Department of Political and Social Sciences

The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A Comparative Federalism Approach

Fernando Mendez

Thesis submitted for assessment with a view to obtaining the degree of
Doctor of Political and Social Sciences of the European University Institute

Florence, March 2007

EUROPEAN UNIVERSITY INSTITUTE
Department of Political and Social Sciences

The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A Comparative Federalism Approach

Fernando Mendez

Thesis submitted for assessment with a view to obtaining the degree of
Doctor of Political and Social Sciences of the European University Institute

Jury Members:

Prof. Martin Rhodes (EUI/Denver University) (Supervisor)
Prof. Andreas Auer (University of Geneva)
Prof. David McKay (University of Essex)
Prof. Alexander Trechsel (EUI)

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

to my parents, José y Emelina

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Acknowledgments

'The time you enjoy wasting is not wasted time'

Bertrand Russell

For a number of reasons, most of them unconnected to the task at hand, writing this dissertation took considerably longer than it should have. While this may be true of most PhD's, it has been particularly so in this case. Because of this, the support network that made it possible needs to be especially singled out. It is not possible to give sufficient credit to all of those who contributed to this endeavour but the very few that are mentioned in these acknowledgments deserve a special thanks. Apart from my parents, to whom this PhD is dedicated, I need to thank my thesis supervisor Martin Rhodes. I was far from being a model student, and his patience has been more than tested throughout this haphazard intellectual journey of mine. Yet, he managed to persevere with what for him must have seemed an awkward case. For his patience I am especially grateful. At the same time, this dissertation would not have been possible without spending quite lengthy periods in both the US and Switzerland. Two individuals, Martin Rhodes and Alexander Trechsel, allowed this to happen and my sincerest gratitude goes out to them for making these intellectually stimulating and personally enriching experiences possible. In addition, two research centres provided me with a valuable academic home and support environment – BRIE, at Berkeley, and the c2d, at the University of Geneva. In particular, I cannot give sufficient credit to the c2d and its academic staff. They have all provided me with much support and friendship, as well as helping me to make sense of a fascinating political system, the Swiss one, in many ways a microcosm of the EU.

Another microcosm of the EU, the European University Institute, has also helped to shape my ideas and views. I am grateful for the opportunity and the privilege to have studied in this unique academic environment. The social bonds that were formed (and broken) in this remarkable Renaissance setting, the endless discussions and late dinners, all contributed to making this period

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

in my life especially rewarding. Despite my many failings, Raphael Kies and Melonie Rogers were always there for me and deserve my sincerest gratitude. Some very special friends also made my experiences in Florence incredibly enriching, they include Javier Ramos-Diaz, Navraj Ghaleigh, Jonathan Wheatley, Jesse Scott and Gopal Balakrishan.

I have also been blessed by the good fortune of having two brothers, Mario and Carlos, each in their own way a specialist in areas of EU policy and law. I have learned more from them than I have ever cared to admit. Our intellectual jostles over the years have helped to shape and refine many of the arguments I have advanced. But more important than this has been their unwavering support. In particular, Mario, who not only had to endure the misfortune of sharing an apartment with me, but who also painstakingly read and commented on the entire manuscript. For these and many other efforts, I am eternally grateful.

Others who deserve a very special mention include: Philippe Schmitter, Daniel Verdier, Stefano Bartolini, Andreas Auer, David McKay, Michael Newman, John Zysman, David Bach, Frank Brouwer, Mary Farrell, Uwe Serduelt, Michael Peart, Mike Butzer, Gabriella Unger, Maureen Lechleitner, Marie-Ange Cattotti, Nancy Altobelli, Virginie Barral, and others that will be mentioned simply by their first names, Andria, Katia, Heidi, Manon and Maxime, Eva and Irina, Maria, Metereta, and Hugo. Last, but by no means least, I should thank Vicky Triga who has provided relentless support, especially during the final stages.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

TABLE OF CONTENTS

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Summary

This dissertation analyses the dynamics of EU policymaking through a structured and focused comparison with two other federal polities: the United States and Switzerland. To this end, it draws on the wider comparative federalism literature to examine how basic federal political institutions *structure* the development of policy outcomes. The empirical *focus* is on the regulatory challenge posed by the internet's spectacular proliferation during the period of 1995-2005. Two hypotheses are formulated as to how basic federal political institutions shape the development of policy outcomes in the three polities under investigation. First, given the cross-border nature of the policy challenge, we expect to find similar interactions among the different levels of government in all three units of analysis. In particular, federal level political actors should be similarly mobilised into offering centralising solutions to problems with cross-border effects. Furthermore, this could provoke allocational shifts in authority towards the centre in the three units of analysis. Second, it is expected that differences in the policy *process* and the 'power capabilities' of the centre help to explain the variance in policy outcomes. The main findings of the empirical investigation suggest that the dynamics of policymaking in the realm of internet regulation exhibit similarities that make EU comparison with other federal polities across these dimensions especially revealing. This is particularly the case when comparing the EU with polities characterised by an extremely decentralised federal configuration, institutionally weak centres, consensual modes of decision-making, and decentralised modes of policy implementation such as Switzerland.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 1 Introduction

The internet's proliferation over the past decade has been nothing short of spectacular. In little over a decade, and especially since the development of the first internet browser in 1995, the new medium has literally exploded into the public domain. Apart from its many liberating and positive features, it has triggered a series of governance dilemmas and raised some thorny regulatory issues for policymakers. Some of the most controversial policy problems touch upon a very sensitive area of national sovereignty: internal security. These include addressing the availability of illegal and harmful content (e.g. child pornography, obscene and xenophobic material), curbing the possibilities for mass-scale copyright infringement or the scope for the illegal collection of personal data. All of these problems have been exacerbated to an unprecedented scale by the internet's proliferation. New problems have also emerged as a result of our increasing reliance on computers and information networks. We are more vulnerable to the spread of computer viruses or, in the case of many corporate organisations, to the dangers posed by denial of service attacks from hackers. Moreover, in the post-9/11 context, there are increasing concerns about the safety of vital information infrastructures, such as telecommunications and financial services, and the latter's susceptibility to cyber attacks from terrorists or disgruntled hackers. In parallel, the timely access by law enforcement to citizens' data, much of it stored in cyberspace by private sector organisations, has become a politically controversial issue. All of these problems have in common the fact that they activate, whether directly or indirectly, important concerns about internal security, such as the role of law enforcement agencies or defence/security agencies, and, more generally, the very operation of the criminal and justice system. In other words, these are all issues that go to the very core of national sovereignty and statehood.

It is very surprising, therefore, that during the period of 1995-2005, the EU, which is not a state in the traditional sense, has managed to: harmonise penal legislation among its member states in the area computer crime and in

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

relation to illegal internet content; create a new regulatory agency responsible for cybersecurity and a task force for addressing cyberterrorism; develop new mechanisms for investigating copyright theft; harmonise certain criminal penalties for copyright violation; introduce measures that harmonise how law enforcement agencies within member states retain and gain access to sensitive communications data for internal security purposes; introduce a European arrest warrant that includes within its scope of applicability many internet-related crimes. All these developments, and the many more that are brought out in the investigation, go well beyond the scope of the EU's traditional regulatory remit and touch upon core areas of statehood. This dissertation's main argument is that the EU has responded to the internet challenge in a way that is comparable to that of a very particular type of political organisation: a federal system. The answer to the puzzle, therefore, is to analyse the EU from an explicit 'comparative federalism' perspective. The explanation put forward implies that, not only is it more profitable to analyse the EU from a comparative perspective than as a unique case, but that such a framework should be based on a particular class of federal system: a 'compound polity'. Drawing on a 'compound polity' conceptualisation, this dissertation analyses the policy dynamics in the area of internet regulation during the period 1995-2005 in three federal systems, the US, Switzerland and the EU, with a view to better understanding the latter's version of federalism.

The major objective of this dissertation is to gain theoretical insights on the political system of the EU through a structured and focused comparison with two other federal systems. The substantive justification for doing so is directly related to the 'state of the art' in a sub-discipline of political science, EU studies. The sub-discipline is dominated by a dispute that is not always explicitly stated, but concerns the ontological nature of its subject matter. Unlike the study of a mature political system, the ontological status of the EU is far from settled and this has profound implications for our empirical understanding of the EU as a polity. Moreover, it generates one of the major tensions in EU studies: How are we to empirically study the EU political system? For many justifiable reasons the EU has traditionally been studied in

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

a *sui generis* manner, as if it were a unique case of political integration. This has generated numerous novel insights on the particularities of the EU political system. However, it has also produced a tendency for scholars to study their subject matter in isolation from some of the wider concerns and debates in the discipline. Over time this can take the form of ever more sophisticated and new conceptualisations of unique governance or integration dynamics within the EU, or 'thick' descriptions of how a particular event or policy has been crafted in the corridors of Brussels. An alternative is to view the EU as a functioning political system that may have certain unique features, but can still be profitably compared to other political systems.

The dualism noted above is one of the major fault-lines in EU studies. Indeed, it is greater than the methodological disputes in EU studies concerning different techniques (qualitative case study methods, formal rational choice models, discourse analysis techniques etc). The latter simply mirror debates within the discipline as a whole, whereas the former is unique to EU studies. Therefore, one of the principal aims of this dissertation is to investigate the explanatory potential of the second strategy: that is to view the EU as a functioning political system which invites comparison with other political systems. Yet, in order to do this I have preferred to study, not just the political dynamics in areas which invite comparison, but to also look at those 'more difficult' or 'least likely' areas. This should provide a better test for the comparative strategy. The underlying logic is that, if even seemingly unique areas of EU governance need not be studied in comparative isolation, then the theoretical value of adopting the comparative strategy ought to become even more compelling.

Throughout, the guiding principle of this dissertation is to draw on theoretical insights from the wider political science literature on comparative politics, and especially that of comparative federalism. To this end, this dissertation asks how federal political institutions matter. Although EU studies has for a long time debated whether federal-type political institutions exist, the argument put forward in this dissertation is that it is promising to ask, not just whether the latter exist and can be compared, but to take the next logical research step

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

and ask *how* they matter. By directing our attention to *how* EU federal political institutions matter, across a number of dimensions and issue areas, our ability to identify purported causal mechanisms affecting policy outcomes is potentially enhanced. And, as a result, our hypotheses about the specific effects of EU federal political institutions may be more amenable to further empirical testing through explicit comparison with other federal polities. Using insights from comparative federalism I proceed to develop conceptual model which allows for a structured and focused comparison of how federal political institutions are activated in response to a particular policy challenge. Two guiding hypotheses are formulated as to how basic federal political institutions shape the development of policy outcomes in the three polities under investigation. First, given the cross-border nature of the policy challenge, it is expected that similar *vertical* interactions among the different levels of government in the three polities under investigation will be generated. In particular, federal level political actors should be similarly mobilised into offering centralising solutions to problems with cross-border effects in the three units of analysis. Over time this can provoke allocational shifts in authority towards the centre. Second, it is hypothesised that differences in the way in which political inputs are processed in the three polities –in particular the decision-making process and modes of policy implementation– affect the 'power capabilities' of the centre and help to explain the variance in policy outcomes.

One of the central goals of this dissertation is to investigate whether the dynamics of EU policymaking exhibit similarities that make comparison of the EU with other federal polities inviting. One of the main conclusions drawn is that this is especially the case when comparing the EU with polities characterised by an extremely decentralised federal configuration, institutionally weak centres, consensual modes of decision-making and decentralised modes of policy implementation. The major implication of this claim for the study of EU politics is that the second strategy, the explicit comparison of the EU with other political systems, may shed greater explanatory light than the development of *sui generis* theories of the EU political system. Furthermore, it is possible that by following the comparative

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

strategy, the study of the EU may even serve to enrich the broader discipline itself, especially that of comparative federalism.

To achieve its research goals, the dissertation is divided into three main sections:

Part 1, 'Theory and Design', consists of two chapters. The first, chapter 2, critically reviews the state-of-the art in the field of comparative federalism and, in particular, its somewhat uneasy relationship with EU studies. The chapter demonstrates how developments in the broader field of comparative federalism have impacted on how those theories are subsequently applied to the EU. Furthermore, it contrasts an explicit comparative federalism approach to the EU with some of the dominant approaches in the EU studies literature. One of the major differences noted between the competing approaches is that a comparative federalism understanding of the EU is less concerned with identifying 'unique' insights than it is with pointing to 'comparative' insights. In chapter 3, the explicit focus is on questions related to research design and case selection. It begins by establishing a broad area of homogeneity among federal systems. By systematically highlighting similarities and differences among federal systems the chapter proceeds to narrow the federal sample to a limited universe of three cases which conform to a so-called 'compound polity' conceptualisation. The discussion in chapter 3 is mostly devoted to the purported effects of federal political institutions, i.e. the independent variable, in shaping policy outcomes. This forms the basis for generating two guiding hypotheses to structure the empirical investigation. Thus, the research design employed in this dissertation is in line with the comparative federalism literature where federalism is used as an independent variable to explain political outcomes.

Part 2 constitutes the empirical section. It begins in Chapter 4 by focusing on the regulatory challenge that is the subject of the empirical investigation. It offers a theoretically guided analysis of how and why the internet's politicisation has taken the form it has, the policy implications that flow from its developmental trajectory, and the considerable constraints it imposes on

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

policymakers in the three units of analysis. Broadly speaking, the regulatory challenge is analytically similar and can therefore be viewed as a parameter that affects the three polities in an analogous way.

Chapters, 5, 6 and 7, constitute the in-depth case studies. The chapters are organised thematically and focus on three distinct but overlapping internet-related issue areas: data privacy, copyright and cybercrime. Chapter 8 provides a cross-polity comparative review of the major findings and revisits the guiding hypotheses. It analyses the political dynamics involved and the specific policy regimes that have emerged in the three compound polities.

The concluding chapter brings the discussion firmly back to the EU. It reviews some of the insights that comparative federalism, as a distinct method for analysing the EU's political system, can bring to the wider EU studies literature. It also focuses on the institutional contours of a so-called ‘compound polity’ and how it can be applied to the EU.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Part I Theory and Design

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 2 Comparative Federalism meets the EU: Problems and Prospects

The aim of this chapter is to critically asses the literature on comparative federalism with a view to evaluating its application to the field of EU studies. Definitional and taxonomic disputes concerning the concept of federalism are first identified. This is followed by a section on the state-of-the-art in the broader field of comparative federalism and how those theories are subsequently applied to the EU case. Based on the insights gained, these approaches are contrasted with some of the more traditional approaches to EU studies, especially when conducting policy analyses. In the concluding section, an operational definition of comparative federalism and its application to the EU is offered.

1. Definitions and Taxonomies of Federalism

Federalism was famously described by one of its most prominent scholars, William Riker, as a theory of government that uses a system of checks and balances to curb power and offers an alternative to empire.[1] If it were that simple, it would be possible to circumvent the endless definitional and taxonomic disputes the concept of federalism has given rise to. But this appears not to be the case. The key to Riker's above understanding of federalism is that there are two sets of government, one of the federation and one of the member units, and that each has authority to make at least one decision independently of the other. Indeed, this creative tension, to the extent that it is kept in check, could sustain cooperative arrangements thereby avoiding empire altogether. Building on these insights, Andreas Follesdal offers a useful working definition which will be followed in this dissertation.[2] According to Føllesdal, a federal arrangement refers to a political order where 'final authority is divided between sub-units and a center' and in which 'sovereignty is constitutionally split between at least two territorial levels so that units at each level have final authority and can act independently of the

[1] See Riker, W.H. (1964a), *Federalism: Origins, Operation, Significance*. Boston: Little, Brown.

[2] Definition found in Føllesdal, A. (2003), "Federalism", The Stanford Encyclopedia of Philosophy (Winter 2003 Edition), Edward N. Zalta (ed.), URL http://plato.stanford.edu/archives/win2003/entries/federalism/

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

others in some area.'[3] Countless other definitions could be offered. Mainly because of this, it is difficult not to agree with Fillipov et al who argue that despite decades of research and considerable intellectual energies dedicated to studying federalism's properties, a universally agreed upon definition of federalism still eludes us and is likely to continue to do so.[4] Another controversial point, especially when the EU is brought into the federal equation, concerns federalism and statehood. But, as one eminent scholar of federalism has argued, a federal arrangement need not be coupled with notions of statehood.[5] One of the central arguments of this dissertation –and this chapter in particular- is that by adopting a more relaxed taxonomic attitude to the EU and its federal architecture, it is possible to focus on federalism as a dynamic process characterised by a continuous ebb and flow of authority among various levels of public authority that typically generates high levels of 'constitutional politics' over the appropriate vertical allocation of authority.[6]

If definitions of federalism are problematic, then so too are the taxonomic pathologies that afflict the concept of federalism. As Forsyth has noted, federalism is a pervasive concept that, with sufficient effort, can be detected almost everywhere.[7] Because of this, much intellectual effort has been expended on trying to achieve a taxonomic consensus on what constitute federalism's defining features. Elazar has offered a useful distinction, based on a biological analogy, according to which federalism is considered a genus of political organization that contains various species.[8] However, this has not

[3] Ibid., 1.

[4] See Filippov, M., Ordeshook, P.C., and Shvetsova, O. (2004), *Designing Federalism: A Theory of Self-Sustainable Federal Institutions*, Cambridge: Cambridge University Press.

[5] On this point, see Elazar, D. J. (1987), *Exploring Federalism*, Tuscaloosa: University of Alabama Press; For an overview on this point see Börzel, T. and Hosli, M. (2003), Brussels between Bern and Berlin: Comparative federalism meets the European Union, *Governance* 16:2, pp. 179-202.

[6] Some authors who have given a similar consideration of federalism are: Bermann, G. A. and Nicolaidis, K. (2001), Basic Principles for the Allocation of Competence in the United States and the European Union in Nicolaidis, K. and Howse, R., eds. (2001) *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press; Donahue John D, Pollack Mark A. (2001), Centralization and Its Discontents: The Rhythms of Federalism in the United States and the European Union in Nicolaidis and Howse (2001); Follesdal (2003); Filipov et al (2004).

[7] Forsyth, M. (1981) *Unions of States: The Theory and Practice of Confederation*. Leicester: Leicester University Press.

[8] In Elazar (1987): 6.

DOI: 10.2870/1208

satisfied some scholars who have felt the need to further distinguish between federalism as a normative or philosophical concept and its usefulness as an empirical descriptive term. Thus, Watts has urged scholars to use the term 'federal political systems' to refer to the 'genus of political organization that is marked by the combination of shared rule and self-rule'.[9] Other scholars have employed the term 'federal arrangement'[10] or 'federal polity.'[11] In this dissertation I will use the terms 'federal political system', 'federal arrangement' and 'federal polity' interchangeably to refer to the genus of political organization as identified by Elazar. Having described the genus we may proceed to identify several species of federal political systems. Elazar identified a continuum ranging from federations through to loose confederations. Within this continuum a number of species could be identified including federation, union, federacy, condominium and leagues.[12] Without downplaying the importance of Elazar's taxonomic efforts, we may presently limit ourselves to just two species: federations and confederations.

Follesdal's encyclopaedia entry on 'federalism' provides a useful starting point for discussing the two species, especially when applied to the EU.[13] The basic distinguishing feature between a confederation and a federation concerns the powers of the centre, one of the central themes in this dissertation. Typically confederations tend to have weaker centres. According to Follesdal, a confederation is characterised by the following features: 'a) sub-units may legally exit, b) the center only exercises authority delegated by sub-units, c) the center is subject to sub-unit veto on many issues, d) center decisions only bind sub-units but not citizens directly, e) the center lacks an independent fiscal or electoral base, *and/or* f) the sub-units do not cede authority permanently to the center'.[14] Yet Follesdal admits that the EU possesses many features that are at variance with a confederation.[15] In the realm of

[9] See p. 120 in Watts, R. (1988) Federalism, Federal Political Systems, and Federations, *Annual Review of Political Science*, Vol. 1, pp.117-137
[10] For example, Follesdal (2003).
[11] Gross, G. M (1996) Spinoza, and the Federal Polity. *Publius*. 26:1 pp117-135
[12] In Elazar (1987).
[13] Follesdal (2003).
[14] Ibid.
[15] Ibid.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

market regulation the EU functions like a fully fledged federation, while qualified majority voting ensures that in many areas member states can, and are, outvoted. Moreover, European legislation has direct effect on EU citizens, whom in turn, directly elect MEPs.

The field of comparative federalism, however, is more than just concerned with distinguishing between certain structural or basic institutional configurations. The problem is that this appears to be producing certain perverse effects. As Von Beyme has noted, every year new 'epitheta-federalisms' appear purporting to capture new elements of the genus we call federalism.[16] The list below, which could be considerably extended, gives an indication of the terminological proliferation that has gripped the field: cooperative federalism, competitive federalism, dual federalism, legislative federalism, executive federalism, administrative federalism, interlocking federalism, centralised federalism, coercive federalism, regulatory federalism, juridical federalism, structural federalism, market preserving federalism, devolutionary federalism and asymmetric federalism. The concept of 'epitheta-federalisms' is a useful one for drawing attention to a problem in the field. To illustrate this we may begin with a classic distinction between *dual* federalism and *cooperative* federalism. Both *epithets* aim to classify varieties of federations, i.e. to point to differences among federal states. For instance the epithet, *dual federalism*, has a particularly long pedigree and has been traced back to Hamilton,[17] A.V. Dicey and K.C Wheare.[18] It is used to denote a federal state in which there is a clear separation of powers. Two levels of authority exist, the federal and the state level, each with its well defined responsibilities and operating with a significant degree of independence. According to Boerzel and Hosli, in this model the 'entire government machinery tends to duplicated, as each level manages its own affairs autonomously'.[19] Classic examples of dual federalism include the US and Canada. *Cooperative federalism*, on the other hand, is an epithet-federalism

[16] von Beyme, K. (2005), Asymmetric Federalism between globalization and regionalization, *Journal of European Public Policy* 12:3, pp. 432-447.

[17] Zimmerman, J.F. (2001). National-state relations: Cooperative federalism in the twentieth century. *Publius: The Journal of Federalism*, 31(2), pp.15-30

[18] See Watts (1988).

[19] In Börzel and Hosli (2003), 183.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

usually employed to denote federal states in which powers are functionally divided between territorial levels. In this subspecies of federation, the central level makes the laws while the subunits are responsible for implementation. Germany is usually offered as a paradigmatic case.

This distinction has been commonly used to demonstrate purported differences in performance, or policy outcomes. Yet it is puzzling a distinction. For a start, the concept of 'cooperative federalism' was originally applied to the US in the 1960s by Elazar, although, depending on the author, the current literature largely refers to the US as a case of 'dual federalism' and not 'cooperative federalism'. Switzerland is an even more problematic case, frequently classified as both dual federalism[20] and cooperative federalism.[21] The distinction between 1) certain *structural* properties concerning the relative autonomy of two levels of government, which underpins the concept of dual federalism and 2) what could be considered as the *process* properties of cooperative federalism, which refer to the complex and pluralistic relationship of sharing and mutuality across levels of government in policy making, have generated taxonomic pathologies. The two elements have been frequently conflated in the literature and have resulted in numerous misapplications of epithets.

The major problem with epitheta-federalisms is that they are originally coined to identify specific structural or political process features of federations, but then indiscriminately applied to different levels or domains. They have become redundant catch-all categories devoid of their original meaning and, despite the heroic taxonomic efforts of scholars, no consensus appears to be forthcoming on the use of epitheta-federalisms. It is not necessarily just the sheer terminological proliferation that is problematic, since this could be justified in terms of new insights gained and would only require keeping abreast of innovations. The problem is that the new terms are used in an inconsistent way. Furthermore, the problem is compounded when epitheta-

[20] Ibid.

[21] Linder, W. and Vatter, A. (2001), Institutions and outcomes of Swiss federalism: The role of cantons in Swiss politics, *West European Politics* 24:2 95-121.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

federalisms are applied to the EU. Thus for some analysts the EU possesses features of cooperative federalism,[22] interlocking federalism[23] executive federalism,[24] regulatory federalism[25] and the list could be extended. Perhaps in recognition of these difficulties, McKay's comprehensive comparative federalism approach to the EU has conspicuously avoided epitheta-federalisms altogether.[26] This is not to in any way downplay the constructive insights offered by the above scholars, most of whom make the argument that the EU appears to be moving in the direction of this or that model, but rather to underscore that, in the absence of a general consensus on the meaning and application of epitheta-federalisms, it may be more prudent to avoid them. This applies with extra force where the EU is concerned.

2. State-of-the-Art

As noted above, the field of comparative federalism is more than simply concerned with identifying taxonomic distinctions among federal political systems. In this section I will provide a brief overview of the broader literature with a view to showing how a comparative federalism lens has been applied to to the EU. Contrary to the claim or rhetoric of many authors who, in applying a comparative federalism lens to the EU, imply that such an approach is novel, the argument put forward below is that the study of European integration using insights from federalism has a longer history than is commonly acknowledged. Though, to be fair, federalism has never quite acquired the status of a 'dominant paradigm'. Three strands of the comparative federalism literature are identified below that, in one way or another, have influenced the study of the EU. This is not to suggest that these are the only approaches, but rather that they are the most pertinent to this

[22] See Börzel and Hosli (2003).

