarre. Cambridge, McDonald Institute for Archeological Research: 7-17.

- EDELMAN, MURRAY J. (1964). *The Symbolic Uses of Politics*. Urbana., University of Illinois Press.
- EGERBERG, MORTEN (2002). An Organisational Approach to European Integration. What Organisation Tells us about System Transformation, Committee Governance and Commission Decision Making
- EGGERTSSON, THRAINN (1990). *Economic Behavior and Institutions*. Cambridge England ; New York, Cambridge University Press.
- EISENBERG, ANDREA (2001). *Stabilität und Wandel informeller Institutionen*. Kassel.
- ENGEL, CHRISTOPH (1988). "Die Bedeutung des Völkerrechts für die Anwendung in- und ausländischen Wirtschaftsrechts." *RabelsZ* **52**: 271-302.
- ENGEL, CHRISTOPH (1999). Vertrauen – ein Versuch. Preprints aus der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter Bonn 1999/12
- ENGEL, CHRISTOPH (2000). The Internet and the Nation State. *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values*. Christoph Engel und Kenneth H. Keller. Baden-Baden, Nomos: 201-260.
- ENGEL, CHRISTOPH (2001). Die Grammatik des Rechts. *Instrumente des Umweltschutzes im Wirkungsverbund*. Hans-Werner Rengeling. Baden-Baden, Nomos: 17-49.
- ENGEL, CHRISTOPH (2001). "Offene Gemeinwohldefinitionen." *Rechtstheorie* **32**: 23-52.
- ENGEL, CHRISTOPH (2002). *Abfallrecht und Abfallpolitik*. Baden-Baden, Nomos.
- ENGEL, CHRISTOPH (2002). The Role of Law in the Governance of the Internet
- ESTY, DANIEL C. (2000). "Regulatory Competition in Focus." *Journal of International Economic Law* **3**(2): 215-385.
- FARNSWORTH, WARD (2000). Do Parties to Nuisance Cases Bargain After Judgement ? A Glimpse into the Cathedral. *Behavioral Law and Economics*. Cass R. Sunstein. Cambridge, Cambridge University Press: 302-322.
- FARRELL, HENRY (2002). "Hybrid Institutions and the Law. Outlaw Arrangements or Interface Solutions?" *Zeitschrift für Rechtssoziologie*: Forthcoming.
- FARRELL, HENRY (2002). Negotiating Privacy across Arenas. The EU-US 'Safe Harbour' Discussions. *Common Goods. Reinventing European and International Governance*. Adrienne Héritier. London, Rowman & Littlechild: 105-126.
- FELDMAN, ALLAN M. (1980). *Welfare Economics and Social Choice Theory*. Boston, Martinus Nijhoff Pub.

- FESTINGER, LEON (1957). *A Theory of Cognitive Dissonance*. Evanston, Ill., Row Peterson.
- FOWLER, BRENDON, CARA FRANKLIN, et al. (2001). "Can you Yahoo!?! The Internet's Digital Fences." *Duke Law and Technology Review*: 0012.
- FREY, BRUNO and FELIX OBERHOLZER-GEE (1999). Natural Environment. Fair Siting Procedures. *Economics as a Science of Human Behaviour*. Bruno Frey. Boston: 23-48.
- FREY, DIETER and ANNE GASKA (1993). Die Theorie der kognitiven Dissonanz. *Theorien der Sozialpsychologie I Kognitive Theorien*. Dieter Frey und Martin Irle. Bern, Hans Huber: 275-326.
- FROOMKIN, A. MICHAEL (1996). "Flood Control on the Information Ocean. Living With Anonymity, Digital Cash, and Distributed Databases." *University of Pittsburgh Journal of Law and Commerce* **15**: 395-507.
- FROOMKIN, A. MICHAEL (1997). The Internet as a Source of Regulatory Arbitrage. *Borders in Cyberspace. Information Policy and the Global Information Infrastructure*. Brian Kahin und Charles Nesson. Cambridge, MIT Press: 129-163.
- FROWEIN, JOCHEN A. (2000). "Konstitutionalisierung des Völkerrechts." *Berichte der Deutschen Gesellschaft für Völkerrecht* **39**: 427-447.
- GEIST, MICHAEL A. (2001). "Is There a There There? Toward Greater Certainty for Internet Jurisdiction." *Berkeley Technology Law Journal* **16**: 1345-1406.
- GEIST, MICHAEL A. (2001). "The Legal Implications of the Yahoo! Inc. Nazi Memorabilia Dispute." *Juriscom*: January/March.
- GERKEN, LÜDER, Ed. (1995). *Competition Among Institutions*. Houndmills, MacMillan.
- GIGERENZER, GERD, PETER M. TODD, et al. (1999). *Simple Heuristics that Make us Smart*. New York, Oxford University Press.
- GINSBURG, JANE C. (2000). "Copyright Use and Excuse on the Internet." *Columbia Journal of Law and the Arts* **24**: 1-38.
- GOLDSMITH, JACK (1998). "Against Cyberanarchy." *University of Chicago Law Review* **65**: 1199-1250.
- GOLDSMITH, JACK (2000). The Internet, Conflicts of Regulation, and International Harmonization. *Governance of Global Networks in the Light of Differing Local Values*. Christoph Engel und Kenneth H. Keller. Baden-Baden, Nomos: 197-208.
- GOLDSMITH, JACK (2000). "Unilateral Regulation of the Internet. A Modest Defence." *European Journal of International Law* **11**: 135-148.