[23] See Abromeit, H. (2002), Contours of a European Federation *Regional and Federal Studies*, 12:1, pp.1-20 and see also Scharpf, F.W. (1988), The joint-decision trap: Lessons from German federalism and European integration, *Public Administration* 66, pp. 239-278.

[24] Dann, P. (2003), The European Parliament and Executive Federalism: Approaching a parliament in a semi-parliamentary democracy, *European Law Journal* 9:5 (December), p. 549-574.

[25] See Kelemen, D. (2002), Regulatory Federalism: EU environmental regulation in comparative perspective. *Journal of Public Policy*; 20(3): 133-167.

[26] McKay, D. (2001), Designing Europe: Comparative Lessons from the Federal Experience, Oxford: Oxford University Press. See also McKay, D (1999), *Federalism and European Union: A Political Economy Perspective*. Oxford: Oxford University Press

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

dissertation's theoretical and empirical goals. I provide a brief overview of each approach below.

1) Normative theories of federalism: Whether explicitly stated or not, the term federalism, as with other *ism's* (e.g. socialism, liberalism, anarchism), has a certain ideological or normative component involving the *advocacy* of federal principles. Forsyth[27] identifies a number of strands beginning with Kant's moral theory of an ever-expanding federation between states contained in his essay on *Perpetual Peace*. A second stream he connects to certain participatory variants as expounded by thinkers such as Rousseau and Proudhon, and which, incidentally, include advocates of the Catholic doctrine of subsidiarity. Finally, according to Forsyth,[28] the classical tradition can be said to have commenced with the publication of a series of articles by Madison, Hamilton and Jay known as the *Federalist Papers*. The importance of the latter is to be found in its advocacy of federalism as a pragmatic mechanism for splitting sovereignty between two territorial levels, the subunits and a centre, which would keep each other in check, thus protecting the rights of the individual from abuse by authorities at either level.[29] According to the above schema, it is possible to contrast two variants of federal thought: a more philosophically oriented European tradition of federalism which incorporates the concept of subsidiarity as a principle for allocating functions, and a North American variant focusing on the pragmatic balancing of citizen's preferences.[30] One of the distinguishing features of the classical approaches is their normative component - the overt *advocacy* of federalism as a form of political organisation.

Normative theories of federalism have also been applied to the European integration process well before its institutional configuration took the format we recognise today. Indeed, over the past two centuries a long list of eminent European thinkers have advocated the application of the federalist principle at

[27] Forsyth, M (1996). 'The Political Theory of Federalism: The Relevance of Classical Approaches' in Joachim Jens Hesse and Vincent Wright (eds), *Federalizing Europe: The Costs, Benefits and Preconditions of Federal Political Systems*. Oxford: Oxford University Press.
[28] Ibid.
[29] See Follesdal (2003).
[30] On this point, see Watts (1988).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

a pan-European level. At the risk of simplifying, it is possible to distinguish between at least two types of normative theories of federalism that are pertinent to the present process of European integration. The first strand can be traced back to the aftermath of the Second World War when federalist solutions calling for an all embracing Federation in Europe were frequently expressed by individuals such as Altiero Spinelli and Ernesto Rossi (e.g. the Ventotene Manifesto). These proposals drew heavily on classical federalist doctrine for their inspiration and were overtly ideological.[31] A second strand, generally much less ideological, has emerged more recently. Examples include Forsyth,[32] who uses classical federal political theory to argue that the current approach to European integration shows serious limitations which 'a more explicit and determined recourse to federal-constitutional principles could help to rectify'. In a more philosophical vein, the recent work of Follesdal[33] draws on Madisonian insights to stress the need for generating a sense of justice among Europeans and sets out the conditions most likely to facilitate trust and trustworthiness in a federal European political order.

2) Covenantal theories of federalism: As one of the distinguishing features of a federal polity, covenantal approaches emphasise the voluntary yet contractual coming together of equal partners in the creation of a new body politic. However, unlike unitary states, where the contract is between individual leaders, a federal covenant involves a contract between otherwise independent sovereign states. The resulting covenant is therefore based on a special partnership: one that involves a 'special kind of sharing that must prevail among the partners, based on a mutual recognition of the integrity of each partner and the attempt to foster a special unity among them.'[34] According to Elazar, the foremost contemporary exponent of the covenantal approach to federalism, the key to understanding federalism is the combination of *self-rule* and *shared rule.* He argues that federalism thus understood, involves a contractual linkage that provides for elements of power

[31] For a review see O'Neil, M. (1996), *The politics of European integration: A reader*, London: Routledge.

[32] Forsyth (1996), pp25-26.

[33] Follesdal, A. (2005), Towards a stable *finalité* with federal features? The balancing acts of the Constitutional Treaty for Europe, *Journal of European Public Policy* 12:3 (June), pp. 572-589.

[34] Elazar (1987), pp5.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

sharing, cuts around the thorny issue of sovereignty and, most importantly, supplements rather than seeks to replace prior organic ties.[35] A key concept that emerges from a covenantal approach is the distinction between decentralisation and non-centralisation. The former implies the existence of a central authority, which can decentralize or recentralize at will and, in which, 'the diffusion of power is a matter of grace, not right.'[36] On the other hand, in Elazar's non-centralised polity, power is so diffused that it cannot be legitimately centralized or concentrated without breaking the spirit of the constitution. This last point, concerning the spirit of the constitution, is crucial to the covenantal conceptualisation of federalism. To the extent that polities are founded on federal covenants, the latter will obviously reflect important questions of constitutional design. Indeed, for Wheare,[37] who shares with Elazar a cooperative understanding of federalism, both the *supremacy* of the constitution and its *written* form are essential institutions if government is to be deemed federal. In sum, the key to covenantal approaches to federalism is *cooperation*.

Covenantal inspired approaches have been fruitfully applied to the EU's federal arrangement. They tend to emphasise the covenant or cooperative arrangement that underpins the EU. In many respects, they can be considered as the 'good story' of EU federalism. Questions of constitutional design and institutional configuration tend to be paramount in this school. Not surprisingly, some of the earliest approaches were provided by legal scholars when describing the contours of the emerging European constitutional order. Stein[38] was one of the first legal scholars to analyse its federal architecture and especially how the ECJ 'has fashioned a constitutional framework for a federal-type structure in Europe.' A seminal contribution by Cappelletti, Secombe and Weiler[39] drew attention to similarities in the judicial activism of the ECJ with that of the US Supreme Court. Since then, it is fair to say, that a federal understanding of the EU constitutional order underpins most EU legal

[35] Ibid.
[36] Ibid. pp8 .
[37] Wheare, K.C. (1967), *Federal Government (4th edition)*, London: Oxford University Press.
[38] Stein, E. (1981), Lawyers, Judges, and the Making of a Transnational Constitution, *American Journal of International Law* 75, p. 1-27.
[39] See Cappelletti, Secombe and Weiler (1986).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

studies. As Auer[40] has noted, the EU presently fulfils the criteria of federalism through a combination of self-rule and shared-rule while its constitutional architecture accomplishes specific functions, such as distributing powers between the centre and the sub-units and providing for a conflict resolution scheme.[41]

In line with the focus of covenantal approaches on institutional design and cooperative engagement among political actors, political scientists such as Burgess[42] have drawn attention to the institutional framework and policymaking processes 'as sites for federalist influences to act upon national and supranational elites, as well as mass publics, in a significant way'. Other efforts have suggested a case for neo-federalism to account for the federalising process taking shape in the mid-1980s.[43] More recent approaches in the literature emphasise that the EU seems to be moving in the German direction of cooperative federalism[44] or, to use an alternative epithet, interlocking federalism.[45] Some have noted parallels with Swiss institutional trajectories, especially in regard to the increasing use of, and potential for, EU-related referendums.[46] Others prefer the US benchmark, where 'notions of 'cooperative federalism' in the US context and 'pooling of sovereignty' in the EU context have been applied to capture the [same] phenomenon.'[47] What seems to link this, admittedly, broad church is a focus on constitutional design and formal institutional structures on the one hand, and, the need for cooperative engagement among the different levels of government on the other.

[40] See Auer (2005a).

[41] Other recent contributions by constitutional lawyers have, somewhat haphazardly, drawn insights from the comparative federalism literature in political science to argue that the basic structure of the EU corresponds to that of executive federalism and that, on this basis, calls for strengthening the Parliament's role in the election of the EU's executive would break the existing covenantal spirit (Dann 2003).

[42] Burgess, M. (1989), *Federalism and European Union*, London: Routledge.

[43] For example, Pinder (1986).

[44] See Börzel and Hosli (2003).

[45] In Abromeit (2002).

[46] See Trechsel (2005); and Papadopoulos, Y. (2005), Implementing (and radicalizing) art. I-47.4 of the Constitution: is the addition of some (semi-)direct democracy to the nascent consociational European federation just Swiss folklore?, *Journal of European Public Policy* 12(3): 448–467.

[47] Nicolaidis and Howse (2001).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

3) Rationalist theories of federalism: The rationalist[48] inspired theories of federalism reject the so-called 'good story' of federalism based on consensus and cooperation that appears to unite covenantal approaches. While acknowledging the importance of constitutional design, scholars have cautioned against taking this 'to mean that the mere act of drafting an appropriate constitutional contract is sufficient for viable federalism.'[49] Those working within this rationalist paradigm are critical of giving too much weight to constitutional provisions and too little weight to ancillary institutions, such as the party system.[50] This approach to comparative federalism has acquired growing importance recently and although the 'rationalist' label could also be applied to economic inspired federalism approaches,[51] it differs from the latter in that it is less concerned with the specific socio-economic conditions for federalism and places, instead, an emphasis on federalism understood as a process of bargaining among political actors. Rather than offering a 'good story' of federalism, rationalist theories of federalism take seriously the words of Thomas Hobbes for whom 'Covenants without the sword are but words, and of no strength to secure man at all.'[52] The intellectual godfather of this approach to federalism is William Riker, both in terms of his contribution to the field of comparative federalism in particular, but also, more generally, for his role in introducing methodological individualism to the discipline of political science. Two versions of the rationalist school can be identified, Riker's original contribution and a more recent strand.

In 1964 Riker published his seminal article taking issue with much of the existing literature on federalism, which he considered to be ideological and of

[48] The term 'rationalist' is used by Kelemen, for instance, while an alternative description could be methodological individualism as used by Filipov. See Kelemen, D. (2003). The Structure and Dynamics of EU Federalism, *Comparative Political Studies*, 36: 1/2 pp184-208; Filippov, M. (2005) Riker and Federalism, Constitutional Political Economy, 16, pp93-111.

[49] See Filippov et al (2004)

[50] Ibid.

[51] For an example of economic inspired theories see especially Buchanan, J. (1995). Federalism as an ideal political order and an objective for constitutional reform. *Publius* 25:2 (Spring), pp. 19-27. Weingast, B R. (1995). The economic role of political institutions: Market-preserving federalism and economic growth. *Journal of Law, Economics, and Organization* 11, 1-31.

[52] P. 196 in Hobbes, T. (1968), *Leviathan*, edited by C.B. MacPherson, New York: Penguin Classics.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

dubious scientific worth.[53] In critiquing the literature Riker purported to offer a general theory of the origins and sustainability of federalism based on a theory of bargaining among political elites. In surveying all instances of the creation of federations since 1786, Riker concluded that he could empirically demonstrate that the primary motive for political integration is the existence of a real or perceived military threat.[54] Historically then, the existence of a military threat has been the single most powerful explanation of why political leaders have adopted a rational bargain to create a federation. Unfortunately, much of the subsequent criticism of Riker's theory has focused disproportionately on the so-called military threat hypothesis which, according to his defenders, has to be seen in the context of a field that was dominated by a focus on abstract interactions between collectivities such as nations, peoples or social and economic preconditions.[55] Riker, in many ways, shattered this understanding by putting rational politicians, engaged in strategic interactions at the heart of the analysis. Thus, in Riker's theory the central focus is on how institutions shape political conflict and create incentives for political elites to either support or reject federalism. Rational human calculation is the mechanism by which federations are successfully created and maintained. Once created, it is the institutionally derived motives of political elites that help to sustain federation. For Riker, among the most crucial institutional variables are the constitutional architecture and the nature of the party system. Indeed, the latter may be regarded as the main variable intervening between background social conditions and the specific nature of federalism. Recent attempts at a general theory of federalism have built on, and modified, Rikerian insight in at least two ways.

First, they have been less concerned with explaining the origins of federalism and have relaxed the Rikerian military hypothesis. In particular, they have modified the military threat and reconceptualised it more broadly to refer to strong external pressures.[56] Thus, external threats of an economic or cultural

[53] See McKay, D (2004). William Riker on federalism: sometimes wrong but more right than anyone else? Regional and Federal Studies, 14: 2, pp.167-186.
[54] See Riker (1964a).
[55] See in particular Filippov, M. (2005)
[56] See in particular, McKay (1999)

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

nature can induce analytically similar responses to the military threat. The crucial point is that in the typical and frequent conflicts over the appropriate locus of political authority generated in federal polities, sub-unit political elites are only likely to accept a loss of competencies in a given area when they are compelled to do so by a strong external pressure or threat.[57] In fact, this is a modification that Riker himself seemed to acknowledge in one of his last essays on the possibilities of a so-called trade motive for federalisation. [58]

Second, since Riker's seminal contribution formal methods, such as game theory, have been increasingly applied to analyse the way in which the institutional architecture structures the federal game played by political actors. Filippov et al[59] have advanced the Riker framework, especially with regard to the role of the party system, to offer a theory of the self-sustainability of federal institutions, while Bednar[60] explains 'authority migration' among levels of government using a similar game theoretic framework.

Rather than focusing on the positive aspects of either *cooperation* or *economic competition,* as the other federalism approaches do, the rationalist school is principally concerned with the institutionally generated incentives, e.g. through constitutional provisions or ancillary institutions such as the party system, which define the way in which the federal game is played by political actors. The federal game can be expressed succinctly: how to stop central government from overwhelming the sub-units on the one hand and, on the other, how to prevent the sub-units from taking advantage of each other and failing to cooperate thereby undermining the very stability of the federation. Naturally, this type of reductionist ontology can lend itself to formal modelling and the use of game theoretic techniques. In sum, *bargaining* is the key to this approach.

[57] See Filippov (2005).

[58] See Riker, W.H. (1996), 'European Federation: Lessons of Past Experience', in Hesse, J.J. and Wright, V. (1996).

[59] Filippov *et al* (2004).

[60] Bednar, J. (2004), Authority migration in federations: A framework for analysis, *PS: Political Science and Politics* 37, 403-408.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

As in the general comparative federalism literature, *rationalist federalism approaches* to the EU have also acquired a growing importance of late. They purport to offer a powerful theory, which is largely based on new institutionalist insights. Three influential approaches to this more 'selfish story' of bargaining in EU federalism will be singled out. One of the earliest, and most penetrating, rationalist analyses was offered in Scharpf's influential 'joint decision trap' theory. Unlike earlier comparative federalism approaches to the EU, Scharpf's contribution was analytically sophisticated rather than overtly prescriptive. He first distinguished between the US variant of federalism and the -at the time- West German model of federalism. Critical of Anglo-American approaches to federalism,[61] which operate according to a zero-sum logic, i.e. either one level of government or the other, Scharpf argued that such conceptualisations failed to take account of other models of federation.[62] The German variant (as does the Swiss) consist of overlapping jurisdictions, or what Scharpf calls '*Politikverflechtung*'. Second, these joint arrangements are predisposed to decision traps and policy pathologies. His major contribution is in applying these comparative federalism insights from the German case, to the EU's version of '*Politikverflechtung*'. It is rationalist to the extent that it focuses on the decisional dynamics within the EU which produce outcomes that tend to be inherently suboptimal but, nonetheless, 'represents a 'local optimum' in the cost-benefit calculations of all participants that might have the power to change it.'[63] He also offers a rationalist understanding of the sustainability of the EU polity, in terms of concentrating net contributions on those member states which would have most to lose economically and politically from the dissolution of the internal market.

More recently, and by far the most comprehensive application of rationalist theories of federalism to the EU, is the work of Mckay.[64] McKay has consciously adapted Riker's rationalist theory of the origins and viability of federations to explain the EU case. In doing so, however, he has relaxed

[61] For example, see Riker (1964a).

[62] Scharpf (1988). See also Scharpf (2001), European Governance: Common Concern vs the Challenge of Diversity. *Jean Monet Working Papers*. No. 6/01 Symposium: The Commission White Paper on Governance.

[63] Scharpf (1988).

[64] See especially Mckay (1999) and McKay (2001).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Riker's problematic military threat hypothesis since 'there is no reason why averting economic or cultural threats should not be part of framers' original bargaining calculus.'[65] Indeed, in a posthumously published essay Riker[66] addresses the 'trade motive', as he calls it, but reaches ambivalent conclusions as to its importance for the EU case. Nonetheless, according to McKay, Riker still offers, more than forty years on, the most powerful theory on the origins of federal states.[67] McKay's contribution is in systematically applying Riker's insights to the EU case in terms of both explaining its origins and its sustainability. His core Rikerian assumption is 'that politicians do not cede authority over crucial aspects of domestic policy (or give up some part of their power resources) voluntarily unless they believe that the benefits of doing so exceed the costs.'[68] In the first of two influential monographs he takes issue with the *sui generis* nature of much current theorising on the EU and provides a compelling explanation for the origins of the EU and the adoption of EMU, which are both conceived as the outcome of a rational federal bargain.[69] A second monograph[70] places the EU in a historical comparative context by comparing its origins, constitutional design and institutional development with five other federations: Australia, Canada, Germany, Switzerland and the US. In concluding this work, McKay argues that although the EU has much to learn from all five federations mentioned above, 'perhaps most can be learnt from the very decentralized institutions of the Swiss confederation.'[71]

A third rationalist approach is Filippov et al's[72] application of their general theory of the self-enforceability of federal institutions to the EU case. Their institutional analysis is predominantly focused on the role of parties and the problems surrounding the emerging pan-European party system. Although penetrating, and offering useful insights as to the future sustainability of EU

[65] McKay (2001), 8.
[66] Riker (1996).
[67] McKay, D (2004) William Riker on federalism: sometimes wrong but more right than anyone else? *Regional and Federal Studies*, 14: 2, pp.167-186
[68] McKay (1999), pp4.
[69] McKay (1999).
[70] McKay (2001).
[71] See especially pp153 in McKay (2001)
[72] Filippov et al. (2004).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

institutions, their contribution is more of an addendum to their general theory rather than a systematic account on the EU in the style of McKay. One could also mention the more narrowly focused rationalist comparative federalism approaches that have been applied to particular EU policymaking areas such as the environment.[73] These will be dealt with in more detail in the following section however.

In concluding this section, it should be noted that the comparative federalism literature is considerably more extensive than this brief survey has suggested. The main concern, though, has not been to offer an exhaustive review of the literature, but rather to bring out some of the major bones of intellectual contention among the competing federalist paradigms, especially in the context of their application to the EU case. Furthermore, it should be clear that although the federalism lens has been applied to the EU since the 1950s,[74] and especially following the Single European Act,[75] the Maastricht Treaty, and of late with European constitutional process,[76] over recent years a growing sophistication in the literature can be detected, both in terms of how theories are applied and the methods used. Of the three approaches identified, much attention has been focused on the third approach, the so-called rationalist inspired theories of comparative federalism. There are very good reasons for this bias since these approaches appear to be more suited to studying the bargaining and political conflict that surrounds policy-making. To the extent that this is the case, the rationalist theories of federalism are more relevant for deriving hypotheses, especially with regard to the strategic interactions and conflict over the allocation of political authority among levels of government around particular policy domains –i.e. the core empirical focus of this dissertation.

[73] See for example Kelemen (2002).
[74] See Forsyth, M (2000).
[75] Take, for example: Burgess, M., ed. (1986) *Federalism and Federation in Western Europe*, Croom Helm, USA Cambridge: Belknap Press; and Pinder, J. (1986), European Community and nation-state: a case for neo-federalism? *International Affairs*, Vol. 42:1, pp. 41-54.
[76] See Auer, A. (2005a), The constitutional scheme of federalism, *Journal of European Public Policy* 12:3 (June), 419-431; and see also Trechsel, A.H. (2005), How to federalize the European Union...And why bother, *Journal of European Public Policy* 12:3 (June), 401-418.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

3. The EU policy dimension

Having shown that comparative federalism approaches to the EU have a rather long pedigree in EU studies, we can now direct our attention to the policy dimension. This is especially important since the major theoretical and empirical objectives of this dissertation concern the effects of political institutions on policy outcomes. Although space constraints do not permit us to survey the ever-growing EU integration literature in depth,[77] some of the major schools that explicitly focus on the policy dimension will be identified and compared to comparative federalism approaches that have similar foci. Thus, the major goal of this section is to situate comparative federalism approaches to EU policymaking within a specific EU studies theoretical context.

In the recent history of European integration theorising a focus on the policy-making dimension of the EU appears to have been a necessary condition for theoretical advancement. For instance, an explicit focus on policymaking was an important element in overcoming some of the earlier controversies in European integration theorising, namely the longstanding dispute between state-centric paradigm (mostly referred to as intergovernmentalism) and a supranational paradigm (which came to be known as neo-functionalism).[78] Already in the late 1970s the purported shortcomings of American inspired state-centric and supranational paradigms had begun to give way to a wave of new approaches that sought a better empirical understanding of the link between national politics and EC policy-making. With its major focus on the nature of EC policy making, the Wallace et al 1977 volume marked an important milestone in this new line of empirical inquiry. Indeed, a few years after its publication William Wallace welcomed the collapse of integration theory and argued in favour of applying a federal analogy to EC politics since the latter 'is a profoundly political process, best understood in the familiar

[77] For comprehensive surveys on EU integrations theories see: Caporaso, J. and Keeler, J (1995) 'The European Union and Regional Integration Theory', in S. Mazey and C. Rhodes (eds.) The State of the European Union: Building a European Polity? Boulder: Lynne Rienner, pp. 29-62; O'Neil (1996); Rosamond, B. (2000), *Theories of European Integration*, Basingstoke: Macmillan; and Diez T. and Wiener A. (2004), *European Integration Theory*, Oxford: Oxford University Press.

[78] For a critical overview of the earlier debates, which tended to be inspired by international relations approaches, see in particular Hix, S. (1994), The study of the European Community: the challenge to comparative politics, *West European Politics* (1994).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

terms of political analysis, not in the arcane language of functionalism or the loose concept of regime theory'.[79] Legal scholars had, incidentally, reached very similar conclusions about the federal analogy.[80] More recently, a new wave of theorising has brought the policy dimension firmly to the forefront of EU integration theory and empirical focused policy analyses. These include the pervasive concept of multi-level governance, the Europeanization literature, and the policy modes inspired literature. I outline the basic elements of each of these approaches below and compare them to comparative federalism inspired policy analysis.

1) *Multi-Level Governance*: Initially introduced by Gary Marks, the concept of 'multi-level governance' (MLG) arose in great measure as a response to a frustration with the dualism in EU studies between international relations and comparative politics. According to Marks et al, the EU had created a situation where the separate existence of these two disciplines was increasingly problematic.[81] A new synthesis between what goes on inside a state and what goes on outside a state was called for.[82] Rather than seeking to explain the dynamics of European integration, the MLG model takes the EU polity as fixed and seeks to understand the nature of decision-making within the system. From the MLG perspective, the EU is viewed as a unique polycentric arena in which myriad actors, organised along non-hierarchical lines, intermesh to form a complex web of decision-making. It is crucial to note in the context of this dissertation's theoretical and empirical ambitions that the MLG model arose as a result of a single policy study. The concept was originally launched in a study of the 1988 landmark reforms of the Structural Funds and the consequences for policy implementation. The policy was viewed as 'the leading edge of a system of MLG in which supranational,

[79] See especially p. 57 in Wallace, W. (1982), Europe as a confederation: The community and the nation-state, *Journal of Common Market Studies* 21, pp. 57-68.

[80] Seminal articles in the field of EC legal studies were published most notably by Eric Stein and Joseph Weiler See Stein, E (1981) and Weiler, J.H.H. (1982), Community member states and European integration: Is the law relevant, *Journal of Common Market Studies* 22:1/2, pp. 39-56.

[81] Marks, G. Hooghe, L. and Blank, K. (1996a) 'European Integration from the 1980s: State-Centric V. Multilevel Governance', *Journal of Common Market Studies*, Vol. 34, No.3, pp343-378.

[82] Hurrel A and Menon A (1996) Politics like any other? Comparative politics, International relations and the study of the EU' *West European Politics*, Vol.19, No.2, pp386-402; see also the rejoinder by Hix S (1996) 'CP, IR and the EU! A rejoinder to Hurrell and Menon' *West European Politics*, Vol.19, No.4, pp802-4.

DOI: 10.2870/1208

national, regional and local governments are enmeshed in territorially overarching policy networks'.[83] In other words, Marks employed insights from the vertical intergovernmental relationships embodied in the implementation of one policy sector (EU Cohesion policy) to the general dynamics of the EU polity.[84] Thus, although not explicitly acknowledged in the literature, many of the supposed novelties and insights of the original formulation of MLG shares strong similarities with well-established and more theoretically refined literature on comparative federalism. In conceptual terms, one of the central propositions of the MLG model is that power is "shared" between actors at multiple levels of government, instead of monopolized by central governments.[85] As noted above, a similar understanding of federalism as a combination of 'self-rule' and 'shared rule' has a much longer tradition in the comparative federalism literature, most notably in the work of William Riker.[86] It could be argued that a comparative federalism approaches may therefore rests on stronger theoretical grounds due to the leverage gained from a long-standing tradition in seeking to explain both institutional design and evolution from an explicitly comparative perspective.

2) Europeanization: More recently, the concept of Europeanization has become an "extremely fashionable term" in the EU studies literature[87]. As with the MLG approach, the emergence of the concept is supposed to reflect a so-called "post-ontological" stage in EU theorising[88] in which the EU is taken as given and the analytical focus shifts to its impacts on the polities, politics and

[83] Marks, G. (1993) 'Structural Policy and Multilevel Governance in the EC'. In Cafruny, A.W. and Rosenthal, G.G. (eds.) *The State of the European Community.* Boulder: Lynne Rienner, p.401.

[84] It is worth stressing that to the extent that the EU polity was portrayed to be evolving towards a system of Multi-level governance, Marks considered Cohesion policy to be a reflection of this broader trend and not the cause. Other scholarly analyses of cohesions policy and the structural funds include Allen, D. (2005) 'Cohesion and Structural Funds: Competing Pressures for Reform?'. In Wallace, H. Wallace, W. and Pollack, M. (eds.) *Policy-Making in the European Union*, Fifth Edition (Oxford: Oxford University Press).

[85] Marks et al. (1996), p346.

[86] For a well-known theoretical article on power by Riker, although not explicitly applied in a comparative federalist perspective see: Riker W (1964b) 'Some ambiguities in the notion of power' *American Political Science Review*, 58:2, pp341-349.

[87] Olsen, J.P. (2003) 'Europeanization', in: Cini, M (ed) *European Union Politics*, (Oxford: Oxford University Press), p334.

[88] P. 30 in Caporaso, J. (1996) 'The European Union and Forms of State: Westphalian, Regulatory or Post-Modern?' *Journal of Common Market Studies*, Vol. 34, No. 1, pp. 29-52.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

policies of the Member States.[89] Theoretical and empirical research on Europeanization has advanced significantly since the late 1990's, providing new knowledge and greater understanding of the mechanisms and explanations of adaptation to EU pressures in the member states.[90] However, this research agenda remains somewhat plagued by a number of conceptual and methodological challenges, which can, in part at least, be addressed by integrating certain comparative insights. For instance, identifying and measuring the impact of the EU is the key methodological challenge confronting Europeanization research. Isolating domestic and global factors from European pressures is a difficult task given the close interaction and co-evolution of these separate but interrelated pressures.[91] Thus, by including non-EU cases such as the US and Switzerland within the universe of cases, a comparative federalism approach can enhance the development of causal inference by placing policy outcomes within a broader comparative context. Because of this, the concept of Europeanization is therefore dependent on other established theories within the wider discipline of political science. As with the MLG literature, we can also see clear evidence here of conceptual borrowing from comparative federalism as Europeanization theorists move down the ladder of meta-theoretical abstraction. This is most evident in relation to the central concern with domestic institutional structures in mediating the effects of Europeanization. For instance, Schmidt has borrowed from the federalism literature to explain differential impacts of the EU on member states.[92] It is also evident in the seminal volume by Risse et al, which borrows from the federalism literature to identify 'multiple veto points' (joint-

[89] Radaelli, C. (2000) 'Whither Europeanization? Concept Stretching and Substantive Change'. *European Integration Online Papers* Vol. 4 No. 8; Risse, T. Cowles, M. and Caporaso, J. (2001) 'Europeanization and Domestic Change: Introduction'. In Risse, T. Cowles, M. and Caporaso, J. (eds.) *Transforming Europe. Europeanization and Domestic Change* (Ithaca: Cornell University Press).

[90] Featherstone, K. and Radaelli, C. (2003) 'A Conversant Research Agenda'. In Featherstone, K. and Radaelli, C. (eds.) *The Politics of Europeanization*. Oxford: Oxford University Press; Radaelli C (2004) 'Europeanisation: Solution or problem?' *European Integration online Papers* Vol. 8 , N° 16: http://eiop.or.at/eiop/texte/2004-016a.htm

[91] Wallace, H. (2000), Europeanisation and Globalisation: Complimentary or Contradictory Trends? *New Political Economy*, 5:3, 369-82.

[92] See especially Schmidt, V. (2001), 'Federalism and State Governance in the European Union and the United States: An Institutional Perspective' in Nicolaidis and Howse (2001). Also see Schmidt, V (2006) Procedural democracy in the EU: the Europeanization of national and sectoral policy-making processes, *Journal of European Public Policy*, 13: 5, pp. 670-691.

DOI: 10.2870/1208

decision trap) [93] and 'political organizational cultures' (cooperative federalism).[94] While these insights are welcome, others, such as the need to pay attention to the "feedbacks loops" through which Member States may "upload"[95] or "project"[96] their preferences into the EU policy process, are less generalisable and have a tendency towards the emphasis of 'uniqueness'. Unhampered by the conceptual chains of the contemporary literature on Europeanization, a comparative federalism lens allows equal attention to be devoted to the policy design and subsequent implementation phases of the policy cycle and, most importantly, to view this from an explicitly 'comparative' rather than a 'unique' perspective.

3) Policy modes inspired theories have also generated an expanding literature on distinct modes of EU policymaking. Much of this literature builds on a seminal 1964 article by Theodore Lowi who identified three policy types and argued that each was characterised by a distinct form of political contestation.[97] Specifically, Lowi distinguished between 1) distributive policies, such as tariffs or research grants, which tended to be less conflictual than 2) redistributive policies, such as taxes or social assistance, which were characterised by conflictual forms of political contestation. Lowi also identified a third type. These were 3) regulatory policies, such as product standards or process standards (e.g. environmental policies), which tended to be characterised by a pluralist mode of political bargaining. [98] The Lowi policy framework has been generalised from the US context and applied to the EU case most notably in the work Mark Pollack and his analysis of the EU's

[93] The example given by Risse *et al* is the "joint decisionmaking trap" developed in Scharpf's comparative federalist analysis of German and EU decisionmaking.

[94] Here Risse *et al* also refer to the German model, but in terms of the ability of the consensus-oriented decision-making culture of German "cooperative federalism" to facilitate adaptation to EU pressures.

[95] Börzel, T. (2003) 'Shaping and Taking EU Policies: Member State Responses to Europeanization'. Queens Papers on Europeanization, No. 2, Queens University, Belfast.

[96] Bulmer, S. and Burch, M. (2000), 'The "Europeanization" of Central Government: the UK and Germany in Historical Institutionalist Perspective' in Aspinwall, M. and Schneider, J. (eds.) *The Rules of Integration*, Manchester: Manchester University Press.

[97] See Lowi, T.J. (1964), American business, public policy, case-studies, and political theory *World Politics* 16:4, pp. 677-715.

[98] Ibid.

DOI: 10.2870/1208

'creeping competences'.[99] More recently, Helen Wallace has built on the Lowi typology and diagnosed five distinct policy 'anatomies' of EU policymaking.[100] The first three essentially conform to the Lowi types, but Wallace adds two extra modes of policymaking that appear to be specific to the EU. These are 'policy coordination' (a softer form of policymaking involving 'benchmarking' and comparisons of best practices) and 'intense transgovernmetalism' (a policy mode in which member states through the European Council and/or the Council of Ministers, and their national representatives, play the dominant role). Her main argument is that these five policy modes provide an 'institutional anatomy' of the EU policymaking process. Furthermore, the two additional types constitute a distinct new policy mode that has emerged in the newer areas of active EU involvement. She suggests that an important systemic change may be underway as new areas 'of sensitive public policy are being assigned by EU member governments to forms of collective or pooled regimes, but using institutional formats over which they retain considerable control'.[101] These insights could be especially relevant to this dissertation's theoretical and empirical ambitions. In a similar vein, the work of Majone has drawn on the policy modes literature to focus explicitly on the regulatory policies of the EU. His main thesis is that, for a number of structural reasons, the EU has specialised on a regulatory policy mode to become a 'regulatory state' *par excellance.*[102] Interestingly, Majone drew comparative inspiration from the US model where independent agencies play a crucial regulatory role. However, the application of the US model of independent agencies to the EU has not been without criticism.[103] Joerges and Neyer, in particular, have argued that the EU model needs to be distinguished from the

[99] For instance see Pollack, M.A. (1994), Creeping Competence: The Expanding Agenda of the European Community, *Journal of Public Policy* 14, pp. 95-145; on the EU. Also for applications to the Swiss case see Serdült, U. (forthcoming) Drogenpolitik von unten: Drogenpolitische Massnahmen und Politiknetzwerke in Bern, Chur, St. Gallen und Zürich.

[100] These are the 1) classical Community method; 2) the EU regulatory mode; 3) the EU distributional model; 4) the policy coordination model; 5) intensive transgovernmetalism.

[101] See p.89 Wallace, H. (2005).

[102] See for instance Majone, G. (1994) The Rise of the Regulatory State in Europe. *West European Politics*, 17, pp.131-156.

[103] See in particular Shapiro, M (1997), The problems of independent agencies in the United States and the European Union. *Journal of European Public Policy*. 4:2 pp 276-291. See also Follesdal, A and Hix, S. (2006) "Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik." *Journal of Common Market*, 31:2, pp. 153–70.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

adversarial model of delegation to the so-called US fourth branch of government, the independent agencies. [104]

All three strands of the literature discussed above have made important theoretical and empirical contributions to the study of the EU and, in particular, its policy dynamics. Most significantly, the different approaches have put the policy dimension at the core of their analytical efforts. Although they are characterised by notable differences in terms of their theoretical ambitions, empirical focus and favoured methodologies there is one element that tends to unite them. This is the tendency to concentrate on the EU as a single case and to avoid explicit comparison with other polities. Such a tendency can be contrasted with some of the comparative federalism inspired policy studies. In fact, an expanding literature increasingly conceptualises the EU's federal arrangement as an explanatory variable which accounts for particular policy outcomes. Although not all authors necessarily employ the term comparative federalism, it is implicit in the logic of their comparative approach. In other words, their research design is based on a structured and focused comparison of the EU with other *federal* polities in order to explain similarities and differences in policy outcomes. It is this feature which provides the common analytical thread to these comparative federalism inspired policy analyses. Mostly, they consist of comparative case studies involving the 'usual federal suspects', especially the US. These studies have begun to shed new light on dynamics and outcomes in a variety of policy domains including: environmental policy;[105] fiscal relations;[106] water policy;[107] genetically modified organisms and food safety;[108] and even welfare and social policies.[109]

---

[104] See Joerges, C., and Neyer, J. (1997), From intergovernmental bargaining to deliberative political process: The constitutionalization of comitology, *European Law Journal*, 3, pp.273-299.

[105] See Sbragia, A. M., ed. (1992), *Europolitics, Institutions and Policymaking in the New European Community*, The Booking Institute, Washington D.C.; Vogel, D. (2001), Ships Passing in the Night: The changing politics of risk regulation in Europe and the United States, *EUI Working Papers, Robert Schuman Centre*; and Kelemen (2002).

[106] See McKay, D (2000), Policy legitimacy and institutional design: Comparative lessons for the European Union, *Journal of Common Market* Studies 38:1, pp. 25-44. In a later article the focus is on monetary union from comparative perspective, see McKay, D (2005), Economic logic or political logic? Economic theory, federal theory, and the EMU, Journal of European Public Policy 12:3 (June), pp. 509-527.

[107] See Hoornbeek, J. (2004), Policy-making institutions and water policy outputs in the European Union and the United States: A comparative analysis, *Journal of European Public Policy* 11:3 (June), pp. 461-496.

[108] See Bernauer, T. and Caduff, L. (2004), In whose interest? Pressure group politics, economic competition, and environmental regulation, *Journal of Public Policy* 24, 99-126.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Among the more theoretically sophisticated research designs one could include Kelemen's analysis of environmental policymaking.[110] Inspired by rationalist theories of federalism, Kelemen applies a Rikerian type analysis of strategic bargaining to the interactions between political elites from the state level and the federal level in the environmental the policy domain. More importantly, he does so by explicitly comparing the EU to three other federal political systems. His major thesis is that the federal institutional structures of the EU and the US tend to generate more similar policy dynamics in the area of environmental regulation than the two other federal polities (Australia and Canada) he analysed. Given the characteristically high negative externalities and the potentially large economies of scale derived from pursuing EU level policy action, environmental policy is a domain that is especially suited to comparative analysis. The same could be said for the field of monetary policy, where similar dynamics are likely to be present. The case of European Monetary Union (EMU) has been used by McKay as a basis for reformulating Riker's external threat hypothesis[111] and, more recently, for critiquing the basis of the EU's Stability and Growth Pact by drawing on comparative federal theory.[112]

A *prima facie* more difficult case for comparative analysis would include social and welfare policies.[113] Undeterred by this, some analysts have analysed the EU's policy constraints in the domain of social policies by making an explicit comparison of the EU with six other federations. Despite the peculiarities of the EU, and the fact that its joint decision-making system tends to inhibit social policy change, Obinger *et al* found certain striking similarities with the Swiss case. These include a tendency to specialise in regulatory social policy rather than redistributive social policies. Thus, they draw on parallels between the asymmetry of the Swiss case, a pioneer in regulatory social policy and a

[109] Obinger, H, Leibfried, S. and Castles FG (2005), "Bypasses to a social Europe? Lessons from federal experience", *Journal of European Public Policy*, 12:3, pp.545-571.

[110] See Kelemen (2002)

[111] See for instance McKay, D. (1997) On the Origins of Political Unions: The European Case, *Journal of Theoretical Politics*, Vol. 9, No. 3, 279-296

[112] See in particular McKay (2005).

[113] For an overview of challenges to the welfare regimes from an EU perspective see Rhodes, M (1997) The Welfare State: Internal Challenges, External Constraints', in M. Rhodes, P. Heywood and V. Wright (eds.) *Developments in West European Politics*, Macmillan Press.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

laggard in redistributive social transfer payments, and similar patterns that, they argue, can be observed in the EU. Another important policy domain that ought to be singled out and is becoming the subject of increasing academic attention is the development of policies related to organised crime in the third pillar domain. A number of scholarly studies, by both lawyers and political scientists, have begun to investigate the dynamics of this area and that of the broader so-called justice and home affairs pillar.[114] Some of these studies, although initially drawing on comparative insights have ultimately refrained from conducting an explicit comparative analysis.[115] Thus, there appears to be a dearth of comparative research, where EU developments in the field of justice and home affairs are compared to historical processes in other polities.

All of the policy analyses noted above suggest that, in the context of EU policy-making, the choice of policy domain matters. Both Wallace and Majone's insights are therefore relevant to this discussion. While Majone has alerted us to the fact that the EU specialises in 'regulatory policy', Wallace's recent focus on the emergence of new policy modes for sensitive areas, such as those of the EU's third pillar, are also especially pertinent. This suggests that where externalities are high, and where regulatory policy action can be pursued rather than, say, redistributive policies, it is possible that the EU can act in a similar fashion to fully fledged federations. Such policy areas are therefore more likely to invite comparative analyses and, to the extent that this is possible, such analyses ought to yield more generalisable insights. On the other hand, some studies have also broken new ground by focusing on EU policy domains which do not appear, at first sight, to invite comparison with other polities. This is especially the case for research designs comparing developments in fiscal relations[116] (e.g. McKay) and social policies[117] (e.g. Obinger et al) in the EU with that of other federal polities. The fact that both

[114] See in particular Walker, Neil. 2003. The Pattern of Transnational Policing. In A Handbook of Policing. Ed. Neburn, Tim ed. London: Willan Publishing; den Boer, Monica and Wallace, William (2000). Justice and Home Affairs in H. Wallace and W Wallace, Policy-making in the European Union. Oxford: Oxford University Press; Monar, Jorg (2001). Justice and Home Affairs. Journal of Common Market Studies 39 Annual Review pp121-137.

[115] This is the case for Occhipinti, J D. (2003) *The Politics of EU Police Cooperation: Toward a European FBI?*, Boulder: Lynne Rienner.

[116] McKay, D (2000).

[117] See, Obinger, Liebfried and Castles (2005).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

these contributions have shed new comparative light on seemingly unique policy areas of the EU is testament to the value of applying the federal comparative design to EU policy studies.

4. An operational definition of comparative federalism

To further review the growing differentiation in current European integration theorising would only detract from the object of enquiry. I shall therefore focus on what constitutes a comparative federalism approach and how it differs from others. Put simply, the major difference is that comparative federalism is explicitly concerned with federal polities as units of analysis. Comparative federalism can be further distinguished from other comparative politics derived approaches because of its primary focus on certain very specific features of a polity. This predisposition (or bias) should therefore be laid out in the open since it has considerable normative consequences. For instance, it is possible that when discussing preferred normative trajectories for the EU one of the root causes of the academic disputes that tend to be generated is intrinsically connected to a tension between the 'democratic principle' and the 'federal principle'. The tension is how to square the democratic principle of 'one person, one vote' with the federal principle of 'one sub-unit, one vote'. The latter tends to be the major concern for scholars of federalism and constitutes a core analytical component of the comparative federalism literature. Other scholars may choose to give primacy to the democratic principle.[118] This ought to alert us to the important implications and normative preferences that follow from adopting a particular empirical conception of the EU. With the federal bias fully laid out it is possible to offer a definition of comparative federalism as used in this dissertation.

Comparative federalism approach is here understood to denote a theory-driven empirical exercise rather than a normative or philosophical one. Its focus is on the empirical study of federal political systems using structured and focused comparison which may involve: (1) the classification of the various species or sub-species that form the genus of federal political systems or (2) the development of theories and/or the formulation of hypotheses which purport to explain causal connections between

[118] See for instance Hix (2005).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

'federal political institutions' and the way in which these define and/or regulate interactions among political actors or (3) combinations theoreof. A comparative federalism approach to the EU is therefore understood as one that uses the above logic to *explicitly* include the EU case within its research design.

The rest of this dissertation is concerned with this undertaking.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 3 Research Design: Case Selection, Hypotheses and Methods

This chapter begins by identifying a (new) federal species that has reappeared in the literature –the compound polity.[1] I begin by outlining some of its basic features and then proceed to identify a very limited universe of compound polities: the US, Switzerland and the EU. Questions related to case selection when incorporating the EU as a unit of analysis in comparative political research are then addressed. Having identified a broad area of homogeneity among cases, I then outline similarities and differences among the cases as a basis for a 'most similar case' design. This is followed by a section on the selection of a policy domain and the presentation of two guiding hypotheses for structuring the empirical investigation. In the final section issues related to the research methodology are addressed.

1. The 'Compound Polity': A new federal species?

In this section I will attempt to flesh out the basic features of the conceptualisation informing the research inquiry. Central to this endeavour is the concept of a 'compound polity'. Drawn from the literature on comparative federalism, and with recent applications to the EU case, the term is employed by Fabbrini[2] to describe a form of political organisation that is characterised by a *dual* separation of powers. A '*compound polity*' is also analytically analogous to Kelemen's '*separation of powers federal systems*.'[3] Both Kelemen[4] and Fabbrini[5] are describing a particular species within the genus of federal political systems and employ a similar taxonomic logic although they use different labels. I will employ the less wordy concept of 'compound polity' to denote this particular species within the genus of federal political systems. Central to Fabbrini and Kelemen's conceptualisation is the existence of a *dual* (Kelemen) or *multiple* (Fabbrini) separation of powers. Essentially, both are

[1] The concept of a compound polity, or republic, was first identified in the *Federalist Papers.*

[2] See Fabbrini, S. (2004), Transatlantic constitutionalism: Comparing the United States and the European Union. *European Journal of Political Research* 43:4, pp. 547-569; and Fabbrini, S. and Sicurelli, D. (2004), The Federalization of the EU, the US and Compound Republic Theory: The Convertion's Debate, *Regional and Federal Studies,* 14:2 pp.232-254.

[3] Kelemen, D. (2002), Regulatory federalism: EU environmental regulation in comparative perspective, *Journal of Public Policy*; 20:3, pp. 133-167.

[4] Kelemen (2002) and (2004), *The Rules of Federalism,* Cambridge, MA: Harvard University Press.

[5] Fabbrini (2004).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

referring to a distinction between a vertical and horizontal dimension. According to Fabbrini, a compound polity is defined by a multiple separation of powers: vertically between the sub-units and the centre; and horizontally in terms of divided institutions. Kelemen uses the terminology of a 'fragmented centre' to refer to the same feature[6]. Fabrinni has argued that although all federal states have a vertical separation of powers this does not 'imply any horizontal separation' and these 'countries continue to be organized along parliamentary lines, in the sense that power remains in the hands of the legislature, or rather of the government and its leader supported by the legislative'.[7]

According to Fabbrini,[8] apart from the US, the only other 'compound polity' that exists is Switzerland, which since the adoption of its 1848 constitution 'has continued to be organized around a federal distribution of territorial power and a separation of institutions at the governmental level'. Kelemen, does not mention Switzerland as another case of, to use his terminology, a 'separation of powers federal system'. But Fabbrini does. His principal argument is that the EU is a compound polity *à la US*.[9] Having identified the only three existing cases of compound polities, Fabbrini then proceeds, on the basis of a rather weak form of argumentation, to dismiss one of the cases on the grounds of size. For Fabbrini, '[a]lthough the United States and Switzerland were demographically comparable at the turn of the eighteenth century, they now differ immensely in the complexity of their societies. In sum, *size matters*¸ and it is difficult to compare a continent-wide polity with one that is peculiarly small.'[10] The problem with such a line of reasoning is that it *logically* implies that there must be a certain geographical extension or demographic threshold condition for a compound polity. Incidentally, neither condition actually figures in Fabbrini's operational definition of a compound polity. This may appear even more problematic given that the question of size or scale has not hindered the development of comparative federalism as a field of inquiry.

[6] Ibid.
[7] Ibid., 553. This is similar to the definition offered by Kelemen (2002), although he uses the term separation of powers federal systems.
[8] Fabbrini (2004).
[9] See also Fabbrini and Sicurelli (2004).
[10] See Fabbrini (2004), 553.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Indeed, the field of comparative federalism has developed *not* because it has taken account of variations in size or scale among states, but rather because it has *ignored* such variables. This has permitted the fruitful comparison of political dynamics in federations, including large ones such as India and Russia and much smaller ones such as Belgium.[11] But the more serious objection is connected to the juxtaposition of complexity and size[12]. There is no necessary correlation between the two, especially in relation to Switzerland and the US. The US political system does not possess a greater degree of complexity than the Swiss one. For instance, the US has a less complex cleavage structure (e.g. cultural, religious and linguistic) than Switzerland[13] and, when it comes to powers vested in the centre, it is also more centralised.[14]

2. Case selection: The limited universe of compound polities

As Ragin et al[15] have argued, there are serious methodological grounds for including all cases of a known but limited universe since the exclusion of any single case may alter the findings. This view is taken seriously for the purposes of research design in this dissertation and we can now proceed to develop aspects of the research design for the comparative analysis of three compound polities.

Thus far some of the basic defining features of a distinct federal species, the compound polity, have been identified. Following Fabbrini two compound polities have been identified, the US and Switzerland, to which the EU could be added[16]. We can describe this as an n=2 + EU research design. The 2

[11] Lane, J. and Ersson, S. (2000) The new institutional politics: Performance and outcomes, London: Routledge.

[12] This is not to argue that size as shown by Dahl, R. and Tuft, E.R. (1973), *Size and Democracy*, Stanford, CA: Stanford University Press, does not matter, but rather that in terms of the operation of federal political institutions we should not exclude cases on the basis of size.

[13] Lijphart, A. (1984), Democracies: Patterns of majoritarian and consensus government in twenty-one countries, New Haven, CT: Yale University Press.

[14] McKay, D. (2001), Designing Europe: Comparative Lessons from the Federal Experience, Oxford: Oxford University Press.

[15] Ragin, C., Berk-Schlosser D., and de Meur G. (1996), 'Political methodology: Qualitative methods' in Goodin, R and Klingemann H (eds.) (1996), *A new handbook of political science*. Oxford: Oxford University Press.