- HANSJÜRGENS, BERND and GERTRUDE LÜBBE-WOLFF, Eds. (2000). *Symbolische Umweltpolitik*. Frankfurt, Suhrkamp.
- HECHT, DIETER (1999). *Stoffpolitik als Ordnungspolitik. Zur marktwirtschaftlichen Steuerung von Stoffströmen*. Marburg.
- HERITIER, ADRIENNE, CHRISTOPH KNILL, et al. (1996). *Ringing the Changes in Europe. Regulatory Competition and the Transformation of the State : Britain, France, Germany*. Berlin ; New York, Walter de Gruyter.
- HETCHER, STEVEN (2000). "The FTC as Internet Privacy Entrepreneur." *Vanderbilt Law Review* **53**: 2041-2062.
- HIRSCHMAN, ALBERT O. (1970). *Exit, Voice, and Loyalty. Responses to Decline in Firms, Organizations, and States*. Cambridge, Mass., Harvard University Press.
- HOBBS, THOMAS (1651). *Leviathan, or, The matter, forme, & power of a common-wealth ecclesiasticall and civill*. London., Printed for Andrew Ckooke i.e. Croke at the Green Dragon in St. Pauls Church-yard.
- HUNTINGTON, SAMUEL P. (1996). *The Clash of Civilizations and the Remaking of World Order*. New York, Simon & Schuster.
- JELLINEK, GEORG and WALTER JELLINEK (1914). *Allgemeine Staatslehre*. Berlin., O. Hèaring.
- JOHNSON, DAVID R. and DAVID G. POST (1996). "Law and Borders. The Rise of Law in Cyberspace." *Stanford Law Review* **48**: 1367-1376.
- JONES, PHIL, Ed. (1999). *Taboo*. Philadelphia, Jessika Kingsley.
- JOSEPH, CUTHBERT (1969). *Nationality and Diplomatic Protection. The Commonwealth of Nations*. Leyden., A. W. Sijthoff.
- KAHLER, MILES (2000). Information Networks and Global Politics. *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values*. Christoph Engel und Kenneth H. Keller. Baden-Baden, Nomos: 141-158.
- KALATHIL, SHANTHI and TAYLOR C. BOAS (2001). The Internet and State Control in Authoritarian Regimes. China, Cuba, and the Counterrevolution. Carnegie Endowment of International Peace Working Paper 21
- KATZ, MICHAEL L. and CARL SHAPIRO (1985). "Network Externalities, Competition, and Compatibility." *American Economic Review* **75**: 424-440.
- KERBER, WOLFGANG (1998). "Erfordern Globalisierung und Standortwettbewerb einen Paradigmenwechsel in der Theorie der Wirtschaftspolitik ?" *Ordo* **49**: 253-268.