[16] Fabbrini (2004).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

refers to the US and Switzerland while the EU as a distinct category intends to convey the fact that the overriding object of the research design is to gain comparative insights on the EU. But in following the n=2 + EU research design, as this dissertation does, other federations have been excluded from the case selection. Below I will attempt to provide a justification for adopting the above research design and compare it to others in the literature. This requires us to refer back to the literature on comparative federalism. The latter tends to identify a special category of federations among advanced industrial economies that I shall refer to as the 'five usual federal suspects' (*n* = 5). These are Australia, Canada, Germany, Switzerland, and the US. These five usual federal suspects have figured quite prominently in policy studies (see chapter 2). Sometimes the federal *n* = 6, when Austria is added.[17] More problematic is the inclusion of other quasi-federal suspects such as Belgium, Spain and Italy. These are can be referred to as a distinct category of 'regionalised systems.'[18] For instance, on the basis of a series of empirical indicators, such as central and sub-unit revenues and expenditures, regional grants from central government, and the strength of bicameralism, Braun[19] identifies a distinct 'federal group' composed of the five usual federal suspects. There is thus a reasonable degree of consensus in the literature as to this special category of advanced industrial states. Some disputes may arise as to whether this category should be expanded to include Austria.[20] It may be better to consider Austria, using Keman's categories, as somewhat of a half-way house between the 'five usual federal suspects' and newer federalising states such as Belgium and Italy.[21]

Our federal universe has been narrowed down to the five usual federal suspects or, depending on the author, an *n* = 6, when Austria is included. The argument put forward in this dissertation is that it is possible to narrow this

[17] Take, for example, Lijphart (1984) and Keman, M. (2000), 'Federalism and policy performance' in Wachendorfer-Schmidt, U. (ed.) *Federalism and Political Performance*, London: Routledge, pp. 196-227.

[18] As in Braun, D. (2000), *Federalism and Public Policy*. Aldershot: Ashgate.

[19] Ibid.

[20] For example Lijphart (1984) and Keman (2000) include Austria, while Braun (2000) argues against it.

[21] See Keman (2000).

DOI: 10.2870/1208

federal group further still. This is precisely the logic behind the concept of a 'compound polity', especially as used by Fabrinni. Nevertheless, many earlier approaches have insightfully compared the EU to the five usual federal suspects. The most comprehensive study of this kind has been McKay's[22] macro-historical comparative study of the EU. McKay uses an *n* = 5 + EU approach (the five usual federal suspects plus the EU). The same logic and design applies to Mckay's[23] policy specific study of fiscal relations. Obinger *et al's* illuminating study of welfare state consolidation, however, uses an *n* = 6 + EU formulation, where the extra unit of analysis is Austria.[24] It is instructive to note that both of these systematic studies suggest that the EU has most to learn from the Swiss case. These findings have been taken seriously for the present research design and case selection.[25]

But this is not the only formula available. For instance, Kelemen[26] breaks new theoretical ground in his attempt to explain regulatory federalism in the EU. His conceptualisation comes closest to the design adopted in this dissertation and is therefore worth investigating more closely. Kelemen seeks to explain patterns of environmental policymaking in federal polities by explicitly incorporating the EU to his research design. Kelemen identifies two types of federal polities: '*separation of powers federal systems'* and '*parliamentary federal systems'*. He includes the US and the EU within the first category, and Australia and Canada within the second. His is therefore an *n* = 3 + EU research design. His central insight is that *separation of powers federal systems*, such as the EU and the US, tend to exhibit similarities in regulatory outcomes. In a further extension of this study Kelemen included Germany in his research design, as another case of *paliamentary federal systems.* Had he included another *separation of powers federal system*, such as Switzerland instead of Germany, he may have provided a more rigorous test of his

[22] McKay (2001).

[23] Mckay, D. (2000), Designing Europe: Comparative Lessons from the Federal Experience, .Oxford: Oxford University Press.

[24] Obinger, H, Leibfried, S. and Castles F.G. (2005), Bypasses to a social Europe? Lessons from federal experience, *Journal of European Public Policy*, 12:3, pp.545-571.

[25] The Obinger et al article is based on the findings of an international research project on OECD federations.

[26] Kelemen (2002 and 2004).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

theory.[27] Nevertheless, Kelemen offers one of the most insightful applications of formal theories of federalism to the EU case in order to explain the dynamics of regulatory federalism. Moreover, unlike many other authors, he focuses on policy outcomes rather than solely on constitutional or institutional set up.

Constitutional and institutional structures are, however, the explicit focus of Fabbrini.[28] Like Kelemen, he also uses a compound polity conception of the EU. Nevertheless, after rejecting the Swiss case on account of its size, Fabbrini effectively adopts an *n* = 1 + EU research design (the US and the EU). Moreover, unlike Kelemen's ambitious explanatory agenda, Fabbrini's focus is on similarities among the institutional architecture of both the EU and the US compound polities, rather than how such similarities may explicitly impact on policy outcomes. This type of *n* = 1 + EU research design tends to be one of the more popular designs and it commonly takes the form of an EU/US comparative study. The edited volume by Howse and Nicolaidis represents one of the most comprehensive contributions following this format.[29] Implicit in their design is the idea that both federal polities can be compared across a number of constitutional, institutional and regulatory policy domains. Part of the justification for the research design employed in this dissertation is to take this strategy further by adding another unit of analysis. To this end, I have taken on board some of the most innovative applications of comparative federalism insights to the EU, in particular the work of Kelemen and Fabbrini, and in doing so added a neglected case: the Swiss one. In doing so, it has also narrowed the federal universe as used by Obinger and McKay. The combined effect of this comparative research strategy could provide new insights for understanding EU policy dynamics.

[27] In Kelemen (2004), Germany, is appended as another 'parliamentary federal system' producing somewhat ambiguous results.

[28] Fabbrini (2004).

[29] Nicolaidis, K. and Howse, R. (eds.) (2001), The Federal Vision: Legitimacy and levels of governance in the United States and the European Union, Oxford: Oxford University Press.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

3. Similarities and differences among 'Compound Polities': Towards a most similar case design

In order to frame the area of investigation -a limited universe of three cases- some rather minimal definitions of what constitutes the defining features of a 'compound polity' have been offered thus far. It somehow relates to a dual (multiple) separation of powers, or, expressed in an alternative way, a federal system with both a vertical and horizontal division of powers. Although a broad area of homogeneity has been defined for establishing the boundaries for case selection, it still appears to be too general. A *dual* separation of powers federal system may serve as a useful working definition, but it is clearly rather reductionist since there seems to be an implicit assumption that it is merely the similarities among macro-institutional settings which produce the analogous outcomes. In order to identify further common variables or isolate potential explanatory ones that are linked to particular outcomes, it will be necessary to analyse the cases more carefully. Thus we need to go beyond the macro institutional features of a compound polity without, in any way, neglecting their importance. Further compelling theoretical and substantive criteria will be required to take account of a wider range of factors than mere 'verticality' or 'horizontality' in institutional settings. In order to do so, it will be necessary to specify potentially important pre-conditions through the further identification of similarities and differences among the cases.[30]

This section will analyse three interrelated dimensions with a view to placing the case studies in their appropriate contextual setting. The three dimensions are: 1) the *origins of compound polities*, namely the dynamics surrounding the historical formation of the three compound polities and how these can affect subsequent institutional developments; 2) the *constitutional and institutional setting* and 3) a set political *process dynamics,* which are mainly connected to decision-making processes and modes of policy implementation and enforcement. This exercise is necessary in order to identify some of the potential explanatory variables impacting on the regulatory outcomes that are the subject of the empirical analysis.

[30] See Ragin et al. (1996) and Mair, Peter (1996), 'Comparative Politics: An Overview' in Goodin, Robert E. and Klingemann, Hans-Dieter (eds.) *A New Handbook of Political Science*, Oxford: Oxford University Press.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

1) Origins of a 'compound polity': According to one influential variant of new institutionalism, history, and the path dependency effects it can generate, is crucial to understanding institutional trajectories.[31] How can the history or the origins of a compound polity affect subsequent institutional evolution? Comparative federalism can again offer us some analytical clues for understanding the EU. One can identify a number of theoretically relevant historical factors concerning the origins of political integration among the three cases. Our concern is not with explaining or looking into the origins of their respective initial federal bargains, but rather to take seriously Elazar's contention that the origins of a polity are important because it tells a lot about the subsequent framework that emerges.[32] Thus, according to the typology developed by Stepan,[33] Switzerland and the US constitute examples of '*coming together*' types of federalism.[34] One could add the EU to this special category. These are to be contrasted with so-called '*holding together*' types of federalism such as Spain, Belgium or Canada. The implication is that the 'coming together' type typically posses institutional arrangements that constrain the centre from overriding the sub-units.[35] According to Stepan,[36] this type tends to be 'demos constraining' polities that are characterised by a fear of excessive central government power. This is a dynamic that is extremely pertinent to the policy issues that are the subject of the empirical investigation.

[31] For a survey of variants of new institutionalism see Hall, P. and Taylor, R.C.R. (1996), Political Science and the three new institutionalisms, *Political Studies*, XLIV:936-957. For an overview on historical institutionalism and path dependency see Pierson, P. and Scocpol, T. (2002), Historical institutionalism in contemporary political science in Katznelson, Ira and Milner, Helen V. (eds) *Political Science: State of the Discipline.* American Political Science Association

[32] Elazar, D. J. (1987), *Exploring Federalism*, Tuscaloosa: University of Alabama Press.

[33] Stepan A. (1999), Federalism and democracy: Beyond the US style, *Journal of Democracy* 10, pp. 19-34.

[34] The Swiss 'coming together' case was not as voluntary as Stepan suggests, there was a coercive element to it as well, see Bachtiger, A and Steiner, J (2004) Switzerland: territorial cleavage management as paragon and paradox. In *Federalism and Territorial Cleavages* (eds)Ugo M. Amoretti and Nancy Bermeo, Baltimore : Johns Hopkins University Press.

[35] See p. 2 in Føllesdal, A. (2003), "Federalism", The Stanford Encyclopedia of Philosophy (Winter 2003 Edition), Edward N. Zalta (ed.),
URL http://plato.stanford.edu/archives/win2003/entries/federalism/

[36] Stepan (1999).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Riker's military threat hypothesis (discussed in chapter 2) is also relevant for understanding the origins of a federal polity. Security certainly matters, but it can also be defined more broadly and in less militaristic terms. This is the logic behind McKay's reformulation of the Rikerian military hypothesis.[37] McKay has highlighted the importance of the 'trade' or 'welfare' motive behind the EU's initial federal bargain. Furthermore, it is patently obvious that the original 'trade' or 'welfare' motive has conditioned many aspects of the EU's subsequent institutional evolution. But we need not deny the importance of the military threat component either. Blondel, for instance, has stated that

'*se non fosse esistita una cortina di ferro non e detto che l'Unione europea sarebbe sorta egualmente, ne che si sarebbe sviluppata con la rapidita con cui si e sviluppata*'.[38]

Blondel, however, goes much further than simply stating that the Cold War context influenced the trajectory of European integration. He draws some intriguing parallels with the Swiss case. In the latter, neutrality emerged as the only available mechanism for overcoming the deep foreign policy divergences among the cantons (some looked to Germany or France and others to Italy). The similarities with the EU case in this context are particularly striking and highlight the perennial problems surrounding the development of a common defence and security policy in the EU.[39] The absence of converging foreign policy preferences among the subunits helps to explain the emergence of 'neutrality' type mechanisms most clearly in Switzerland. A similar dynamic is clearly at play in the context of the EU and its development as a 'civilian power'.

[37] McKay, D. (2001), *Designing Europe: Comparative Lessons from the Federal Experience*. Oxford: Oxford University Press. See also McKay (1999; 2004).

[38] 'If it wasn't for the Iron Curtain it is not at all certain that the European Union would have developed in the way it did nor as rapidly as it has developed.' (authors translation), see pp 213 in Blondel, J. (1998), Il Modello svizzero: un futuro per l'Europa?, *Rivista Italiana di Scienza Politica*, n. 2, pp. 203-227.

[39] See Sidjanski, D (2000), *The federal future of Europe: From the European Community to the European Union*. Michigan: University of Michigan Press.

DOI: 10.2870/1208

In sum, there appear to be striking similarities when comparing the federalist origins of the EU with those of the US and Switzerland. However, these similarities are especially pertinent in the case of Switzerland. According to Blondel,[40] only Switzerland and the EU represent cases of political integration *not* imposed from above that incorporated subunits with completely different social structures and relatively little in common. This was certainly less the case for the culturally and linguistically more homogenous states of the US. It is because of this that the Swiss model of federalism had to invent a different type of federal structure, even though it drew inspiration from the US constitution.[41] In brief, if one takes seriously the Elazar and Stepan argument that origins matter, then it is possible to note the similarities (and differences) among the compound polities under investigation while recognising how these may impact on subsequent political developments.[42]

2. Constitutional and institutional setting: This can be considered to refer to a set of structural variables that have figured quite prominently in the literature. In fact, the constitutional and institutional setting is the core element in conceptualisations of the EU as a 'dual' or 'multiple separation of powers' type of federal polity. This section will focus on certain macro-institutional features of the three compound polities. As has been noted above, the vertical territorial division of power in the three compound polities is similar to that of other federations. At the same time, and unlike many other federations, all three have a clear separation of powers between the legislative and executive at the so-called horizontal level, as well as a separate judiciary. But to solely focus on these macro-institutional variables is clearly unsatisfactory. Furthermore, separation of powers is in many respects a misleading concept. This is because in practice, powers are shared between horizontal institutions in all three polities. Even in the case of the US, the classic example of a separation of powers system, Neustadt famously argued that the constitution, does not separate power so much as create a government of separated

[40] Blondel (1998), p. 215.
[41] See Blondel (1998), 214.
[42] Elazar (1987) and Stepan (1999).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

institutions sharing power.[43] This is an accurate description of the horizontal power structures in the three polities under investigation. Below we briefly outline some of the similarities (and differences) among legislative, executive and judicial functions.

In terms of the legislature, all three polities have a classic two chamber legislature in which a Senate or Council (of States in Switzerland and of Ministers in the EU) represents the subunits and is counterbalanced by a chamber directly elected by the people (the European Parliament, the House of Representatives in the US, and the National Council in Switzerland). However, one potential difference between the polities relates to the respective powers of each chamber. Both the US and Switzerland have symmetric bicameral systems, in which both chambers are formally equal partners in the legislative process. In the EU this is definitely not the case with the Council in an overall much stronger position than the Parliament. Despite this difference, the institutional separation of executive and legislative powers in the EU means that the European Parliament is more like the US Congress or the Swiss Parliament than is the case in most European democracies. The key distinction is between so-called *working* parliaments, characteristic of compound polities such as the US and Switzerland, and *debating* parliaments. In the *working* parliaments there is no fusion of majority party and government and, furthermore, procedural rules prevent members of the executive from sitting on the legislature.[44] The locus of control in *working* parliaments is not exercised through debates on the floor but rather through specialised committees. In a nutshell, committees are at the heart of the system. The US Congress serves as an archetype to which we may add the Swiss and EU cases.

Another feature of all three systems is that the executive does not require the permanent support of a majority in parliament to govern. Even though a censure procedure may exist in the EU, it is more akin to the impeachment of

[43] Neustadt, R. (1991), *Presidential Power and the Modern Presidents*, New York: Free Press.
[44] Dann, P. (2003), The European Parliament and Executive Federalism: Approaching a parliament in a semi-parliamentary democracy, *European Law Journal* 9:5 (December), p. 549-574.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the executive in a presidential system than a parliamentary majority withdrawing its support for the government.[45] Interestingly, the method for choosing the executive is more similar in the EU and Switzerland. In both cases, the election of the executive (the Commission in the EU) is not subject to a competitive *popular* electoral contest but is, instead, the result of negotiation and an election process among the two chambers. Unlike the directly elected US president, who personally embodies the considerable powers of the US executive, both the European Commission and the Swiss Federal Council are collegial bodies. In the Swiss case, a seven-member executive, with an annually rotating presidency, is elected by both chambers to represent major political and territorial groups. In fact, the rotation principle already applies to the Council Presidency on a bi-annul basis among the twenty-five member states.

Lastly, the legal architecture in all three compound polities is similarly characterized by the two fundamental pillars of a federal legal system: the direct effect and supremacy of federal law. These principles are enforced by a separate judiciary with powers of judicial review. Unlike the US Supreme Court however, the Swiss court has limited powers when it comes to the review of federal legislation. In this regard, the US Supreme Court is traditionally a considerably more influential political actor than both the Swiss and EU courts. Still, it has been commonplace among political scientists to proffer explanations of the ECJ's purported activism with the US Supreme Court as the default comparative setting.[46] But this is not an accurate description and the similarities between the two are certainly not relevant when it comes to the judicial review of federal legislation, for instance. In fact, for Chalmers the ECJ's power of 'legislative review is marginal to the point of irrelevance'.[47] Instead, he argues that the ECJ has been an 'aggressive

[45] See Hix, S. (2005), *The Political System of the European Union*, Basingstoke, Hampshire: Palgrave MacMillan.

[46] See Burley, A.M. & Mattli, W. (1993), Europe before the court: A political theory of legal integration, *International Organization*, 47, pp.41-76.

[47] See pp6 in Chalmers, D. (2004), The Dynamics of Judicial Authority and the Constitutional Treaty, in Weiler and Eisgruber, eds., Altneuland: The EU Constitution in a Contextual Perspective, *Jean Monnet Working Paper* 5/04,
Also available at: http://www.jeanmonnetprogram.org/papers/04/040501-14.html

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

administrative court, and very weak in terms of legislative review'.[48] This has been certainly confirmed by the empirical investigation where there has been no judicial review of federal legislation in the EU case (and in the Swiss case given that the Court is prohibited from doing so). In the US, on the other hand, there has been notable judicial activism and the courts have served as a political arena for actors that have been excluded or have been less influential during the legislative phase.

Over time, the EU has developed a sophisticated legislative, executive and judicial system in which the structure of contestation and conflict, driven by a multiplicity of functional and territorial interests, would be familiar to observers of the US and Swiss political system. The similarities should not be exaggerated however, for the EU presents some unique features. But, then so too do the Swiss and the US cases. Of the three compound polities, the macro-institutional similarities are greater, in many respects, among the EU and Swiss 'semi-parliamentary systems' in which the executive is neither directly elected by the people nor accountable to a parliamentary majority, and where there is no single chief executive, whom EU or Swiss citizens can 'throw out'.[49] Below the focus is directed to how these macro-institutional settings could potentially impact on the process dynamics of policy-making in the three compound polities.

3. Process dynamics: The third dimension of contextual variables relates to specific features of the political and policymaking process. Here it is possible to note differences that could potentially impact on regulatory and policy outcomes. Political process dynamics are here understood as a broad category of rules or norms that tend to have a behavioural impact on political actors. Such rules or norms, established either by an explicit or tacit agreement, condition the multiple interactions among political actors and the way in which binding rules or informal conventions are not only produced, but

[48] See *ibid*. Although in a landmark *Tobacco advertising* case the ECJ has, for the first time, recently overturned a piece of central level legislation. This has been interpreted by Hix (2005) as a strategic signal by the ECJ to the member states that it could be trusted at the time of Convention on the Future of Europe.

[49] On the Swiss case see discussion by Rose, R. (2000), The end of consensus in Austria and Switzerland, *Journal of Democracy*. 2: 2 pp.26-40. The EU is addressed in Hix, S (2005).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

also subsequently implemented or enforced. Two types of process dynamics can be identified: 1) those that pertain to how policies are formulated and 2) processes related to the mode in which policy is subsequently implemented and enforced. In discussing the former I am concerned with the decision-making process, which refers to how policy proposals are shaped by multiple political actors, both public and private, and translated into specific legislative acts or binding rules by the central legislative and executive organs. On the other hand, the mode of implementation and enforcement refers to the process by which policy is put into practice and subsequently enforced. Whereas thus far the three units of analysis have displayed notable similarities in terms of certain macro-institutional configurations, when our attention is directed to the way in which political inputs to the policy process are translated into specific policy outputs, important differences can be identified.

1) Decisionmaking processes: Although democracies vary greatly in their institutional structures Lijphart[50] has consistently argued that they tend to cluster so as to form two main types of decision-making styles: majoritarian and consensus. The differences between these two basic models provide for a sharp contrast when we focus on decision-making processes and modes of bargaining in the three compound polities. Majoritarian decision-making tends towards an exclusive, competitive and adversarial style. The system through which interests groups exert pressure on the government is pluralist, uncoordinated and competitive. The US serves as an archetype for this style of decision-making. On the other hand, the prominent features of a consensus decision-making process are inclusion, bargaining and compromise. The system tends to generate elaborate mechanisms of power sharing and, at the level of interest intermediation, gravitates towards interest group corporatism through relatively few, peak associations. The Swiss case serves as the paradigmatic case.[51]

[50] Lijphart, Arend (1984). Democracies: Patterns of majoritarian and consensus government in twenty-one countries. New Haven, CT: Yale University Press; and Lijphart, A (1999). Patterns of democracy. New Haven, CT: Yale University Press.
[51] Ibid.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

When we turn our attention to the EU decision-making process it is evident that a consensus style dominates. A series of consensus inducing mechanisms (both formal and informal) can be clearly identified that include, for instance, qualified majority voting (QMV) in the Council. Nonetheless, although QMV exists, it is subject to a high threshold and the tendency is for the Council to adopt laws by unanimity (in 80 per cent of cases) even where formal QMV is available.[52] With regard to the Commission, the latter operates formally (and informally) as a collegial body. Furthermore, informal procedures such as the elaborate system of committees, known as 'comitology', have been developed where national experts issue opinions on the Commission's proposed implementation measures. Indeed, in a pioneering analysis of the EU's comitology system, Joerges and Neyer argue that a form of institutionalised deliberation has emerged which should be distinguished from the adversarial model of the US.[53] The key to their argument is that comitology is a non-hierarchical, deliberative and consensus achieving mechanism which helps to solve policy problems.[54] In parallel, the Commission has encouraged the development of consultation mechanisms in the formulation of policy. These include the participation of a multitude of peak-level sectorial networks, so long as they operate according to a pan-European rather than a national logic.[55]

Such intricate processes of negotiation and deliberation among all the relevant stakeholders, in which decisions are taken consensually, inevitably slow down the decision-making process and the responsiveness of a political system to major challenges. A similar dynamic exists in Switzerland. Indeed, Kriesi and Trechsel have argued that as a result of Switzerland's inclusive character, the political decision-making process tends to be reactive, slow and incremental and that with regard to major societal problems decision-making

[52] See for instance Costa, O. and Magnette, P.. (2003). The European Union as a Consociation? A Methodological. Assessment. West European Politics, 26(3), pp.1-18.

[53] See Joerges, C. and Neyer, J. (1997). From intergovernmental bargaining to deliberative political process: The constitutionalization of comitology. European Law Journal, 3, pp.273-299. For an alternative view see Majone (1996).

[54] See discussion in Hix (2005)

[55] Ibid.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

is usually only taken up under immense external pressure.[56] The similarities between the Swiss and EU polities in this regard are quite remarkable. As in the EU, where no identifiable head of state possess powers to make sweeping policy decisions, the Federal Council (the Swiss executive body) is a consensus seeking body *par excellance* in which leadership comes from mediating between conflicting interests rather than issuing orders. This feature is firmly embedded in the Swiss political psyche.[57] A major consensus promoting mechanism in the Swiss decisionmaking process is the pre-parliamentary consultation procedure, where draft bills are submitted to a number of political and societal actors, among them the subunits. According to Baechiteger and Steiner, the consultation procedure 'is the locus where corporate actors express their interests and where consensual solutions are crafted'.[58] Moreover, the consultation phase and the numerous expert committees can serve to forge compromise solutions that help to avoid a possible referendum at the end of the legislative procedure.[59] All of this is not to suggest that consultation phases are unimportant in the US, for they are. However, there are major differences in terms of the process of interest representation with the US generally more open and influenced by money interests as well as by party politics.[60] This offers a stark contrast to both Switzerland and the EU where the overall number and variety of interests are usually more restricted and tend to be more sensitive to territorial concerns.

In addition, it is possible to point to the role of political leadership. In this regard, the directly elected chief executive in the US enjoys a greater ability to influence decision-making than in the Swiss and EU context. Some have argued that this can encourage a 'monocratic' style decision-making from the

[56] See Kriesi, H and Trechsel, A (forthcoming) *Swiss politics. Continuity and Change in a Consensus-Democracy*. Cambridge: Cambridge University Press.

[57] For a detailed discussion see in Kloti, U. (2001). Consensual government in a heterogeneous polity. *West European Politics* 24:2 pp.19-25.

[58] See in particular Bachtiger, A. and Steiner, J. (2004: 34). 'Switzerland: territorial cleavage management as paragon and paradox' in Amoretti, Ugo M. and Bermeo, Nancy (eds.). *Federalism and Territorial Cleavages*. Baltimore: Johns Hopkins University Press.

[59] See Kriesi and Trechsel (forthcoming).

[60] For a further development of this argument from an EU comparative persepctive see Schimt, V. (2006).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

centre.[61] This type of decision-making is anathema to Swiss and EU governing styles and would only serve to exacerbate group conflict. A consensus logic therefore operates and is reinforced by a consociational style of interest intermediation at the policy initiation stage. This also can impact on the responsiveness of the system. Unlike the US where lawmakers can be more responsive to pressing policy challenges, the political process in the EU and Switzerland is remarkably slow given the need to secure consensus among multiple veto players at various levels of political aggregation. As a result, both polities have developed a series of mechanisms which allow political elites to reduce the uncertainty of a veto by the Council in the EU, or a referendum vote in Switzerland. Such differences can be expected to impact on the range of issue areas that will be the subject of the empirical investigation.

2) *Modes of policy implementation*: With regard to the second dimension - modes of policy implementation and enforcement- a further potentially important distinction can be identified between the three polities. The distinction revolves around the constraints faced by the centre and, in particular, the centre's dependence on the subunits for the implementation of policies. The difference between the model that exists in the US and how the Swiss and EU systems operate is again quite striking. Once federal legislation is passed in the US, the federal government can draw on a fully developed federal bureaucracy and judiciary for implementing and enforcing its laws. Most importantly, it has the financial resources to do so, and, if necessary, can create new bureaucracies for implementation.[62] Finally, it is able to do so without the support of the sub-units. This suggests that the centre has considerable 'power capabilities' in terms of the implementation and enforcement of policy. This can be contrasted with the much weaker powers of the centre in the EU and Switzerland.

[61] See Baylis, T.A. (1989). *Governing By Committee*. New York: State University of New York Press.

[62] Halberstam, D. (2001), Comparative Federalism and the Issue of Commandeering in Nicolaidis and Howse (2001).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

If our attention is focused on Switzerland it is possible to note that although it may have borrowed heavily from the spirit of the US constitution, Switzerland refrained from following the US model of developing parallel administrations. Thus, the Swiss federal administration has no regional offices in the subunits, and once federal policies are agreed upon they are delegated back to the cantons for implementation and enforcement.[63] The logic of implementation by federal delegation serves not only to strengthen the subunits' discretion during the implementation process, but also enables them to play a key role during the policy formulation stage.[64] Indeed, from a comparative perspective, Blondel argues that the cantonal authorities of Switzerland are more influential and independent than in any other federation.[65] Moreover, what most distinguishes the Swiss system is not so much that the implementation of policy is in the hands of the cantons, but rather that the system generates such heterogeneity during the implementation process and, as a consequence, a high degree of variability in policy outcomes.[66]

In many respects, the EU policy process is strikingly similar to that of Switzerland. Firstly, in terms of the implementation and enforcement of EU legislation and, secondly, with regard to the heterogeneity in policy outcomes that are generated. As in the Swiss case, when it comes to implementation and enforcement, the EU has no regional offices in the subunits with any significant implementation apparatus at its disposal.[67] As a result, it has to rely on the subunits for policy implementation and enforcement. In both the Swiss and EU cases, the institutional framework strengthens the role of the subunits and tends to constrain creeping centralisation.[68] In view of the dominant position of the subunits, the centre has to rely on more cooperative strategies

[63] See Bachtiger and Steiner (2004).
[64] See Kriesi and Trechsel (forthcoming).
[65] Blondel (1998).
[66] See Blondel (1998); Papadopoulos, Y. (2005). Implementing (and radicalizing) art. I-47.4 of the Constitution: is the addition of some (semi-)direct democracy to the nascent consociational European federation just Swiss folklore? *Journal of European Public Policy* 12:3, pp. 448–467. Kissling-Näf, I. and Wälti, S. (2004), 'The implementation of public policies', in Klöti, U., Knoepfel, P., Kriesi, H., Linder, W., and Papadopoulos, Y. (eds), *Handbook of Swiss Politics*, Zurich: NZZ, pp. 563–600.
[67] An exception is of course the decentralised and regulatory agencies, such as the European Central Bank in Frankfurt. But these are specialised agencies which do not involve interactions with the Member State's citizens.
[68] On the EU, see Pollack, M. (1994) Creeping Competence: the Expanding Agenda of the European Community. *Journal of Public Policy*, 14(2), pp. 95-145.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

with the subunits. This provides a contrast with the more fully developed administrative, implementation and enforcement apparatus of the US federal bureaucracy, which is able to pursue independent policy action, even against the wishes of the subunits.

To summarise, the Swiss and the EU model of policy implementation and enforcement seriously limits the possibilities for creating powerful enforcement agencies. Once federal policies are agreed they are delegated back to the sub-units for implementation. Furthermore, the centre has limited power capabilities to enforce rulemaking or to implement policy measures directly within the sub-units. This logic of implementation by complete federal delegation not only serves to strength the subunits' discretion during the implementation process, but also provides the sub-units with an enhanced role during the policy formulation stage. The combination provides significant constraints on the 'power capabilities' of the centre in the EU and Switzerland *vis a vis* the US.

4. Selection of policy domain

Having contrasted similarities and differences among the three cases as a basis for a most-similar research design our attention can now be firmly focused on the policy dimension. In choosing a policy field it is crucial to select one that affects the three units of analysis in a broadly similar way. From a methodological perspective, the intended aim is to try to select a policy field that can serve as a parameter and thus be held constant across the cases. To the extent that this is possible, it would allow us to isolate the net impact of specific 'federal political institutions' on policy outcomes. Obvious policy field candidates include some of the systemic challenges such as globalisation, the environment, immigration pressures, macroeconomic performance etc., which could affect the cases in similar ways. In this dissertation I have opted to focus on a technology-induced challenge that is generating a high degree politicisation: the internet. But we shall need to further explicate this selection. One of the first problems that arise is that there is some uncertainty as to the boundaries of what exactly constitutes an

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

internet policy domain. With very little imagination it is an area that could be stretched to encompass many aspects of policy and political activity: from commerce, health and education to political participation, administration and even democracy. The problem of defining analytical boundaries to this admittedly fuzzy policy field is thus a difficult issue for comparative policy analysis. It is a problem that this dissertation will not attempt to address, although Chapter 4 does provide a contextual overview of the internet's trajectory as a policy issue and object of increasing politicisation. Instead, this dissertation's focus is on a number of internet-related issue areas that have become the subject of increased political contestation over the last decade. What links the diverse issue areas that are the subject of empirical investigation is that they have all been transformed by the new medium.

But a further narrowing-down of the policy challenge is in order. This is because policymakers can view the internet from at least two perspectives. The first sees the internet as a vital tool for enhancing, say, competitiveness, the efficiency of public administration, or civic participation. This calls for 'enabling' policy initiatives for establishing favourable regulatory environments that are conducive to innovation, administrative reform, or new channels of political communication. On the other hand, the Internet can also be seen from a second perspective. Whether it is in the form of provoking copyright infringement on an unprecedented scale, facilitating cyber attacks on critical infrastructures, disseminating child pornography, or permitting the unlawful collection of citizens' private data, the internet can also be seen as a vector for a series of external threats and/or negative challenges. Broadly speaking, therefore, one can distinguish between two types of policy modes;[69] 1) a *proactive policy mode* that aims to channel the positive aspects associated with the Internet and 2) a *reactive policy mode* that attempt to address the negative fallout. This dissertation is concerned with the second type, i.e. the reactive policy mode. The justification for this is linked to the fact that this type of policy challenge tends to require *authoritative* political resolution. Such

[69] This should not be confused with the distinction between "active" and "reactive" policy modes by Mayntz, R. and Scharpf, F.W. (1975), *Policy-making in the German federal bureaucracy*, Amsterdam: Elsevier.

DOI: 10.2870/1208

challenges are therefore unlikely to be left to market players or to epistemic communities of engineers and scientists for resolution. This is not to say that such actors are unimportant but, rather, it is to argue that the so-called reactive policy mode generally concerns politically sensitive issues, which, in turn, require the authority of the state. This is connected to an additional and theoretically relevant factor. In federal polities, the 'reactive' policy mode is likely to activate intense political conflict over issues related to internal security and, in particular, the operation of criminal justice systems. Such issues can trigger fundamental conflicts over the appropriate locus of government authority. From a Rikerian perspective, and as described in chapter 2, this would provide an ideal 'external threat' justification for federal policymakers to offer centralising solutions. As noted by scholars that have modified the Rikerian approach, rational (sub-unit) political elites engaged in strategic bargaining over the allocation of political authority will give up competencies in a given policy domain only when they are compelled to do so by some strong external pressure. This should create incentives for federal policymakers to try to frame the issue areas, to the degree that it is possible, in terms of the need to neutralise a dangerous external threat.

In sum, the empirical focus is on three (broad) issue areas that have been transformed by the internet: 1) data privacy, 2) copyright and 3) new forms of internet-induced criminality. All three issue areas generate significant 'internal security' problems and, in some cases, can even be framed as Rikerian type 'external threats'. Two of these (data privacy and copyright), however, also activate important 'market' related policy concerns. Despite the fact that the main focus is on 'internal security' dilemmas, this type of selection maximises the potential variance in the policy outcomes given that significant 'market' related regulatory factors are also at play. There is, however, an additional reason for why the research design has focused on issue areas that activate both 'market' and 'internal security' issues. This is directly related to the EU studies literature. As discussed in chapter 2, while comparative federalism approaches have been profitably applied to traditional regulatory areas, such as market regulation, environmental regulation, social regulation, it is much less the case for 'internal security' related forms of regulation. Thus, I have

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

largely opted for what George and Bennett refer to as a 'least likely' research design.[70] The logic behind this approach is that if theoretical propositions can be shown to work when conditions are least favourable for their validity, they are more likely to be valid in other circumstances as well. I have therefore chosen a 'tough' case for the EU (mostly involving police and judicial cooperation). It is one where the EU is 'least likely' to resemble another federal state. In this respect, the major part of the empirical analysis relates to issues connected to internal security in the three units of analysis. Such a tidy delineation between what are essentially overlapping issue areas is more difficult in practice however. An important focus of the empirical analysis will also incorporate 'market' type regulatory questions, an area where one could expect the EU to resemble other federal states.

The combined effect of the three issue areas is that they maximise the variance in the type of policy outcomes being studied. This is also theoretically justified because of certain purportedly unique features of the EU. Most notable among these 'unique' features is the EU's cross-pillar modes of policymaking. Since the three pillar institutional structure of the EU generates a number of distinct policy 'logics', the nature of political contestation, as well as the constellation of political actors, will vary greatly depending on whether one is addressing an internal market, justice and home affairs, or security policy issue area. Part of the aim of the present research design is, therefore, to try to incorporate many of these so-called distinct policy modes within the scope of the empirical inquiry. This is especially pertinent given that there is an implicit assumption in the EU variant of the policy modes literature that the EU is unique. Hence, a great deal of effort tends to be expended on identifying unique EU policy modes. The 'comparative' strategy pursued in this dissertation, however, parts from the

[70] Building on Eckstein, H. (1975), 'Case Study and Theory in Political Science' in Greenstein, Fred and Nelson Polsby (eds.), *Handbook of Political Science vol. 7: Strategies of Inquiry*, Reading MA.: Addison -Wesley, pp. 79-137 and the 'crucial case', George, A.L. and Bennett, A. (2005), *Case studies and theory development in the social sciences*, Cambridge, MA: MIT Press, use the concept of a 'least likely' research design which they argue is more relevant for the social sciences than Eckstein crucial case. The latter according to George and Bennett are difficult are rarely identified in social scientific inquiry.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

opposite standpoint and will allow us to observe whether similar policy modes can be detected in other federal polities.

5. Hypotheses

So far the focus has been on certain, specific features of a compound polity which can form the basis for a 'most similar case' research design and the selection of a specific internet policy domain. Our focus can now be directed towards generating a number of working hypotheses about potential relationships among some of the explanatory variables discussed above. The rationalist versions of new institutionalism, and their applications in the comparative federalism literature, are particularly pertinent to this endeavour. As discussed in chapter 2, many of these rationalist inspired federalist theories have tended to focus on institutionally derived incentives that shape strategic interactions among political elites from at least two levels of government. The emergence of new policy challenges with particular attributes, such as considerable cross-border spillovers, provide opportunities for federal policymakers to offer centralising solutions. Furthermore, from a Rikerian perspective, if such purported spillovers can be characterised in terms of an 'external threat' the likelihood of a transfer of political authority to the centre should increase. Whether or not this occurs, the issues are likely to generate intense disputes over the appropriate allocation of authority, activating, in turn, increased vertical interactions among the various levels of government.[71] This type of framework has provided the theoretical basis for a number of comparative federalism inspired policy analyses discussed in the previous chapter.[72] Drawing on the so-called rationalist comparative federalism literature this dissertation will investigate two claims: The first is that in view of the structural similarities among the three compound polities, similar policy dynamics will tend to be activated in response to a given regulatory challenge. This is especially the case where the policy issue has a high salience and potentially significant cross-border effects. Under these conditions, federal actors will have greater incentives to offer centralising solutions to common problems which can, in turn, trigger increased vertical

[71] See Kelemen (2002).
[72] Ibid.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

interactions among federal and subunit political elites[73]. As a result of these increased vertical interactions, however, the centre can eventually come to play a more prominent policy role. Thus, one of the major research goals is to investigate the extent to which similar policy dynamics, especially in relation to the strategic interactions among distinct levels of government, have been produced in the three polities.

The second claim relates to the way in which conflicting demands are mediated within the three compound polities. Although the mobilisation of political actors, and the vertical interactions among them, may exhibit similarities, the way in which conflicting interests are typically mediated varies among the polities. As noted above, decision-making and implementation/enforcement processes differ quite markedly as a result of variations in the 'power capabilities' of the centre. At this stage it is important to further define the notion of 'power capability'.[74] The concept is used here as an analytical device for comparing the three political systems. In this regard, it should be noted that although pronounced variance in the 'power capabilities' among the sub-units exist *within* the three units of analysis, and is a common feature of federal polities, the empirical focus of this investigation is *not* on the sub-units. Instead, the focus is on variations in the 'power capability' of the *centre* across the three units of analysis. By 'power capabilities' of the centre I refer to a) the ability to create federal agencies/departments independently of the consent of the sub-units and b) to endow such agencies/departments with effective implementation and/or enforcement powers that, in some cases, can even allow the centre to undertake regulatory/enforcement actions within the sub-units themselves. Thus, the research goal is to examine the extent to which differences in decision-making processes and the

[73] See Kelemen (2004)

[74] The concept is used in international relations theory (e.g. neo-realism) to distinguish between power asymmetries among nation states and it is this variance that explain differences in international outcomes. It has also been used in European integration theory (Schmitter) and applied to power asymmetries among the member states'. For a discussion of power analysis and the concept of power capabilities in internantional relations theory see Guzzini, S. (1993), Structural Power: The Limits of Neorealist Power Analysis International Organization, 47: 3, pp. 443-478. Krasner S. (1982), Regimes and the Limits of Realism: Regimes as Autonomous Variables, *International Organization* 36:2, pp. 497-510; Krasner, S (1999) Sovereignty: Organized Hypocrisy, Princeton University Press; For an application to European integration see Schmitter, P. and Kim, S. (2005) The Experience of European Integration and the Potential for Northeast Asian Integration, *Asian Perspective*, 29(2): 5-39.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

implementation/enforcement powers of the centre affect policy outcomes in internet related issue areas.

These research goals can now be stated in the form of two working hypotheses to guide the empirical investigation.

Hypothesis 1: Where a policy field has significant cross-border effects there will be greater opportunities for centralisation and the more likely federal actors will be mobilised to offer centralising solutions. As a result of increased interactions among the various levels of public authority around a specific policy field, the centre may be able to take on a more prominent policy role.

Hypothesis 2: Where the 'power capabilities' of the centre are dependent on the resources or the consent of the sub-units, the subunits are more likely to retain important discretionary powers while delegating only coordinating functions to the central level. Where the 'power capabilities' of the centre are strong, the centre can be more responsive to policy challenges, and is able to implement and enforce policy measures independently of the subunits. Under such conditions a greater scope for implementing centralising measures exists.

6. Methodology

Comparative analysis through in-depth qualitative case studies is the research methodology adopted in this dissertation. It has been one of the major research methods of the social sciences and tends to be particularly well-suited for making inductive discovery, especially in the context of a relatively small number of cases. Furthermore, a qualitative methodology, such as the one adopted in this dissertation, is understood as following an explanation route. This is what Ragin et al have in mind when they define qualitative methodology as the focus on the 'presence or absence of specific characteristics or specific configurations of characteristics pursued by means of systematic comparison of multiple cases' with the aim of 'identifying broad conditions for the occurrence of particular outcomes'.[75] The latter is to be

[75] Ragin et al (1996) pp 752

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

distinguished from qualitative *techniques* such as discourse analysis, ethnographic participant observation or hermeneutics.

A qualitative methodology also has to be distinguished from what Ragin et al refer to as the 'many cases, few variables' type research of conventional quantitative methods.[76] This research methodology is ill suited, however, to the 'many variables, few cases' type research pursued in this dissertation.[77] In fact, thus far we have identified a very limited universe of three cases that conform to our definition of a 'compound polity'. The selection of cases has therefore been preceded by an extensive theoretical review of the state of the art in comparative federalism in chapter 2. On this basis, it has been possible to reduce the universe of cases in this chapter by establishing a narrower area of homogeneity among the three compound polities. In doing so, I have taken into consideration the Ragin et al's argument that the 'inclusion or exclusion of any single case may significantly alter the researcher's conclusions' and that no case should be ignored as negligible outliers[78]. This has provided the main justification for adding the Swiss case to the more popular EU and US comparative research design. The research design is therefore of the 'most similar' type and parts from the simple idea that similar outcomes follow from similar causes.

Methodologically, the aim of most similar case designs is to systematically match and contrast cases in order to identify common features and isolate variables that may be linked to particular outcomes. A number of similarities among certain key structural variables of the three compound polities have been identified. But attention has also been drawn to major differences regarding how competing interests are processed in each of the polities. This type of research lends itself to the qualitative research methodology of process tracing.[79] The core of this approach is the attempt to identify a casual chain of events by tracing the sequence of steps leading to particular

[76] Ragin et al (1996).
[77] Ibid.
[78] Ibid., 752.
[79] George and Bennett (2005).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

outcomes through a process of 'redescription'.[80] The aim of process-tracing is to elaborate a *structured* set of questions for each of the case studies, on the basis of a *focused* theory.[81] Each of the in-depth case studies address the same structured questions: 1) which actors have been mobilised? 2) how have their demands been mediated within their respective institutional settings and, in particular, what has been the nature of the strategic interactions among distinct levels of government? 3) what is the form of the emerging policy regime, especially in terms of the regulatory capabilities of the centre?

By answering these questions we will be able to examine the first guiding hypothesis as to whether actor mobilisation has taken similar forms in the three compound polities. It will also provide a test for the second hypothesis as to how the institutional setting, in particular purported variations in the power capabilities of the centre, has affected the specificity of policy outcomes.

There is one final methodological question that needs to be addressed. It concerns the interaction effects among units of analyses. Known as Galton's problem in the methodological literature, it raises important questions about cross-national research strategies. This is largely because comparative analysis is predicated on the assumption that outcomes in the units of analysis can be explained by the *internal* characteristics of the units alone. However, in the context of a high degree of interdependence among units of analysis the behaviour of each is related to the behaviour of others. As Milner has argued, this is a problem that is accentuated when dealing with the internet.[82] This is not to argue that outcomes cannot be explained by the *internal* characteristics of the three units, or that internal/domestic factors may account for far more variance than interaction effects, but rather to be explicit about the basis of interaction rather than simply acknowledging its presence.

[80] Ibid.
[81] Ibid.
[82] Milner, H. (2002) The Global Spread of the Internet: The Role of International Diffusion and Domestic Political Institutions in Technology Adoption. Paper presented at conference on "Interdependence, Diffusion and Sovereignty," held at Yale University, May 10-11, 2002.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

The research method adopted has been a function of the available sources of data. Three principle sources of data have been used 1) official documentation, 2) expert interviews, and 3) the submission of opinions by interest groups during consultation procedures. Where it is appropriate, secondary sources have been used. Official documentation includes legislative documents, policy proposals, Green Papers, White Papers, speeches by relevant representatives and studies that are published by the governments in the three cases. All of these have been an important data source since the governments of each polity have a tradition of stimulating debate with concerned parties before every major legislative proposal. This is done by submitting consultative papers, memorandums stating objectives, and in many cases, by holding hearings that bring together interested parties. Such proceedings provide an extremely useful data source. Another important source includes secondary sources such as the national press and specialised trade journals all of which provide a valuable tool for reconstructing the policy context. Further data has been acquired through in-depth interviews with officials and other participants. Such interviews are usually referred to as in-depth, elite interviews which benefit from the fact that the individuals are well informed experts selected on the basis of their expertise. Where possible I have tried to use more than one method of data collection by combining the analysis of official documentation, consultation documents, secondary sources, and in-depth interviews, in order to reconstruct the processes.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Part II Empirical Analysis

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 4 The politicisation of the internet

This chapter examines how the spectacular growth of the internet, particularly over the last decade, has helped to create a valuable new international resource. Following Douglass North, this is understood as a change in the incentive structure, which, in turn, has triggered the sudden politicisation of a new resource.[1] It is this dynamic that, in large part, has provoked the differential mobilisation of political actors within the three political systems that are the focus of the empirical investigation. To this end, this chapter seeks to understand the internet's politicisation by identifying a series of 'critical junctures' in its technological trajectory and some of the most prominent actors involved in the process. The choices made by this constellation of actors were not politically neutral and have created a series of 'lock in' effects that constrain the regulatory options of policymakers. This chapter therefore provides the contextual backdrop to the in-depth case studies that follow in subsequent chapters.

1. The three internet political arenas

In order to analytically describe when the politicisation of the internet occurred, and how it became a salient policy issue in the three polities under investigation, it will be necessary to track some of its earlier history. The internet's politicisation may be a relatively recent phenomenon, occurring over the course of the last decade, but its evolution during the past forty odd years has been anything but *apolitical*. To make sense of the present politicisation, it is fundamental to keep in mind its connection with the past and, in particular, the subtle interactions between technological innovations, the strategies of key actors and their organisational settings, as well as the institutional context in which they operated. The argument advanced below is that during the 1990s a 'multiple politicisation' of the internet occurred, whose effects are presently constraining political actors' policy options and strategies. To make sense of such a complex and multifaceted process as the internet's

[1] See North, D. (1990). *Institutions, institutional change and economic performance*. Cambridge: Cambridge University Press.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

politicisation three interacting *political* arenas will be identified.[2] It is in these arenas where I shall argue that the struggle to define and create the rules that shaped the internet's regulatory regime has historically taken place. Each of these political arenas has operated according to a distinct logic and involved a multiplicity of public and private actors in their various roles and capacities. By specifically focusing on the *political* dynamics surrounding the internet's development, it will become clear how, in the mid-1990s, the three political arenas identified below intersected with one another to produce a 'multiple politicisation' of the internet as a governance, regulatory and political challenge.

1) The Navigation Arena; This arena is concerned with the internet's technical architecture. It is the abstraction behind our digital screens and consists of an underlying technical and communications architecture that uses a common set of standards and protocols to connect computers around the globe. This architecture has been built by technicians and software engineers. However, this has also involved choosing amongst competing technical standards, protocols and applications. It is in this arena, populated by 'epistemic communities' of software engineers and technicians, where historically much of the behind-the-scenes politics that have shaped the present internet architecture have taken place.[3] The internet is essentially a "network of networks" whose underpinnings are formed by the interconnection of myriad independent computers and information systems. The initial challenge was getting these computers to 'talk to each other'. Furthermore, it was somehow necessary for the computers to be able to 'understand' each other. This, in

[2] This conceptualisation draws on a number of authoritative accounts by historians, political scientists and sociologists who have studied the evolution of the internet and its subsequent politicisation. In particular are the detailed histories provided by the historians Roy Rosenzweig and Richard Griffiths. Political scientists such as Robin Mansell, Mitlon Mueller, and Marcus Franda have also drawn attention to the political aspects of the internet's evolution, as well as Manuel Castells seminal three tome volume on the Information Age. See bibliography for complete references to the literature.

[3] The notion of 'epistemic communities' is developed in Haas, Peter M, (1992) Introduction: Epistemic Communities and International Policy Coordination. *International Organization*, 46:1 pp1-36

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

very simplistic terms, was the challenge that confronted the epistemic community of engineers operating in the navigation arena.[4]

The evolution of the internet in the navigation arena was, in this way, shaped by the above challenge. The response was to draw on an underlying technology of 'packet switching' (this built upon advances in the field of telecommunications) while special standards and protocols (known as TCP/IP) helped establish a 'lingua franca' for computers to understand each other. The key actors operating in this arena consisted of an epistemic community of engineers[5] driven by multiple passions and, in particular, by libertarian political ideologies.[6] Nowhere was this more apparent than in the evolution of the open TCP/IP standard, or more recently the 'open source software' movement, all of which can trace their lineage back to a particular political climate in which an anarchistic predilection among young engineers towards 'openness' and in terms of a distrust of hierarchy, was to have a powerful influence in shaping the trajectory and evolution of the internet.[7] These anonymity-enhancing features of the internet are what presently cause so many problems for the effective regulation of cyberspace.