- KERSTING, WOLFGANG (1997). *Moralphilosophie, Dezsionismus und pragmatische Rationalität. Recht, Gerechtigkeit und demokratische Tugend. Abhandlungen zur praktischen Philosophie der Gegenwart.* Wolfgang Kersting. Frankfurt: 353-396.
- KING, GARY, ROBERT O. KEOHANE, et al. (1994). *Designing Social Inquiry. Scientific Inference in Qualitative Research.* Princeton, N.J., Princeton University Press.
- KLEIN, ECKART (1976). *Umweltschutz im völkerrechtlichen Nachbarrecht.*
- KOBRIN, STEPHEN J. (1997). The Architecture of Globalization. State Sovereignty in a Networked Global Economy. *Governments, Globalization, and International Business.* John H. Dunning. Oxford, Oxford University Press: 146-171.
- LAIBSON, DAVID (1997). "Golden Eggs and Hyperbolic Discounting." *Quarterly Journal of Economics* **112**: 443-477.
- LEHMKUHL, DIRK (2002). "****." *Zeitschrift für Rechtssoziologie* **23**: Forthcoming.
- LESSIG, LAWRENCE (1999). *Code and other Laws of Cyberspace.* New York, Basic Books.
- LESSIG, LAWRENCE and PAUL RESNICK (1999). "Zoning Speech on the Internet. A Legal and Technical Model." *Michigan Law Review* **98**: 395-413.
- LEVINE, DAVID K. (1998). "Modeling Altruism and Spitefulness in Experiments." *Review of Economic Dynamics* **1**: 593-622.
- LIEBOWITZ, S.J. and STEPHEN E. MARGOLIS (1995). "Are Network Externalities a New Source of Market Failure ?" *Research in Law and Economics* **17**: 1-22.
- LITAN, ROBERT E. (2001). "Law and Policy in the Age of the Internet." *Duke Law Journal* **50**: 1045-1085.
- LOEWENSTEIN, GEORGE F. and DRAZEN PRELEC (2000). Preferences for Sequences of Outcomes. *Choices, Values, and Frames.* Daniel Kahneman und Amos Tversky. Cambridge, Cambridge University Press: 565-577.
- LOEWENSTEIN, GEORGE and DRAZEN PRELEC (1992). "Anomalies in Intertemporal Choice. Evidence and an Interpretation." *Quarterly Journal of Economics* **107**: 573-598.
- LÜBBE, WEYMA (2002). Epistemische Pflichten in der "Wissensgesellschaft". *Wissen, Nichtwissen, Unsicheres Wissen.* Christoph Engel, Jost Halfmann und Martin Schulte. Baden-Baden, Nomos: Forthcoming.
- MAJONE, GIANDOMENICO (2001). "Nonmajoritarian Institutions and the Limits of Democratic Governance. A Political Transaction-Cost Approach." *Journal of Institutional and Theoretical Economics* **157**: 57-78.

- MANN, CATHERINE L., SUE E. ECKERT, et al. (2000). *Global Electronic Commerce. A Policy Primer*. Washington, DC, Institute for International Economics.
- MANTZAVINOS, CHRYSOSTOMOS (2001). *Individuals, Institutions, and Markets*. Cambridge, UK ; New York, Cambridge University Press.
- MAYER, FRANZ C. (2000). "Europe and the Internet. The Old World and the New Medium." *European Journal of International Law* **11**: 149-169.
- MENG, WERNER (1994). *Extraterritoriale Jurisdiktion im öffentlichen Wirtschaftsrecht*. Berlin ; New York, Springer.
- MITROFF, IAN I. and RALPH H. KILMANN (1978). "On Integrating Behavioral and Philosophical Systems. Towards a Unified Theory of Problem-Solving." *Research in Sociology of Knowledge, Sciences & Art*: 207-238.
- MONOPOLKOMMISSION (1998). *Systemwettbewerb*. Baden-Baden, Nomos.
- MUELLER, MILTON (1999). "ICANN and Internet Governance. Sorting Through the Debris of 'Self-Regulation'." *info* **1**: 497-520.
- MÜLLER, MARKUS (2000). *Systemwettbewerb, Harmonisierung und Wettbewerbsverzerrung*. Baden-Baden, Nomos.
- MYERSON, ROGER B. (1999). "Nash Equilibrium and the History of Economic Theory." *Journal of Economic Literature* **37**: 1067-1082.
- NACHBAR, THOMAS B. (2000). "Paradox and Structure. Relying on Government Regulation to Preserve the Internet's Unregulated Character." *Minnesota Law Review* **85**: 215-318.
- NATIONAL RESEARCH COUNCIL (1996). *Cryptography's Role in Securing the Information Society*. Washington, National Academy.
- NATIONAL RESEARCH COUNCIL (2000). *The Digital Dilemma. Intellectual Property in the Information Age*. Washington, National Academy Press.
- NATIONAL RESEARCH COUNCIL (2002). *Global Networks and Local Values*. Washington, National Academy of Sciences.
- NATIONAL RESEARCH COUNCIL (2002). *Youth, Pornography, and the Internet*. Washington, National Academy Press.
- NELSON, RICHARD R. (1995). "Recent Evolutionary Theorizing about Economic Change." *Journal of Economic Literature* **33**: 48-90.
- OSBORNE, MARTIN J. and ARIEL RUBINSTEIN (1990). *Bargaining and Markets*. San Diego, Academic Press.