2) The User-end Arena; The politics of this arena could be viewed as concerning the supply and demand for rules that govern how users interact with the informational content on their screens. It consists of an information system that allows for the creation and storage of, as well as access to, a wide range of information resources. In fact, it is the 'user end' we are engaged with when connecting to the Internet and which many people refer to as 'cyberspace'. A variety of grass-root communities, with varying interests and passions, have shaped this sphere. But there is also a public dimension to the user-end, both in terms of the supply of public goods and the demand

[4] Kahn , Robert and Cerf Vint (1999) What Is The Internet (And What Makes It Work) Available at: http://WWW.Internetpolicy.org/briefing/12_99.html

[5] Hafner, K, Lyon, M. (1996) *Where wizards stay up late: The origins of the internet*. New York, NY: Simon & Schuster.

[6] Barbook, R. and Cameron A. (1996), The Californian Ideology, *Science As Culture*. 26:6 Part 1, pp. 44-72.

[7] Jordan, T (2001) Language and Libertarianism: The politics of cyberculture and the culture of cyberpolitics. *Sociological Review*. 49 (1), pp1-17.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

for technology. Historically, the main actors operating at this level have been the grass-roots communities of 'netcitizens', researchers and policymakers. Two types of actors, public and private, can be identified at the user end. One of the principal actors during the internet's formative years was the US defence sector. On the one hand, it played a key role on the supply side by providing huge subsidies and, on the other, a hungry market for research outputs which, in turn, fed the demand side. However, the defence industry was not the only community shaping the evolution of the Internet. A second major actor was the National Science Foundation (NSF), which in 1986 decided to build a network called NSFNET. Most importantly it adopted the TCP/IP protocol to link the science and research communities. The creation of NSFNET was dramatic and encouraged a surge in the usage of the Internet and, as a result, incorporated a large section of the research community in the use of high-speed networks. Within a few years the newly expanded NSFNET had become the primary backbone component of the Internet and by 1990, the military sponsored network had been decommissioned.[8]

The political interactions taking place within the *user-end* arena involved both top-down processes, whereby public actors supplied financial resources and demanded technological outputs, and a bottom-up process, involving a steadily growing and influential grass-roots community of private actors. This creative tension remains to this very day. In fact, many specific features of the internet's development can be traced back to the interactions among these two types of actors and the negotiated compromises concerning the choice of standards and the organisational formats adopted.

3) The Off-line Arena; This arena captures the way in which the internet can affect offline behaviour and, conversely, how the offline context also influences the internet architecture. This dialectic, from the security dilemmas of a bi-polar international order to issues of national industrial policy, has had a significant impacted on the development of the internet. To this end, the Cold War security concerns and the competitive environment of the

[8] The role of the NSF is discussed in detail by Mueller (2002).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

international political economy provided an essential contextual backdrop to the Internet's development trajectory. The nascent space race in which the USSR had been first in launching a spacecraft into orbit, gave a major impetus for the creation of a leading technological think-tank, the Advanced Research Projects Agency (ARPA) within the US Department of Defense. Although most of its work was geared towards ballistic missile and nuclear test monitoring, ARPA had as one of its major objectives the development of a communications network that could survive a nuclear attack.[9] This brought us the technological breakthrough of packet switching which is at the core of the Internet. This Cold War research context was also characterised by a constellation of positive factors, in particular an especially favourable R+D environment.[10] The massive subsidisation of R+D by the US federal government may also have played a part in destroying foreign competition. In fact, one of the crucial reasons why TCP/IP became the *de facto* standard was not unconnected to events in the international political economy. During the 1970s, a 'protocol war' emerged in which European telecommunication companies had pushed for their own alternative standard, known as x.25, as a rival to TCP/IP.[11] Nevertheless, given the enthusiastic support of the US military and, more importantly, their adoption of the standard, the victory of the TCP/IP protocol was ensured over its European rival.[12] It may go some way into explaining the US dominance of the Internet that, in many contemporary accounts, is conveniently overlooked when praising the marvels of the US free market as an incubator for innovation.[13]

2. Multiple Politicisation: The internet from the mid-1990s

Thus far I have argued that the internet's short history has been anything but *apolitical*. Up until the 1990s, the internet's history had an important political

[9] See Griffiths (2002).

[10] See Rosenzweig (1998).

[11] See in particular the discussion by Werle, R. (2001) Internet @ Europe: Overcoming institutional fragmentation and policy failure. *European Integration Online Papers*. 5(7).

[12] See in particular Norberg, A. and O'Neil, J. (1996), *Transforming Computer Technology: Information processing for the Pentagon, 1962-1986*, John Hopkins University Press: Baltimore.

[13] This is the argument advanced by Cohen, S., Delong B., and Zysman J. (2000), Tools for Thought: What is new about the 'E-conomy', *Berkeley Roundtable on the International Economy* (Working Papers 138).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

component where distinct but interacting political arenas shaped the development of this new information and communication medium. It is a uniquely fascinating story from the connection of 4 host computers in the late 1960s and the first public demonstration of email in a computer conference in 1972, to the development of the World Wide Web (www) in the early 1990s.[14] We can now focus on the 'multiple politicisation' of the arenas that occurred during the mid-1990s.

2.1 Politicisation of the navigation arena

Until now, most of our attention has been squarely focused on developments taking place in the US. We can now turn to technological developments concerning the navigation arena that took place in Europe, and more specifically in Switzerland. In 1991, scientists at the CERN research centre in Geneva released the World Wide Web (www). The technological stage was now set for the prolific expansion of the internet. The key to the web was a simplified protocol for writing addresses and calling up documents for viewing known as Hypertext Transfer Protocol (*http*, the familiar prefix at the beginning of many web site addresses). Behind the scenes, a simplified system known as Hypertext Markup Language (html) allowed for links to be activated at the click of a mouse creating the sensation and, indeed, the reality, of a seamless web of information.[15] Following the public release of the web program in 1993, a group of US students launched Mosaic, the first Internet browser. It incorporated many of the features that are familiar to users of Netscape (the commercial version of Mosaic) and Internet Explorer today. Up until the development of the web and the web browser, the internet had been primarily used by the scientific and academic community. With the advent of the web, however, the floodgates for the proliferation of the internet were thrown wide open. The timing was also crucially important. It occurred in a context of growing household computer penetration at the user-end and an increasing capacity in the telecommunications infrastructure.[16] All in all, the right

[14] For an economics approach to the internet's evolution see Hutter, M. (2001), Efficiency, viability and the new rules of the Internet, *European Journal of Law and Economics* 11(1):5-22. A historian's approach is offered by Griffiths (2002).

[15] This is how the inventor of the web of describes it. See Berners-Lee, T (1996) The World Wide Web: Past, Present and Future, available at: http://www.w3.org/People/Berners-Lee/1996/ppf.html

[16] See Cohen, DeLong, and Zysman (2000).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

conditions were in place for the web to take-off and, in doing so, become the subject of intense politicisation.

Nevertheless, although the technical availability of the web was a necessary condition, it was not a sufficient one for the take-off phase. It still relied on the internet architecture for diffusion and this was heavily conditioned by the political context in the US. In the early 1990s, the internet architecture was becoming the object of increasing politicisation in the US.[17] We have already noted how the expanded NSFNET had become by 1990 the primary backbone component of the Internet. But as the Internet began to grow in the early 1990s, especially outside of the academic and research communities, business began to express a greater interest in its development. With growing commercial interest being expressed in the management of the Internet backbone, the argument that responsibility for the management of the Internet's backbone should be privatised began to take hold.[18] The stage was set for allowing the private sector to take a more prominent role. In 1991, Al Gore, at the time a U.S. senator, proposed widening the architecture of NSFNET to include more schools and community colleges. The resulting legislation expanded NSFNET and renamed it NREN (National Research and Educational Network). Crucially, the new legislation[19] also allowed businesses to purchase part of the network for commercial uses thereby spawning a new industry, Internet Service Provision. This new industry would play a major role in the regulatory battles that subsequently unfolded and are examined in the following chapters. By 1995, the NSF had effectively ceased its support for NSFNET and commercial networks were now performing the task. The era of 'commercialisation' had begun.[20]

But there was more to the politics of the navigation arena than the backbone. Largely as a result of the commercialisation of the Internet, various regulatory agencies, international organisations, task forces and standard setting

[17] See Mueller, M. (2000), Technology and Institutional Innovation: Internet Domain Names. *International Journal of Communications Law and Policy*. Summer (5) pp731-760.
[18] See Mueller (2000).
[19] See the High-Performance Computing Act of 1991.
[20] See the book-length treatment of this topic by Mueller (2002)

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

agencies also began to play a more prominent role in the politics of the navigation arena.[21] What was at stake in this crucial navigation arena was not only how the internet was presently managed but, crucially, how it would be managed in the future. While this may have been relatively easier during its formative years, the internet's transnational nature was to ensure that it would remain the subject of increasing political contestation among users, bureaucracies, governments and international organisations. In terms of periodisation, the year 1995, although an arbitrary date, marked a crucial juncture in the take-off phase of the Internet. It was in 1995 that the NSF stopped running the Internet backbone and its function was taken over by private firms. It was also the year in which the Web became popularised following the commercial availability of the Netscape browser and the year in which the US government allowed a private contractor to register domain names. Moreover, new actors, such as certain commercial entities and international organisations, were newly empowered while the influence of others was effectively marginalised[22].

2.2 Politicisation of the user-end

Developments in the navigation arena - technical innovations such as the Web, a commercially available user-friendly browser and a growing institutionalisation of the internet's governance structure- were aided by a favourable policy environment, which included a growing penetration of computers into the home and office and an increasingly liberalised and deregulated telecommunications sector in the world's major economies. The telecommunications sector, in particular, became the subject of increased policy activity in the three polities under investigation with a significant impact on the user-end. Reform of the telecommunications sector through a process known as 'local loop unbundling' was deemed a crucial aspect for the increased uptake of the Internet, especially in Europe. Yet, after the wave of

[21] A plethora of specialised international organisations, many of which operate under the auspices of the Internet Society (ISOC), dominate the politics of the navigation arena. This is particularly the case with the Internet Engineering Task Force (IETF), which comprises hundreds of specialised working groups and plays a central role in the standard setting process. Other important bodies with an interest in the standard setting process are the International Telecommunications Union (ITU), the Organization for International Standardisation (ISO) and the World Wide Web Consortuim (W3C).

[22] This was the case for military interests for instance.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

privatisation and deregulation in the telecommunications sector during the 1980s, the former state monopolies still kept control of the 'local loop' or the last mile connection between the local exchanges and the domestic phone user. In fact, one of the principal objectives of liberalising the last mile was to open up the way for high speed Internet access for domestic or small businesses operating at the user end. Since the local loop determined the cost of Internet access, ie the cost of local calls, this, in turn, could influence the level of Internet penetration in a country.

The US was the first to address the 'unbundling' (i.e. freeing up the last mile) issue. Twelve years after the historic break up of AT&T in 1984, US lawmakers passed the 1996 Telecommunications Act which laid the groundwork for breaking up the remaining local networks –the so-called Baby Bell carriers- and contained central provisions for local loop unbundling. Events in Europe were more complicated. In the EU during the course of the 1990s, the Commission in partnership with the member states had begun to bring about a common market for telecommunications.[23] However, many aspects, such as the local loop, were controlled by former national monopolies. Following the passing of various EC directives a milestone for liberalization was set for 1 January 1998. As the date came and passed, the EU telecommunications sector was, at least on paper, fully liberalised.[24] But many gaps remained, especially concerning the local loop. By stressing the urgency, and playing on fears of technological lag, the Commission was able in 2000 to pass a regulation forcing the incumbent operators to open up local loops by January 2001.[25]

[23] Thatcher, M (2001) The Commission and national governments as partners: EC regulatory expansion in telecommunications 1979–2000, *Journal of European Public Policy*, August 2001, vol. 8, no. 4, pp. 558-584(27).

[24] See Kiessling, T and Blondeel, Y (1998) The EU regulatory framework in telecommunications. A critical analysis, *Telecommunications Policy* 22 (7) pp. 571-592.

[25] By choosing a regulation instead of a directive it was able to introduce the legislation for unbundling in record time, just 6 months between the regulation being first proposed and it being introduced, that is taking effect. A directive would have taken possibly two years and additional time to be transposed into national law. See Regulation 2887/2000/EC of the European Parliament and of the Council On Unbundled Access to the Local Loop.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Developments in Switzerland literally followed the EU rhythm of liberalisation. Beginning in the early 1990s and culminating with a new Telecommunication Law in 1997, Swiss telecommunications policy was thoroughly reformed.[26] In line with developments in the EU and the US, the Swiss telecommunication act established new regulatory agencies and broke up former monopolies. However, the most notable point about developments in Switzerland is how the policy schedule was hugely affected by the EU agenda. Swiss regulators fully internalised the EU schedule for liberalisation and were able to effectively marginalise vocal domestic opponents to reforms.[27] Some analysts have referred to an indirect 'Europeanization' of Swiss telecommunications policy through self-imposed EU deadlines and by passing EU-compatible regulations.[28] In sum, telecommunications reform was an important area that underlines the interaction between the navigation and the user-end political arenas. Although it is related to important infrastructure aspects it has had significant user-end implications in terms of the cost of Internet access.

But there was more to the regulatory problematique than simply getting citizens connected to the Net. These policy challenges were increasingly identified in numerous policy papers, which stated policy positions, government strategies, and major issue areas to be addressed. Most policy documents were framed in terms of the emerging 'information society' and how to cope with the new challenges it was unleashing. One user-end issue area, which was the subject of much media attention, was the new potential for e-commerce. At the time, the concept of e-commerce was used to refer to a number of different and overlapping issues. In April 1997, the Commission published its 'European Initiative in Electronic Commerce'.[29] It provided a framework for action to create a favourable legislative framework, to enable access to infrastructure and technology, and to improve the business and

[26] Mach, A. Hausermann, S. and Papadopoulos, Y (2003) 'Economic regulatory reforms in Switzerland: adjustment without European integration, or how rigidities become flexible', *Journal of European Public Policy* 10:2 pp.301–318.

[27] See Mach et al (2003)

[28] Sciarini, P, Fischer, A, Nicolet, S (2004) How Europe hits home: evidence from the Swiss case. *Journal of European Public Policy*, Volume 11:3 pp. 353-378.

[29] See the European Commission's Communication: *A European Initiative in Electronic Commerce*, COM (97) 157.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

consumer environment. It was followed in June 1997 with a much quoted White House political initiative 'The Framework for Global Electronic Commerce.'[30] The Swiss Federal Council followed with its own broader 'Strategy for an Information Society' in February 1998, in which e-commerce figured as one of the major issues to be addressed, requiring the introduction of digital signatures and other security and confidence enhancing measures for the anticipated uptake of internet commerce.[31]

But these were not merely policy statements generated for domestic audiences. They should also be seen as strategic policy statements outlining the international agenda for negotiation.[32] This is especially the case for some of the major EU and US policy initiatives. One of the most salient differences concerned the role of government, with US policy statements usually couched in more market-friendly terms than the EU. These differing views as to the role of public policy actors will, no doubt, ensure that regulatory differences will continue to persist. Swiss policy statements also made for some subtle differentiation. Contrary to the personalised initiatives of the US and the EU, the Swiss preferred a low key approach as the Federal Council put it, its strategy ' *n'est pas non plus personnifiée comme c'est le cas par example aux Etats-Unis (Clinton et Al Gore) ou dans l'UE (Bangemann)'.* [33]

There is therefore considerable scope for differences which, in turn, affects issue framing and policy definition by policymakers in their respective political arenas. During the late 1990s as the 'internet' became the subject of heightened media and public attention, many hyperbolic statements were made by governments and policymakers concerning, for instance, the potential for e-commerce. Nevertheless, despite the hyperbole, difficult questions related to the type of rule structures that would eventually come to

[30] See the White House (1997) *A Framework for Global Electronic Commerce*. Avaialble at http://usinfo.state.gov/journals/itgic/1097/ijge/gj-12.htm

[31] Strategy of the Federal Council for an Information Society in Switzerland, Decision 18 February 1998. Also available from http://www.infosociety.ch/site/default.asp?dossiers=106.

[32] Bar, F and Murase, E (1997) The potential for transatlantic cooperation in telecommunications service trade in Asia. *Berkeley Roundtable on the International Economy*. 1997(Working Paper 108).

[33] See pp4 of the Strategy of the Federal Council for an Information Society in Switzerland, Decision 18 February 1998. Also available from http://www.infosociety.ch/site/default.asp?dossiers=106. 4

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

regulate how users interacted with the abstraction in front of their digital screen needed to be addressed. New legal and regulatory questions related to, for instance, intellectual property rights, the protection of personal electronic data, consumer rights and legal liability with regard to e-commerce etc., needed resolving and became the subject of domestic political contestation. Many of these regulatory issues will be examined in greater detail in the case studies that follow. In addition to the new regulatory dilemmas, the user group had also been radically altered, from a largely specialised community of researchers and engineers, to a digitally connected international civil society that could now mobilise even at the transnational level.[34]

2.3 Politicisation of the offline arena

The internet's effects were not restricted to what occurs at the user end, or even within the navigation arena. In fact, the internet's impact on the offline arena has also dramatically increased since its take off in 1995. Internet related criminality offers one of the best examples of how the new medium affects the offline political arena. Since issues related to internet criminality are the subject of the following empirical chapters, this section will focus on a crucial contextual backdrop to the in-depth case studies that follow. It will serve to neatly illustrate the international level politicisation of the internet's offline effects.

At the same time as policymakers were proactively engaged in implementing 'enabling' type initiatives to establish favourable regulatory environments for user-end activities during the mid-1990s, government officials were meeting in an international forum in an attempt to draw up a multilateral treaty to address the new threat of internet related criminality. Although various international organisations, including the OECD, the G8 and the United Nations, had been working on issues related to cybercrime, some of the most important multilateral coordination took place at the Council of Europe (CoE). In

[34] Della Porta, D and Mosca, L (2005) Global-net for Global Movements? A Network of Networks for a Movement of Movements. *Journal of Public Policy*. 25 :1. pp165-190.

DOI: 10.2870/1208

February 1997, the Council of Europe created a Committee of Experts on Crime in Cyberspace to draft a binding legal document on cybercrime. Officials from 45 countries including Switzerland, the EU[35] and its member states, and the US were involved in drawing up a draft Convention between April 1997 and April 2000. Although the US is not a member of the Council of Europe, it was a signatory and a key driving force behind the Convention (other non-European countries which have signed the treaty include Canada, Japan and South Africa). The Convention[36] set itself apart from what was occurring in other international forums such as the G8, OECD and the United Nations due to its binding nature. Just as the foundation of ICANN –the internet governing board- in 1998 has been referred to as the 'constitutional convention' of the navigation arena,[37] the Council of Europe Convention on Cybercrime, which entered into force in July 2004, constitutes one of the first attempts to specifically address negative externalities in the offline arena via an international Convention on Cybercrime.

The Convention is based on the premise that the risks related to cybercrime and its offline effects need to be addressed at the international level. But, when the text was released in April 2000,[38] it prompted an immediate flurry of protest from civil liberties organisations and Internet businesses as well as other interest groups. The aspects of the treaty which were most politically controversial related to the section that dealt with procedural law, i.e. interception of communications and seizure of computer data by governments. Civil liberties organisations across the globe were immediately mobilised and condemned the unbalanced nature of the treaty's very detailed procedures for interception and seizure mechanisms and lack of corresponding limits to government powers.[39] For instance, the Centre for Democary and Technology, a respected US civil liberties organisation,

[35] The European Commission participated in the negotiations, although, of course, the EU is not a signatory to the Convention.

[36] See the Council of Europe -ETS 185-Convention on Cybercrime available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[37] See Mayer, F. (2000), Europe and the Internet: The Old World and the New Medium, *European Journal of Internation Law* 11(1), pp. 149-169.

[38] Available at http://conventions.coe.int/treaty/en/projets/cybercrime.htm

[39] See Giacomello, G. and Mendez, F. (2001), ‘‘Cuius Regio, Euis Religio, Ominum Spatium?’’ State Sovereignty in the Age of the Internet. *Information and Security.* 7 pp15–27.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

captured the prevailing mood by pointing to the paradoxical nature of the draft which is not "focused on viruses, hacking or other attacks against computer systems or the computer-dependent critical infrastructures. Instead, central provisions of the treaty are intended to require governments to adopt laws on search and seizure of computer evidence, disclosure to governments of computerized records of any kind, and electronic interception of communications—*for all kinds of crimes*." [40] In other words, the major focus of the treaty was on enhancing the investigative powers of law enforcement agencies. These policy battles, which were simultaneously being played out within the three polities under investigation, will be systematically addressed in chapter 7. The main point to underline, therefore, is the multi-level nature of the policy disputes around this particular issue area.

3. Summary

This chapter has argued that what happens behind and in front of the digital screen has a significant impact on the offline world and these issues, as some of the examples above demonstrate, have been the subject of increased politicisation. The Cold War concerns of the internet's formative years have been replaced by new security concerns. National security specialists, especially in the US, have been quick to identify new threats, in the form of cyberterrorism and information warfare, which are capable of inflicting massive physical damage on the economy or on vital public services.[41] On the other hand, law enforcement agencies, aided by the media, have warned parents of the paedophiles lurking in 'chat rooms' attempting to lure minors into real world meetings or of the dangers of cyber criminals stealing personal identities and bank accounts details. The offline effects, especially in the case of cybercrime or cyber terrorism, have been accentuated by a heightened media attention that has merged two little understood spheres –technology and crime. In the mid-1990s many of these elements, in particular the

[40] See the letter from the Center for Democracy and Technology (CDT) to the CoE. http://www.cdt.org/international/cybercrime/010206cdt.shtml

[41] See Bendrath, R. (2001), Cyberwar debate: Perception and politics in US critical infrastructure protection, *Information and Security* 7, pp. 80–103.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

interactions between the three political arenas came together to produce a 'multiple politicisation' that is explored in the next four chapters.

The aim of this chapter has been to emphasise the diversity of interests and the specific cultural and institutional factors that shaped the internet's evolution. In particular, it has sought to capture the multiple interactions between the navigation, user-end and offline political arenas. Put simply, the choices made within each of these distinct political arenas have reverberated across the entire system. Moreover, the choices that have been made were not politically neutral and certainly did not arise 'spontaneously'.[42] Instead, they were consciously shaped and were the result of the power exercised by individuals, firms, governments and other interest groups. The best summary, is perhaps left to an historian for whom

> "[s]uch a profound and complex development cannot be divorced from the idiosyncratic and personal vision of some scientists and bureaucrats whose sweat and dedication got the project up and running, from the social history of the field of computer science, from the Cold Warriors who provided massive government funding of computers and networking as tools for fighting nuclear and conventional war, and from the countercultural radicalism that sought to redirect technology towards a more decentralized and non-hierarchical vision of society"[43]

As the internet's impact shifted across the political arenas during the mid-1990s and began to capture the public imagination, it acquired a distinctive political significance. The new 'hot issue' advanced on the international and domestic political agenda in an environment of changing issue definitions and heightened attentiveness by the media and broader publics. By the late 1990s, a multiple and reinforcing politicisation of the three political arenas described above was well underway producing the within-case political mobilisation that is the subject of the next four empirical chapters.

[42] See Mansell and Silverstone (1996).
[43] See Rosenzweig (1988), pp 1552.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 5: Data Privacy

Governments have had a rather long tradition of regulation in the area of privacy and personal data protection, with the first wave of reform in most western legal systems emerging in the 1970s and 1980s. The legislation was largely a reaction to the new threats to privacy caused by the expanded possibilities for collecting, storing and transmitting data via information technologies. Data protection laws were enacted and have since been constantly revised and updated with the aim of protecting citizens' right to privacy.[1] The explosion of the internet in the mid-1990s accentuates this old policy problem that has traditionally pitted civil liberties groups against government for decades. Nonetheless there have been shifts that alter the fundamental nature of the problem.

Part of the goal in dealing with the old policy problem was to prevent abuses by the public sector. In recent years, however, the commercial organisation has increasingly replaced the national government as one of the largest potential threats to data privacy. Corporations tend to be better at data processing than public sector organisations and are subjected to limited public control. It thus became clear that the safeguarding of privacy within the data protection area also had to consider the multitude of private computer systems and establish a difficult balance of interests between the privacy interests of data subjects and the economic freedom of the holders of personal data.[2] The other part to the data privacy problematique relates to government surveillance for internal security purposes. In recent years, and especially in the post-9/11 policy context, access to citizens' data, much of it stored in cyberspace by both public and private organisations, is perceived to be an important tool for addressing the terrorist threat as well as for general crime-fighting purposes. Taken together, these policy dilemmas reveal a

[1] For an authoritative overview see in particular Bennett, Colin (1992). *Regulating privacy: data protection and public policy in Europe and the United States*. Ithaca : Cornell University Press; Bennett, Colin and Raab, Charles Raab (2003) *The Governance of Privacy: Policy Instruments in Global Perspective*. Ashgate

[2] See the report commissioned by the European Commission by Sieber, U. (1998), Legal Aspects of Computer-related Crime in the Information Society. COMCRIME Study.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

striking paradox: political authority is both the solution and the problem in relation to data privacy.[3] To address the threat to one's privacy as a result of unfettered information gathering by the private sector requires an increase in government regulation. On the other hand, access to electronic data is perceived as an increasingly important tool for combating crime or terrorism and has provoked calls by law enforcement for greater monitoring capabilities of cyberspace. Here, government authority is the problem. This paradox can be particularly acute in multi-tiered polities with different traditions and sensitivities to centralised forms of surveillance. All of these problems have been amplified by the internet's vastly enhanced scope for amassing citizens' private data by both private and public actors.