- OSTHAUS, WOLF (2000). Local Values, Global Networks, and the Return of Private Law. On the Function of Civil Law and Private International Law in Cyberspace. *Governance of Global Networks in the Light of Differing Local Values*. Christoph Engel und Kenneth H. Keller. Baden-Baden, Nomos: 209-236.
- OSTROM, ELINOR (1998). "A Behavioral Approach to the Rational Choice Theory of Collective Action." *American Political Science Review* **92**: 1-22.
- PERRITT, HENRY H. (1996). "Jurisdiction in Cyberspace." *Villanova Law Review* **41**: 1-128.
- PERRITT, HENRY H. (1998). "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Stengthening National and Global Governance." *Indiana Journal of Global Legal Studies* **5**: 423-442.
- PILDES, RICHARD H. and CASS R. SUNSTEIN (1995). "Reinventing the Regulatory State." *Univer-sity of Chicago Law Review* **62**: 1-129.
- POST, DAVID G. (1997). "Governing Cyberspace." *Wayne Law Review* **43**: 155-171.
- POST, DAVID G. (2000). "What Larry Doesn't Get. Code, Law and Liberty in Cyberspace." *Stan-ford Law Review* **52**: 1439-1459.
- PRICE, MONROE E. and STEFAN G. VERHULST (2000). In Search of the Self. Charting the Course of Self-Regulation on the Internet in a Global Environment. Cardozo Law School Public Law Working Paper 015
- PRZETACZNIK, FRANCISZEK (1983). *Protection of Officials of Foreign States According to Inter-national Law*. The Hague ; Boston; Hingham, MA, Martinus Nijhoff.
- RADIN, MARGARET JANE and R. POLK WAGNER (1998). "The Myth of Private Ordering. Redis-covering Legal Realism in Cyberspace." *Chicago Kent Law Review* **73**: 1295-1317.
- REIDENBERG, JOEL (1996). "Governing Networks and Rule-Making in Cyberspace." *Emory Law Journal* **45**: 911-930.
- REIDENBERG, JOEL (1998). "Lex Informatica. The Formulation of Information Policy Rules Through Technology." *Texas Law Review* **76**: 553-593.
- REIDENBERG, JOEL (2000). "Resolving Conflicting International Data Privacy Rules in Cyber-space." *Stanford Law Review* **52**: 1315-1376.
- REIDENBERG, JOEL (2002). "Yahoo and Democracy on the Internet." *Jurimetrics* **42**.
- RIBSTEIN, LARRY E. and BRUCE H. KOBAYASHI (2001). State Regulation of Electronic Com-merce

- RICHTER, RUDOLF and EIRIK FURUBOTN (1999). *Neue Institutionenökonomik. Eine Einführung und kritische Würdigung*. Tübingen, Mohr.
- ROWLEY, CHARLES K. (1993). The Relevance of the Median Voter Theorem. *Public Choice Theory. I: Homo Oeconomicus in the Political Market Place*. Charles K. Rowley. Aldershot, Elgar: 202-224.
- SAMUELSON, PAMELA (2000). Five Challenges for Regulating the Global Information Society. *Regulating the Global Information Society*. Chris Marsden, Routledge.
- SAMUELSON, PAUL A. (1954). "The Pure Theory of Public Expenditure." *Review of Economics and Statistics* **36**: 387-389.
- SAMUELSON, PAUL A. (1955). "A Diagrammatic Exposition of a Theory of Public Expenditure." *Review of Economics and Statistics* **37**: 350-356.
- SASSEN, SASKIA (1996). *Losing Control? Sovereignty in an Age of Globalization*. New York, Columbia University Press.
- SASSEN, SASKIA (1998). "On the Internet and Sovereignty." *Indiana Journal of Global Legal Studies* **5**: 545-560.
- SCHÄFER, WOLF (1999). Globalisierung: Entmonopolisierung des Nationalen ? *Globalisierung der Wirtschaft. Ursachen - Formen - Konsequenzen*. Hartmut Berg. Berlin: 9-21.
- SCHARPF, FRITZ WILHELM (1997). *Games Real Actors Play. Actor-centered Institutionalism in Policy Research*. Boulder, Colo., Westview Press.
- SCHARPF, FRITZ WILHELM (1997). "The Problem-Solving Capacity of Multi-Level Governance." *Journal of European Public Policy* **4**: 520-538.
- SCHLICHT, EKKEHART (1998). *On Custom in the Economy*. Oxford ; New York, Clarendon Press.
- SCHWARCZ, STEPHEN L. (2002). *Private Ordering*. Duke University
- SHAFFER, GREGORY (2000). "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards." *Yale Journal of International Law* **25**: 1-88.
- SHAPIRO, CARL and HAL R. VARIAN (1998). *Information Rules. A Strategic Guide to the Network Economy*. Boston, Mass., Harvard Business School Press.
- SIMON, LESLIE DAVID (2000). *NetPolicy.Com. Public Agenda for a Digital World*. Washington, D.C., Baltimore, Md., Woodrow Wilson Center Press.
- SLAUGHTER, ANN MARIE (1997). "The Real New World Order." *Foreign Affairs* **76**: 183-&.

- SMITH, ADAM (1776). *An Inquiry into the Nature and Causes of the Wealth of Nations*. London, Printed for W. Strahan; and T. Cadell ...
- SPAR, DEBORA L. (2001). *Ruling the Waves. Cycles of Discovery, Chaos, and Wealth from Compass to the Internet*. New York, Harcourt.
- STARK, ODED (1995). *Altruism and Beyond. An Economic Analysis of Transfers and Exchanges within Families and Groups*. Cambridge <England> ; New York, NY, Cambridge University Press.
- STRÖBELE, WOLFGANG (1987). *Rohstoffökonomik. Theorie natürlicher Ressourcen mit Anwendungsbeispielen Öl, Kupfer, Uran und Fischerei*. München, Vahlen.
- STRÖBELE, WOLFGANG (1991). Abdiskontierung als kontextabhängiges Problem. *Die ökologische Herausforderung für die ökonomische Theorie*. Frank (ed.) Beckenbach. Marburg: 151-155.
- SUNSTEIN, CASS R. (1996). "Legislative Foreword. Congress, Constitutional Moments, and the Cost-Benefit State." *Stanford Law Review* **48**: 247-309.
- SWIRE, PETER (1998). "Of Elephants, Mice and Privacy. International Choice of Law and the Internet." *International Lawyer* **32**: 991-1025.
- TESSER, ABRAHAM, DIEDERIK A. STAPEL, et al. (2002). *Self and Motivation. Emerging Psychological Perspectives*. Washington, DC, American Psychological Association.
- THOMPSON, M., RICHARD ELLIS, et al. (1990). *Cultural Theory*. Boulder, Colo., Westview Press.
- TRACHTMAN, JOEL P. (1998). "Cyberspace, Sovereignty, Jurisdiction and Modernism." *Indiana Journal of Global Legal Studies* **5**: 561-582.
- TRACHTMAN, JOEL P. (2001). *Economic Analysis of Prescriptive Jurisdiction and Choice of Law*. Tufts University
- VANBERG, VICTOR and JAMES M. BUCHANAN (1989). "Interests and Theories in Constitutional Choice." *Journal of Theoretical Politics* **1**: 49-62.
- VERWEIJ, MARCO (2000). *Transboundary Environmental Problems and Cultural Theory. The Protection of the Rhine and the Great Lakes*. Houndmills, Basingstoke, Hampshire ; New York, Palgrave.
- VISCUSI, W.KIP (2000). *Risk Equity*. Harvard John M. Olin Center for Law, Economics, and Business Discussion Paper
- VON NEUMANN, JOHN and OSKAR MORGENSTERN (1944). *Theory of Games and Economic Behavior*. Princeton, Princeton university press.

- WEBSTER, HUTTON (1942). *Taboo. A Sociological Study*. Stanford University, Calif; London,, Stanford University Press; H. Milford Oxford University Press.
- WEGNER, GERHARD (1996). *Wirtschaftspolitik zwischen Selbst- und Fremdsteuerung - ein neuer Ansatz*. Baden-Baden, Nomos.
- WEGNER, GERHARD (1997). "Economic Policy from an Evolutionary Perspective. A New Approach." *Journal of Institutional and Theoretical Economics* **153**: 485-509.
- WEIGEND, A (1994). On Overfitting and the Effective Number of Hidden Units. *Proceedings of the 1993 Connectionist Models Summer School*. Michael C. Mozer. Hillsdale, New Jersey, LEA: 335-342.
- WEINBERG, JONATHAN (1997). "Rating the Net." *Hastings Communications and Entertainment Law Journal* **19**: 453-482.
- WILHELMSSON, THOMAS, SALLA TUOMINEN, et al. (2000). *Consumer Law in the Information Society*. London ; Boston, Kluwer Law International.
- WITT, ULRICH (1996). Path-Dependence in Institutional Change. *The Evolutionary Principles of Economics*. K Dopfer. Cambridge, Cambridge University Press.
- YEE, ALBERT S. (1996). "The Causal Effects of Ideas on Policies." *International Organization* **50**: 66-108.