1. The United States

As with many other areas, the starting point for any discussion on data privacy and the surveillance or monitoring of cyberspace in the US is the Constitution. There are a number of provisions in the US constitution that significantly impact on federal and state-level policymakers' ability to regulate the collection and use of personal data in both the private and the public sector. The most important of these are the 1st and 4th Amendments. By way of simplification, the free speech rules of the 1st Amendment impose a restraint on the power of government at all levels of public authority to enact legislation that curtails the private sectors' right to 'commercial free speech', even when this relates to the collection and processing of customer's personal data.[4] On the other hand, the 4th amendment bans the government from undertaking unreasonable searches and seizures of citizens' property, which applies to their personal information as much as it does to their physical property. Both provisions would be tested by the internet's rapid diffusion in the 1990s.

[3] For a systematic development of this line of argumentation see in particular Nelson, L. (2004), "Privacy and Technology: Reconsidering a crucial public policy debate in the post-September 11 era." Public Administration Review 64 (3) 259-269.

[4] This point is discussed in detail by Cate, F. and Litan, R. (2002), "Constitutional issues in information privacy." *Michigan Telecommunications and Technology Law Review* 9 (1) 35-63.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

In many ways the constitutional context in relation to data privacy has been somewhat skewed in favour of the private sector.[5] The US regulatory context provided virtually no constraints on data processing by the private sector, while imposing significant limitations on government through the 4th Amendment. Early privacy concerns resulted in the enactment of the 1974 Privacy Act,[6] which regulated data privacy only in relation to *public* sector organisations. Moreover, it applied *only* to federal agencies. One of the distinguishing features of early US regulatory initiatives in the area of data privacy is that they led to a rather uneven sectoral approach. For instance, whereas data privacy regulations in the banking sector were easily passed, in the health care sector, many influential health care organisations successfully opposed a uniform federal law explicitly arguing that the matter should be left to the states.[7] Throughout the 1990s, federal policymakers succeeded in passing legislation to regulate different private sector activities. However, rather than adopting a comprehensive set of privacy rules, US regulators initially pursued a sectoral approach to data privacy in the private sector - a strategy that has since come under increasing pressure with the internet's expansion.[8]

With the rapid commercialisation of cyberspace beginning in the mid-1990s, and the ease with which personal data could now be collected, concerns about data privacy were greatly exacerbated. In this new regulatory context, the Federal Trade Commission (FTC)[9] would emerge as a major policy actor. The latter initiated a series of hearings and consultations with most of the

[5] See Brenner, S. W. (2004) US Cybercrime Law: Defining Offences, *Information Systems Frontiers* 6:2 pp115-132.

[6] According to one analyst it would not have been passed in 1974 had it not been for the Watergate scandal see Bennett, C. (1992). *Regulating privacy: data protection and public policy in Europe and the United States*. Ithaca : Cornell University Press.

[7] Gellman, R., who was involved in drafting the legislation, notes that industry groups opposed the bill on federalism grounds. For further information see Gellman, R. (1996), *Politics, Policy, and Technology: Perspectives on Proposals for Federal Health Confidentiality Legislation in the United States*, available at: http://www.privacyexchange.org/iss/confpro/bcfedhealth.html

[8] See in particular discussion by Heisenberg, D. (2005), *Negotiating Privacy: The European Union, the United States and Personal Data Protection*. Lynne Rienner Publishers.

[9] The FTC is an independent US agency essentially charged with the enforcement of federal antitrust and consumer protection laws.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

major interest groups between 1996 and 2000.[10] At stake was the role to be played by the government in regulating online services. Whereas the industry emphasised the need for a self-regulatory model, privacy advocates favoured government regulation.[11] The self-regulation advocates took the early initiative and by 1998 had created a powerful industry alliance to promote self-regulation as the appropriate response to consumer privacy concerns. Known as the Online Privacy Alliance (OPA), it put forward the argument that technological solutions would be more effective than government legislation.[12] Its membership, which included some of the largest corporations, would adopt and implement online privacy policies, thus demonstrating the industry's ability to police itself.

The outcome of the major hearings during the mid to late 1990s was the adoption of a self-regulatory model in which the FTC was granted a monitoring role. This is perhaps not so surprising given that the mood in Washington was definitely in favour of governmental *non-interference* with the internet.[13] Throughout much of the period, however, the FTC used the threat of regulation to try to encourage the industry to develop a framework for self-regulation.[14] At one point in 2000, a surprising about-turn took place as the FTC called on Congress to enact comprehensive on-line privacy legislation. The FTC had concluded that industry self-regulatory efforts had had limited success and that it was time for Congress to enact legislation ensuring adequate online consumer privacy protection.[15] Nevertheless, it did not

[10] This included ISPs, direct marketers, civil society privacy advocates, information industry representatives and consumer groups, see the *Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996). Available at http://www.ftc.gov/reports/privacy/privacy1.htm
Also, the testimony from the public hearing is available at http://www.ftc.gov/bcp/privacy/wkshp96/privacy.htm

[11] See the transcripts from the Public Workshop on Consumer Information Privacy, June 10-13, 1997. Available at http://www.ftc.gov/bcp/privacy/wkshp97/index.html

[12] The Online Privacy Alliance was created in early 1998 and included more than eighty online companies and trade associations, see http://www.privacyalliance.org/

[13] See for instance *A Framework for Global Electronic Commerce*, The White House, July 1 1997 available at http://www.technology.gov/digeconomy/framewrk.htm where the White House states its preference for self-regulation in the privacy context

[14] See for instance the FTC testimony on "Consumer Privacy on the World Wide Web" before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Commerce Committee, July 21 1998. Available at http://www.ftc.gov/os/testimony/105hearings.htm

[15] Privacy Online: Fair Information Practices in the Electronic Marketplace - A Report to Congress (May 2000), at 38. Available at http://www.ftc.gov/reports/index.htm

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

remain committed to a legislative response for long. With a change in the US Administration, from Clinton to Bush, and under a new Chairman, the FTC changed its track. In October 2001, its new Chairman outlined the new FTC privacy agenda and asserted that what is needed was 'more enforcement, not more laws'.[16] This is a strategy that it has pursued since. The FTC can prosecute companies or individuals engaged in unfair and deceptive trade practices and it has sought to extend this jurisdictional authority to website information privacy policies. Thus, despite favouring a self-regulatory approach, the FTC has nonetheless acquired an expanded jurisdictional role. To this end, it has pursued enforcement strategies to hold websites to their privacy policies.[17] In addition, the FTC has vigorously promoted privacy policies and this strategy has contributed to an increase in its jurisdiction over private sector websites. Indeed, one analyst has rejected claims that the agency, in favouring self-regulation, has been captured by industry. He notes that, to the effect that jurisdiction is power, the FTC has effectively gained jurisdiction over the commercial internet by promoting website privacy norms and enforcing such rules when necessary.[18]

Although a self-regulatory approach was initially favoured in relation to data privacy, between 1999 and 2005 numerous internet privacy laws at the federal level, over 30 according to one government source,[19] were considered by policymakers. Nonetheless, despite this apparent legislative frenzy, none of the initiatives were cleared by Congress apart from certain minor rules that affected federal websites and a set of privacy regulations related to children's

[16] See the remarks of FTC Chairman Timothy J. Muris on *Protecting Consumers Privacy: 2002 and Beyond*, at the Privacy 2001 Conference, Cleveland, October 4 2001 available at http://www.ftc.gov/speeches/muris/privisp1002.htm

[17] This theory was first tested out in 1998 in an action against an internet company alleged to have misrepresented the purposes for which it collected personal information. The case (decision *Geocities*, FTC Dkt. No. C-3850) was eventually settled with the relevant company agreeing to implement various privacy practices and the FTC has since brought several similar actions which can be viewed at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[18] Hetcher, S. "The FTC as Internet Privacy Norm Entrepreneur", 53 *Vand. L. Rev* (2000) 2041, especially at pages 2053-2061.

[19] For an overview of federal level internet privacy laws see in particular, Congressional Research Services Order Code RL31408, *Internet Privacy: Overview and Pending legislation, 2004*. And Congressional Research Services, Order Code RL31408, *Internet Privacy: Overview and Legislation in the 109th Congress*

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

online privacy[20]. In the absence of a comprehensive response to data privacy concerns at the federal level, the states were therefore left with a significant free reign to develop their own response. The problem of unsolicited commercial email, otherwise known as spam, perfectly illustrates the regulatory dynamics in multi-tiered polities such as the US.

Spam was a problem that mostly came to prominence in the late 1990s, although as early as 1997, the FTC had already begun to take a keen interest in the issue. It organised workshops[21] and set up a broad-based Working Group. However, privacy and self-regulation advocates clashed on the matter and no new federal laws on spam were proposed by the Working Group.[22] Nevertheless, a number of legislative initiatives were proposed by legislators at the federal level, as well as by five state legislatures.[23] But the federal legislative response was not forthcoming.[24] In the meantime, the states took the lead in implementing anti-Spam measures and, between 1997 and 2003, thirty-six states had enacted legislation.[25]

Inevitably, such a degree of state legislative activity resulted in a patchwork of regulations. This variance was most notable between states adopting a weaker form of regulation, known as an *opt-out* regime, and those which adopted tougher rules, known as *opt-in.*[26] One of the unintended consequences of this proliferation of uncoordinated state level initiatives was the mobilising effect it had on industry which had previously opposed federal

[20] See the Children's Online Privacy Protection Act of 1998

[21] See in particular a specially organised workshop by the FTC in 1997, proceedings available at http://www.ftc.gov/bcp/privacy/wkshp97/volume3.pdf

[22] See the article by CNN.com, July 14, 1998, FTC study details the burden of junk e-mail, Report recommends moderate measures against junk e-mail. Available at: http://www.cnn.com/TECH/computing/9807/14/junk.email.02/

[23] The different state laws related to internet privacy can be viewed at the National Conference State Legislatures at http://www.ncsl.org/programs/lis/privacy/eprivacylaws.htm

[24] One legal scholar has argued that ever since spam first came onto the congressional radar screen in 1997, the marketing industry had succeeded in blocking federal anti-spam measures year after year, see W. P. Baxter (2003) Has Spam been Canned? Consumers, Marketers, and the Making of the CAN-SPAM Act of 2003, *NYU Journal of Legislation and Public Policy*, Vol 8 number 1 pp 163 at 166.

[25] See Sorkin, D. (2003), "Spam Legislation in the United States", 22 *J. Marshall J. Computer & Info. L.*

[26] In the 'opt-in' regime the party interested in sending out bulk email must first seek permission from the prospective recipient (i.e. the latter 'opts-in' to receive information) whereas in the 'opt-out' regime the recipient has to be offered the possibility to request *not* to receive any further information.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

legislation. In this new regulatory context, industry now pushed for a federal measure that would pre-empt the diverse state measures.[27] Much political wrangling took place and in late 2003, a powerful industry lobby urged Congress to pass a new federal measure.[28] Referring to the varying state legislative responses as a knee-jerk reaction, industry now sought a uniform response at the federal level that, preferably, would lower standards while also pre-empting state law.[29] This is exactly what the CAN SPAM Act of 2003, which came into force the following year, implemented.[30] Not only did the Act grant the FTC an enforcement role -which it has duly pursued[31]- but, crucially, it provided for the pre-emption of state law.[32] This meant, amongst other things, that at least fifteen state spam laws that required unsolicited commercial emails to be labelled, not a requirement included in the CAN SPAM Act, could no longer be applied.[33] The latest initiative seeks to expand the FTC's enforcement powers in relation to cross-border issues while also making it easier to obtain information from US criminal agencies and federal financial regulators.[34]

The issue of anti-spam legislation neatly illustrates the problems concerning just one aspect of data privacy regulation of the private sector. However, its insights apply to the wider domain of data privacy regulation in the US. In the absence of federal legislation, regulation has largely been pursued by the

[27] Noteworthy in this respect is the change in the approach of the Direct Marketing Association(DMA), the largest trade association for businesses interested in marketing and electronic commerce representing well over 4500 companies. In 1998 it testified before Congress against legislation although by late 2002 it issued a press release announcing that it would pursue legislation. See DMA Press Release, The DMA announces support for Spam Legislation, October 20, 2002 available at http://www.the-dma.org/cgi/pressarchive.

[28] This comprised three influential trade groups representing over 6000 companies, the DMA, as well as the American Association of Advertising Agencies and the Association of National Advertisers.

[29] The Open Letter of November 13, 2003 is available at http://www.ana.net/news/2003/11_13_03.cfm

[30] See The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN SPAM Act)

[31] By late 2005 it had brought twenty cases alleging violations of the Act, see *Effectiveness and Enforcement of the CAN SPAM Act: A Report to Congress*, December 2005 available at http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf

[32] This was subject to certain minor exceptions, for further details see Sorkin, D. (2003) Spam Legislation in the United States, 22 *J. Marshall J. Computer & Info. L.*

[33] In particular, a recently introduced Californian law that would have essentially banned all unsolicited commercial email, according to the so-called opt-in regime, was immediately annulled by the federal rules California had passed its measure in 2003

[34] See in particular the US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud – A Legislative Recommendation to Congress (June 2005) available at http://www.ftc.gov/reports/

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

individual states. Not only are the laws broad ranging in their scope, but they are also characterised by notable divergences. The end result is that the US currently has in place a patchwork of regulations, mostly at the state level, where many of the 50 states have implemented legislation governing data privacy.[35] Moreover, the number of state laws appears to be increasing. This has led to a remarkable u-turn by some of the most influential industry players. In this regard, Microsoft, previously an advocate of self-regulation by industry, has since 2005 called for comprehensive federal regulation to overcome inconsistent state laws.[36] It has been joined by other high profile companies and these have now formed a new industry alliance. Contrary to the one formed in 1998 against federal regulation, the new alliance (including many of the same members) is now in favour of a comprehensive federal data privacy law.[37] Since 2005, therefore, the chances of passing comprehensive data privacy rules for the private sector look infinitely higher, a remarkable turnaround from the regulatory context of the previous decade.

The issue of government sponsored surveillance of cyberspace has also generated major policy debates in the US, especially in the aftermath of the 9/11 attacks. From a regulatory perspective, electronic surveillance by law enforcement has been governed by three major federal laws. Two of these, the Electronic Communications Privacy Act (ECPA) and the Patriot Act of 2001 can be dealt with simultaneously. The ECPA was the first comprehensive legislation to cover various forms of electronic communications and was supposed to prevent government entities at all levels from acquiring traffic and communications data from providers unless certain guidelines had been followed.[38] Passed in 1986, the ECPA appeared to offer protections against the dangers of surveillance and information

[35] These include different areas related to data privacy such as anti-spam legislation, spyware, Disclosure of Security Breaches Involving Personal Information, Privacy of Personal Information, Employee E-mail Communications and Internet Access, Privacy Policies on Web Sites. The different state laws related to internet privacy can be viewed at the National Conference State Legislatures at http://www.ncsl.org/programs/lis/privacy/eprivacylaws.htm

[36] See Microsoft's press release on the issue, available at: http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx

[37] It is known as the Consumer Privacy Legislative Forum and includes some of the biggest US companies. See their Statement of Support in Principle for Comprehensive Consumer Privacy Legislation available at http://www.cdt.org/privacy/20060620cplstatement.pdf

[38] See Nelson, L. (2004).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

gathering by governmental authorities. Following the 9/11 attacks, the ECPA was amended by the controversial Patriot Act of 2001. Since it had been drawn up a decade before the internet revolution, there was a legitimate case for the revision of ECPA.[39] However, in updating the regulatory framework, the DOJ and the law enforcement community were able to capitalise on the unique opportunity offered by the terrorist attacks to push for surveillance powers which would not have been considered in the pre-9/11 policy context.

Pushed by the Bush Administration through Congress with unprecedented speed (just one month after the 9/11 attacks), the 2001 Patriot Act expanded the federal government's ability to monitor cyberspace under the rubric of investigating terrorism. It has done so in two principal ways: first, by expanding the surveillance powers of law enforcement and streamlining investigative procedures through further federalisation,[40] and, second, by lowering the burden of proof required.[41] Although the Patriot Act covered many other areas of internal security, its impact on cyberspace has been tremendous and has provoked prominent civil liberties groups to refer to it as a 'dragnet approach' to law enforcement.[42] Not surprisingly, there has been a notable backlash to the Patriot Act that has activated state actors and civil liberties groups, many of whom were excluded from the legislative drafting process. One of the problems concerned the Act's expansion of federal powers by requiring, in some instances, state and local authorities to assist federal agencies in their investigatory efforts. Recently, many state and local authorities have resisted, claiming cooperation will force them to violate civil

[39] See in particular Kerr, O S. (2003), Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't. *Northwestern University Law Review*, Vol. 97, pp 607-674.

[40] For instance, it makes it easier for law enforcement agencies to obtain information from ISP's such as records of sessions and times, IP addresses and means and sources of payments and streamlines investigative procedures by enabling federal courts–with jurisdiction over an investigation – to issue a search warrant to compel the production of information that is stored with an ISP outside their district. Prior to the Patriot Act if an investigator wanted to obtain the contents of an unopened email from an ISP, they would need to obtain a warrant from the jurisdiction where the latter was located. For a detailed discussion see the Statement of Steven M. Martinez, Cyber Division, Federal Bureau of Investigation. Before the Subcommittee on Crime, Terrorism, and Homeland Security Committee on the Judiciary, U.S. House of Representatives, April 21, 2005. Available at: http://www.fbi.gov/congress/congress05/martinez042105.htm

[41] In this context the Patriot Act reduced the need for probable cause to be shown.

[42] Statement of James X. Dempsey Deputy Director Center for Democracy & Technology before the House Committee on the Judiciary Forum on National Security and the Constitution January 24, 2002). See http://www.cdt.org/security/usapatriot/020124dempsey.shtml

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

liberties. Grassroots civil rights movements have been mobilised and have successfully lobbied local and state authorities to pass anti-Patriot Act Resolutions.

By the end of 2005, over 400 local, county and state resolutions had been passed calling, amongst other things, on Congress to repeal or change parts of the Patriot Act law.[43] There is a great deal of variation across these resolutions and they raise important constitutional issues.[44] One crucial aspect of the resolutions is the extent to which they purport to limit state level or local level cooperation with the Patriot's Acts provisions.[45] Indeed one such local provision in California went as far as to impose a fine on any city official who assists in enforcing the Patriot Act.[46] At the same time there have been constitutional challenges to some of the Patriot Act's controversial provisions, although these have been few in number.[47] This has been the case concerning the so-called National Security Letters (NSLs), which enable the FBI to seek records without the need for court approval.[48] Put simply, NSLs can be used without any judicial oversight to obtain information from communications providers such as Internet Service Providers (ISPs) about their subscribers. A newspaper article famously reported in 2005 that the FBI was issuing more than thirty thousand such letters a year.[49] The first constitutional challenge -brought about in 2004 by an ISP which had been served with an NSL- resulted in a New York court ruling the same year that found the provisions in breach of both the first and fourth amendments.[50] Civil

[43] See Bill of Rights Defense Community (BORDC) which lists the "Resolutions Passed and Efforts Underway, By State" available at http://www.bordc.org/list.php?sortAlpha=1 .

[44] See Herman, S. (2005), Collapsing Spheres: Joint Terrorism Task Forces, Federalism and the War on Terror, 41 Williamette Law Review, 941-949.

[45] For a brief discussion see S. Herman, S. "Introduction", in Trager Symposium: Our New Federalism? National Authority and Local Autonomy in the War on Terror, 69 *Brooklyn Law Review* 1201, at 1214-1418 (2004).

[46] The City of Arcata Ordinance No 13339 discussed in Herman, S. (2005).

[47] See S. Herman, (2006), The USA PATRIOT Act and the Submajoritarian Fourth Amendment, 41 Harvard Civil Rights – *Civil Liberties Law Review* 67, pp 71.

[48] For discussion on section 505 see Herman (2006).

[49] See article by Gellman, B., The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans, *Washington Post*, November 6th 2005 stating that 'The FBI now issues more than 30,000 national security letters a year, according to government sources, a hundredfold increase over historic norms.', available at http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html

[50] *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004)

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

liberties groups are still mobilising against the Patriot Act and, in particular, the latter's cyberspace provisions. Moreover, they are mounting further constitutional challenges to this effect.[51]

The second element in the framework governing law enforcement's surveillance capabilities in cyberspace brings to the fore the extent to which the government, and the FBI in particular, can mandate technology standards on network providers to facilitate the interception of communications. The issue acquired prominence in the early 1990s when the National Information Infrastructure (NII) –the precursor of what we now refer to as the internet- was being rolled out. It was at this point that a regulatory battle erupted concerning how this new infrastructure would be designed. Realising that the transformation heralded by the internet could have potentially negative implications for electronic surveillance, the FBI put forward a set of legislative proposals in 1992 to regulate emerging information services offered over the internet.[52] The FBI argued that the measures were needed to retain law enforcement's ability to perform legitimate electronic surveillance and that this was particularly important for under-resourced state and local law enforcement agencies.[53] A coalition of civil liberties organisations and network providers, however, viewed it as a cynical ploy to turn the emerging NII into a 'nation-wide surveillance system'[54] and successfully mobilised to neutralise the bill.[55] In 1994, the FBI introduced a modified version, eventually known as CALEA,[56] in which the initial scope of the bill was greatly narrowed to apply only to telecommunications rather than 'information services' over the internet. The CALEA represented a policy bargain in which the FBI and the Federal

[51] For a list of further actions see the ACLU at http://aclu.convio.net/reformthepatriotact/ , or the CDT at http://www.cdt.org/publications/policyposts/2006/6

[52] The proposals were known as the *Digital Telephony bill.* For a detailed discussion see Landau, S. (2005), Security, Wiretapping, and the Internet, *IEEE Security and Privacy*, vol. 3, no. 6, pp. 26-33.

[53] Testimony of William C. O'Malley, President National District Attorneys Association before a joint hearing of the Senate Judiciary Subcommittee on Technology and the law and the House Judiciary Subcommittee on civil and constitutional rights concerning: the digital telephony and communications privacy improvement act of 1994 on Friday, march 18, 1994. Available at http://www.eff.org/Privacy/Surveillance/CALEA/omalley_031894_hearing.testimony

[54] See the *Electronic Frontier Foundation Statement on FBI Draft Digital Telephony Bill*, available at http://www.eff.org/Privacy/Surveillance/CALEA/digtel94.announce

[55] The Digital Privacy and Security Working Group (DPSWG), also see the DPSWG Coalition's Digital Telephony Letter to the White House, March 9, 1994.

[56] The Communications Assistance for Law Enforcement Act of 1994, it has its own dedicated website, see http://www.askcalea.net/

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Communication Commission (FCC) –the main regulator in this area- would not interfere in the technology standard setting process for information services offered over the internet.

The CALEA policy bargain of the mid-1990s, which was always an uneasy compromise, has since begun to unravel. This is related to the proliferation of new internet enabled services such as internet telephony, email, instant messaging and other online services which are not subject to CALEA design rules. In light of these advances, in 2003 the FBI asked the FCC to incorporate internet enabled services, and in particular internet telephony, within the remit of CALEA.[57] The following year, the FCC stated its intention to regulate so called IP-enabled services within the CALEA framework.[58] The FCC Chairman stated that, henceforth, IP enabled services providers would need to ensure that their equipment was capable of providing surveillance capabilities to law enforcement[59]. Furthermore, the FCC also moved against a number of states that had shown signs of regulatory intervention over IP enabled services. In a crucial jurisdictional decision, the FCC effectively confirmed its regulatory authority to pre-empt state regulation in relation to IP services[60]. Thus, the new data privacy battle over IP enabled services, and the FBI's role in setting technology standards for facilitating interception and surveillance in cyberspace, revisits the battle of the early 1990s. The same civil liberties groups and technology companies have been mobilised although, this time, the new battle will be mainly fought through the courts given the FCC's current rulings in the area. Unlike the earlier battles, for the time being the FBI and the FCC appear to be in a stronger position, at least until the Courts rule otherwise.

[57] See the 2003 Joint Petition for Expedited Rulemaking by the Department of Justice and the Federal Bureau of Investigation, available at http://www.cdt.org/digi_tele/20040310fbipetition.pdf

[58] See the FCC's Notice of Proposed Rulemaking in the matter of IP-Enabled Services, WC Docket No. 04-36 released March 10, 2004.

[59] See the statement by Chairman Powell in FCC's Notice of Proposed Rulemaking in the matter of IP-Enabled Services, WC Docket No. 04-36 released March 10, 2004.

[60] Press Release by Federal Communications Commission FCC finds that Vonage not subject to patchwork of state regulations governing telephone companies, November 9, 2004. Available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254112A1.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

2. The European Union

Much of the current academic debate on the EU's data protection regime focuses on the adoption of the landmark data protection directive in 1995 and its subsequent modifications.[61] This is not unconnected to the international implications of the directive, whose entry into force coincided with the explosion of the internet. What tends to be missed by focusing solely on the adoption of the 1995 directive, however, is the degree to which the Community, and the Commission in particular, had been previously tracking developments in the field of data privacy.[62] In fact, concerns about data privacy had been first voiced by Community institutions in the 1970s, nearly two decades prior to the adoption of the directive.[63] The new information technology threat to personal data had prompted some member states to enact regulations such as general data protection laws and sector specific laws (e.g. health sector or financial sector). Indeed, from a comparative international perspective, the nations at the forefront of the newly emerging field of data protection regulation were actually EU member states, especially France and Germany. Also, in tandem with developments at the national level, and because of the growing importance of transborder data flows, an epistemic community of privacy advocates was mobilised in a variety of national and international forums. Nonetheless, although the activities of the privacy advocates produced a relative degree of convergence in privacy rules, notable differences remained.[64] It was these discrepancies that the data protection directive sought to address.

[61]The discussion focuses on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[62] For an authoritative account on the background to the EU's data protection regime see Heisenberg, Dorothee (2005) *Negotiating Privacy: The European Union, the United States and Personal Data Protection*. Lynne Rienner Publishers

[63] For instance, following the first direct elections to the European Parliament in 1979, one of the first policy statements of the newly elected body was to urge the Commission to prepare proposals for Community action in the area of data privacy OJ C 100/79 of 08.05.1979. See also the Commission's earlier1976 resolution relating to the protection of the individual against the technical evolution of informatics, see the OJ C 100/27 of 03.05.1976;

[64] For instance, administrative regulations concerning procedural requirements and the role of data protection authorities varied considerably in Europe as did differences in criminal sanctions where some member states, such as France, included criminal sanctions for certain privacy violations in its general Penal Code while others, such as Germany, regarded the same violations as administrative offences punishable by fines. For detailed discussion on divergences see Sieber, U. (1998), pp 6

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

It was against the specific backdrop of implementing the internal market programme, where the window of opportunity presented itself to a number of privacy advocates to promote the harmonisation of data privacy rules at the European level.[65] In the early 1990s, the Commission put forward a draft package of policy measures on data protection as a response to growing divergences among member states in the rules governing the processing of personal data by both public and private actors, as well the exchange of such data across borders.[66] The Commission was also aided in its efforts by an influential coalition of national regulators who were driven by a shared desire to use legislative mechanisms to address the threats posed by information technology to data privacy.[67]

EU policymakers' concerns were further amplified by the fact that some member states lacked a comprehensive privacy regime. In the absence of EU level harmonisation, the high-protection member states feared that they would be put at a competitive disadvantage *vis-a-vis* the low-protection member states in the emerging information society. This provided a window of opportunity for a coalition of member state and EU level policy entrepreneurs to put forward a set of harmonisation proposals. The formal adoption of these measures, known as the 1995 data protection directive, marked the culmination of a long process which had began in the 1970s and now defines the basic rules governing data privacy across the EU. But the directive did more than merely harmonise the substantive legal norms. It also created new national regulatory agencies in those member states where these had not previously existed and, furthermore, it provided mechanisms for the supervisory authorities to coordinate their activities though an EU level

[65] For a detailed discussion on this issue see Heisenberg, D. (2005), *Negotiating Privacy: The European Union, the United States and Personal Data Protection*. Lynne Rienner Publishers

[66] See the European Commission's Proposal for a Council Decision in the field of information security COM/90/314 Final

[67] See especially Newman, A. and Bach, D (2004), Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States. *Governance*. 17:3 pp. 387-413. This point is developed more fully in Newman, Abraham (2005) Creating Privacy: the international politics of personal information. Doctoral Dissertation, Department of Political Science, University of California at Berkeley.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

organisation, commonly referred to as the Article 29 Working Party.[68] The latter has come to play an important role in the development of an EU data protection regime.

The main substantive elements of the EU data privacy regime were, in this sense, already well-established before the expansion of the internet. However, with the spectacular growth of the internet during the late 1990s, the issue of data protection began to acquire an even greater salience. Since the 1995 directive had been drafted at the beginning of the decade, i.e. before the internet's proliferation, by the end of the same decade it was clear that modifications would be needed to take specific account of the new internet reality. The revisions, adopted within a short time span of the 1995 directive, have since generated major tensions among the EU institutions and the member states.

The updating of privacy rules for the internet age came in two waves. The first of these was specifically geared to the telecommunications sector.[69] It was quickly followed by a broader legislative measure, known as the e-Privacy Directive of 2002, which sought to address *all* forms of electronic communications and not just the telecommunications sector.[70] The combined effect of these measures is to regulate a number of key internet related issues such as the security of digital networks; the confidentiality of communications; the storage of internet users' traffic and location data. Another area that was also addressed by the EU's new data privacy regime was the problem of how to deal with spam. The 2002 e-Privacy directive sought to address this by prohibiting the sending of spam unless internet users had specifically consented to receiving such electronic communications. Known as the 'opt-in' regime, it forms the cornerstone of the EU approach in dealing with the

[68] This working party has been established by Article 29 of Directive 95/46/EC. It is was set up to provide member state level privacy authorities with a forum to advise the Commission on questions of data protection.

[69] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

[70] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

growing problem of spam. Of course, in the absence of an effective enforcement regime, legislative measures prohibiting certain activity alone are unlikely to be sufficient. Thus, the Commission[71] has been quick to point to a series of enforcement gaps that need to be addressed through further harmonisation of the legal framework.[72] These enforcement gaps have provided the justification for further attempts to harmonise or coordinate actions at the EU level. Following a consultation process on spam that brought together the relevant stakeholders a pan-European organisation, the Contact Network of Spam Enforcing Bodies (CNSA), has been created. Even though most spam originates from outside the EU, the new body was a response to the growing demand for intra-EU coordination of cross-border enforcement and greater information exchange among the member state enforcement agencies.[73] Other gaps related to the implementation of the 'opt-in' regime, as well as other areas of the e-Privacy directive, have led the Commission to launch infringement proceedings against member states. Thus far, three Member States have been found by the ECJ to have breached their obligations under the e-Privacy Directive by failing to implement it within the prescribed period.[74]

It should be noted that data privacy has also become enshrined in the EU treaties, with important implications for the emerging regulatory regime in this area. Privacy advocates received a boost with Article 286 of the Treaty of Amsterdam, which applied the general rules of the 1995 directive to the EU institutions. The Treaty also included provisions for the establishment of an independent supervisory body responsible for monitoring data protection concerning public EU institutions (the European Data Protection Supervisor). The tasks of the new EU authority will follow the same logic as the national

[71] See the European Commission's Communication on unsolicited commercial communications or 'spam', COM(2004) 28 final

[72] For instance the Commission identified notable divergences in penalties (e.g. these varied from 145 Euros per spam message to fines of 450.000 Euros) and sanctions (such as warnings to offenders through to imprisonment) discussed in the Communication on 'spam', COM(2004) 28 final

[73] European Commission press release of 7 February 2005 European countries launch joint drive to combat "spam" IP/05/146

[74] Case 375/04 Commission v Belgium and 376/04 Commission v Luxembourg, judgments delivered on 28 April 2005, not yet reported, and Case 475/04 Commission v Greece, June 1st 2006, not yet reported.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

supervisory bodies, such as hearing and investigating complaints, and where necessary imposing sanctions and making referrals to the ECJ. Although its remit is limited to Community institutions, the body has attempted to play a prominent role, alongside the Art 29 Working Party, in the development of data privacy legislation. Thus, the federal nature of the European Data Protection Supervisor can be contrasted with the more intergovernmental Art 29 Working Party, the body which brings together the representatives of the member state data authorities.

In all of the developments noted, the newly empowered independent agencies operating at the member state/EU level nexus have played an influential role in pushing for the further harmonisation of data protection rules. Moreover, they have been especially sympathetic to the views of many civil rights organisations and commercial network providers in trying to stem the 'surveillance' agenda of law enforcement agencies and the interior ministries of the member states. This has resulted in a growing tension between privacy and security advocates, a tension that has become by far the single most salient issue in data protection. These tensions have also affected inter-institutional relations, especially between the Council and the rest of the European institutions.[75] The major policy conflict is one that goes to the very core of member state sovereignty in matters of internal security: the retention of communications data for law enforcement purposes. In the post-9/11 security context, access to internet users' traffic data for law enforcement purposes has become perceived as an increasingly important crime-fighting tool. This has generated heated policy debates in most member states about the nature and conditions governing law enforcement agencies' access to citizens' personal electronic data for internal security purposes. But because of the interdependencies among the member states, effective policy needs to be realised through EU level coordination. The issue has mobilised an

[75] In particular it has also caused tensions between the Commission and the European Parliament. The most recent striking example concerns the 2004 agreement between the EC and the US which allows for the transfer of passenger name records to the US. The agreement was adopted contrary to the views of both the EP and the Article 29 Working Party, both of which had questioned its compatibility with European Data protection rules. The EP accordingly brought a challenge to the agreement, supported by the European Data Protection Supervisor, which was upheld by the ECJ: see Joined Cases C-317/04 and 318/04, judgments of 30 May 2006, not yet reported.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

influential coalition of policy actors who increasingly need to pursue their interests through EU level coordination. Interestingly, the real policy debate is not about whether EU level coordination is necessary, but rather a competency clash concerning whether the coordination should take place within the context of the first or third pillar, in other words, whether it is to be governed by supranational or intergovernmental procedures.

Following the 9/11 attacks, and especially after the terrorist attacks in Europe, the position of the privacy advocates has tended to be weakened. But, in many notable respects, the conflict between privacy advocates and law enforcement agencies had been present well before the attacks of 9/11. At the heart of the controversy were the 1995 data protection directive and its subsequent modifications. Much to the dismay of the security advocates, the directive included very stringent provisions for the removal of data. In fact, it established a principle of law that traffic data must be erased by network providers as soon as its storage is no longer necessary. It was this provision in particular that, according to law enforcement agencies, could potentially hamper the fight against terrorism.[76] Although a harmonised EU regime for data privacy was in place, despite some variation in member state implementation, the rules governing 'data retention' for law enforcement purposes was a patchwork of rules. Most crucially, there were major differences concerning data retention periods, which could vary from three months to four years.[77] More problematic still, these differences were likely to grow if member states pursued unilateral measures in response to the threat of terrorism.

Although many discussions on data retention had taken place well before the 9/11 attacks[78] no agreement had been possible between the competing

[76] See the comments of Chief Superintendent Keith Akerman, UK Police and Chairman of the UK Internet Crime Forum, European Commission organised Public Hearing . Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. 2001, March 7.

[77] See the Commission's Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. COM/2005/438

[78] A database of the main EU-level discussion on data retention are available from the civil liberties group Statewatch and can be viewed at http://www.statewatch.org/eu-data-retention.htm

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

interests. The security advocates -who could effectively mobilise through intergovernmental channels -favoured a member state driven initiative that would impose compulsory data retention on network providers.[79] But the initiative did not get very far. A pan-European coalition of independent data authorities from the member states, civil society groups, and influential interest associations such as the network providers, as well as institutional players including the European Parliament, successfully mobilised to temporarily counter the initiative. However, with the recent terrorist attacks of 2004 and 2005 in Europe, the internal security balance on the question of data protection has been dramatically altered. And to the extent that it has been altered, it has strengthened the relative bargaining power of the security advocates within the interior ministries and law enforcement agencies. Their main goal is to relax what they perceived to be excessively stringent data privacy rules that hamper the fight against terrorism. Thus, immediately after the Madrid attacks in 2004, the heads of the member states organised a special summit and adopted a European Council declaration on combating terrorism.[80] It specifically called on the Council to examine measures for establishing rules on the retention of communications data by service providers. Sponsored by four member states and published just one month after the Madrid bombings, the proposed Council measure[81] essentially built on the previous 2002 Belgian initiative. Its main aim was to strengthen law enforcement surveillance powers with regard to all electronic communications. The Council initiative provoked an immediate institutional reaction. The influential intergovernmental body of EU data protection authorities (Art. 29 Working Party) issued a damning official Opinion[82] on the member states' initiative.

[79] A draft of the Belgian intiative for a Council Framework was leaked by the civil liberties group, Statewatch.

[80] Council Document 7764/04 of 28 March 2004

[81] Council Document 8958/04 of 28 April 2004 on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purposes of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

[82] Arguing that the measure proposed were disproportionate, the body noted how 'representatives of the law enforcement community had failed to provide any evidence as to the need for such far reaching measures' and that they had 'been totally and conspicuously absent at recent workshops organised with a view to consider the background and the consequences of the…draft Framework Decisions' pp4. This was hardly surprising since the security advocates were pursuing a successful lobbying strategy

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

The European Parliament was also quick to resoundingly reject the Council proposal in May 2005,[83] even though it has only advisory powers in this area of internal security. It called on the four member states to withdraw the initiative and was particularly critical of the provision which obliged network providers to store data for 12-36 months. Apart from drawing attention to the dangers of infringing upon individuals' data privacy, the European Parliament argued in its resolution that there would be a knock-on effect to the internal market, in terms of the massive cost burden that it would impose on network providers. Such a 'blanket' data retention rule would, in the absence of other harmonisation measures, lead to diverging cost burdens for network providers across the EU, adversely hitting the smaller providers and threatening the internal market. In formulating this argument the European Parliament was trying to raise a 1st pillar argument. The real battle was, in effect, a procedural one: whether data retention would be regulated via the Community method of the first pillar or the intergovernmental third pillar.

The position of privacy advocates was certainly not aided by the fact that within a month of the European Parliament Resolution a second major terrorist attack in Europe took place, the London bombings of June 2005. It served to further amplify the tensions between the competing interests. Whereas the coalition of privacy advocates argued that the current first pillar data protection regime was sufficiently flexible to accommodate the new challenge,[84] the security coalition favoured a third pillar route to enhanced cooperation among member state law enforcement agencies.

The lack of agreement on the rules governing the retention of communications data, as well as the growing inter-institutional conflicts, was threatening the privacy balance that had been carefully crafted since the early 1990s. This was how the Commission viewed the matter and it therefore stepped in to

---

through the member states' interior ministries and, in particular, through the Council. See Opinion 9/2004 of the Article 29 Data Protection Working Party 11885/04/EN.

[83] See the European Parliament's draft resolution A6-0174/2005 of May 31 2005

[84] The EU's data protection directives allow exceptions and derogations for national security and law enforcement purposes.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

offer a compromise solution. In doing so, however, it would promote its own agenda for an EU-wide data retention regime. The plan essentially involved regulating the data retention period through the 1st pillar while enhancing law enforcement cooperation via the 3rd pillar. This would avoid relying exclusively on a member state driven Framework Decision. The Commission did this by adopting two initiatives: the first was a proposal for a new directive on data retention[85]. The Commission drew attention to the patchwork of data retention regimes that presently existed in the EU and how this was likely to be exacerbated as member states embarked on further uncoordinated measures. The patchwork of rules varied significantly with respect to the scope of the measures being proposed, the electronic data to be retained (e.g. emails, IP numbers, and chat room data), the duration of the retention (e.g. between 3 months and 4 years) and the reimbursement possibilities for network providers. In short, the proposed directive sought to keep data retention issues firmly within the supranational 1st pillar framework.

The Commission also put forward plans for a Council Framework Decision which would address the third pillar issues.[86] This included mechanisms for improving the efficiency of data exchange among the member states, as well as the rules governing how law enforcement agencies can access personal data from other member states. In sum, the two proposals sought to keep the different issues firmly within their respective pillars rather than adopt a 'blanket' data retention exclusively via the intergovernmental third pillar. The Commission's proposal have not been free of criticism, especially from civil liberties groups[87] and the European Data Protection Supervisor,[88] who have been the most vocal of critics. The European Parliament nonetheless gave

[85] Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC COM/2005/438

[86] For a discussion see the Commission's Press Release of 21 September 2005'Commission proposes rules on communication data retention which are both effective for law enforcement and respectful of rights and business interests. IP/05/1167.

[87] See Statewatch's documentation at http://www.statewatch.org/eu-data-retention.htm

[88] See the Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005) 438 final).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the green light to the proposal in December of 2005.[89] What does remain clear is that, despite the competency clashes over the first and third pillar, there is an unmistakable trend towards further EU level harmonisation in all areas of the data privacy domain.

3. Switzerland

The introduction of data protection laws in Switzerland has been a typically lengthy affair. Although first efforts can be traced back to the early 1970s, it was only in 1984 when sufficient consensus was reached to put forward initial draft legislation. Over the next half a decade, the plans were heavily criticised for being too complicated with a number of drafts being put forward. In 1992, nearly twenty years after policy discussion was first initiated, the Federal Data Protection Act was finally passed.[90] Apart from the impetus provided by international efforts, especially by neighbouring European privacy pioneers during the 1970s, it is worth noting another factor for the federal response. A number of cantons, e.g. Berne, Neuchatel, Geneva and Ticino, had already passed legislation in the area of data privacy well before the federal act.[91] To avoid potential inconsistencies the federal act sought to harmonise data privacy regulations for the private sector. It did the same for all federal agencies. The rest was the responsibility of the cantons. At the same time, the legislation created a host of new data privacy agencies at the federal and cantonal levels. Furthermore, in many cantons another tier of agencies was also established at the communal level. In this way, the legislation created a whole new set of privacy advocates where, in many cases, these had previously not existed. For instance, the data protection commissioner for Berne has, in theory, 400 partners in the canton although in practice only a dozen make serious contributions[92]. It is hardly surprising that such a multi-

[89] Data retention measures were successfully passed in early 2006, although these are presently the subject of legal challenge by Ireland.

[90] This is not to say that data privacy had not been a concern. In fact, data privacy concerns can be traced as far back as Article 36 (4) of the 1874 Constitution guaranteed 'the inviolability of letters and telegrams', the latter provision was subsequently amended in the 1999 constitution.

[91] See the review by the Cancelleria dello Stato del Cantone Ticino, Rossini,C Fiorenzo (2000), Dieci anni di protezione dei dati e la possibile evoluzione nel prossimo millennio, available at http://www.ti.ch/CAN/RPD/temi/archivio/RDAT-II-2000.pdf

[92] Interview with Cantonal data protection commissioner 30/06/2005

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

tiered format would generate numerous competency clashes among the overlapping privacy agencies.

When addressing the politically sensitive issue of government surveillance for internal security purposes –such as the interception of internet communications- it is important to take account of a national surveillance scandal that erupted in Switzerland during 1989. It followed a parliamentary inquiry which revealed that the federal police had collected files on a large portion of the population.[93] Within two years, a popular initiative had already been launched to abolish the 'federal police' force. However, after delaying the referendum for almost a decade while implementing a complete administrative reform, the federal government managed to save the federal police force in the referendum of 1998.[94] The scandal has ensured that federal proposal related to surveillance would generate intense politicisation and, given this policy context, the issue of surveillance using new technologies was always bound to generate political controversy.[95]

One of the first steps towards a surveillance regime for internet communications was partly the result of liberalization measures in the telecommunications sector. In the 1997 Telecommunication Act,[96] the government issued a regulation that established a specialized agency, *Le Service des Tâches Spéciales* (STS), within the Department of the Environment, Transport, Energy and Communications, for administering interception orders. Shortcomings in the regime soon appeared when, in April 2000, the Federal Court[97] ruled that email was covered by the secrecy of communications with the effect that, in the absence of a legal basis, it was not

[93] Detailed information on the scandal, and the evolution of federal policing, is available from the Swiss federal archives, see the Archivio federale svizzero, Giustizia e polizia, http://virtor.bar.admin.ch/it/default.aspx

[94] For a discussion see the Swiss Confederation section of the Privacy International global survey on data protection laws (2004) available at http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83795

[95] See for instance Manach, Jean-Marc (2003) Transfer.net Societe de l'information, La Suisse légalise son système d'espionnage des télécommunications, available at http://www.transfert.net/La-Suisse-legalise-son-systeme-d

[96] Telecommunications Law (LTC) of April 30, 1997. Ordonnance du 1er décembre 1997 sur le service de surveillance de la correspondance postale et des télécommunications

[97] See Federal Court decision ATF 126 I 50 Swiss Online AG

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

possible to intercept email communications.[98] The legal basis was soon forthcoming when the Telecommunications law was amended the following year to cover email communications[99]. By following the appropriate legal procedures –i.e. cantonal prosecutors issue the interception order- it would be possible to gain lawful access to email communications data from ISP's for law enforcement purposes.

Well before the new measures were passed there had been notable divergences during the consultation procedure. A majority group was very critical about the measures proposed.[100] Pushed by the security advocates, the draft measures had initially covered a broad range of crimes and included provisions that would permit surveillance in order to *prevent* crimes. This met with considerable resistance during the consultation procedure and parliamentary debates.[101] Interest associations such as the SUIG,[102] as well as consumer organisations and data protection authorities, were immediately mobilised against the rules.[103] Given the controversies, the end result was a bundle of watered down surveillance measures that were rather limited and only apply to email communications. Surveillance was also restricted to certain categories of suspected criminals. For instance, investigators cannot check emails when pursuing software pirates, publishers of hate speech or even computer hackers.[104]

Nonetheless, ISPs would now have to keep a log for six months of all the emails sent by their customers and implement the necessary technical changes to their networks for accomplishing such a task. Federal

[98] The case and its legal implications is discussed pp 198 in Auer, A., Malinverni, G., and Hottelier, M. (2006), *Droit Constitutionnel Suisse, Volume II Les Droit Fundamentaux*, Stampfli Editions, Berne.

[99] See the 780.11 Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (OSCPT) avaialble at http://www.admin.ch/ch/f/rs/c780_11.html

[100] See the Federal Council's Message 98.037 concernant les lois federales sur la surveillance de la correspondance postale et des telecommunications et sur l'investigation secrete, 1er juillet 1998.

[101] See for instance the Services du Parlement, Communiqué de presse, Commission des affaires juridiques du Conseil national, *Surveillance de la correspondance postale et des télécommunications : meilleure protection des droits fondamentaux*, Berne, 16 Novembre

[102] This was an internet lobby group known as the Swiss Interent Users Group (SUIG).

[103] See the report on Switzerland by Privacy international (2003) Silenced - Switzerland, available at http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-103784

[104] See article by Swissinfo, Swiss surveillance catches up with email, July 21, 2002. available at http://www.swissinfo.org/eng/Swissinfo.html?siteSect=111&sid=1192676

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

policymakers tried to avoid overburdening ISPs and therefore chose to limit the types of crime where surveillance can be authorised to offences such as paedophilia and child pornography.[105] Furthermore the special unit in Berne, the STS, would be responsible for dealing with interceptions. In effect, this was the other side of the bargain and entailed a federalisation of sorts. The cantons are still the body that initiates the surveillance requests. The special unit acquires the information from the ISP's and communications providers, and then sends it back to the Cantons. The federal unit has no competencies to conduct its own investigations and thus serves only to coordinate procedures[106]. In this way, the special unit acts as a coordination mechanism, which streamlines procedures without overburdening the ISPs and without taking competencies –and this is one of the crucial points- away from the cantons.

One important development that took place in the field of data privacy during the 1990s -at least from a constitutional perspective- is Art. 13 of the new Swiss Constitution of 1999. In many ways a triumph for privacy advocates, the new constitutional provision states that every person has the right to the secrecy of their communications and, furthermore, 'has the right to be protected against abuse of personal data'.[107] This is a notable constitutional development in the area of data privacy, both with regard to the regulation of data collection by the private and public sector, as well as the potential for the surveillance of internet communications. Apart from this formal development, the newly created Federal Data Protection Commissioner's (FDPC) office has played a notable role by drawing public attention to a spectrum of data privacy concerns. The office has served as the focal point for many initiatives, especially in relation to the privacy challenges generated by the internet's

[105] See the article by Swissinfo, Swiss log on to email surveillance, April 1, 2003 available at http://www.swissinfo.org/eng/Swissinfo.html?siteSect=111&sid=1733311

[106] See the message from the Dipartimento federale dell'Ambiente, dei Trasporti, dell'Energia e delle Comunicazioni DATEC, Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, 07/05/2004, available at http://www.uvek.admin.ch/themen/kommunikation/00690/00691/index.html?lang=it

[107] For an authoritative discussion on Swiss constitutional law issues related to privacy see Auer, A, Malinverni, G and Hottelier, M (2006).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

proliferation.[108] Its activities have been mostly informational however, and specifically geared towards raising awareness of the most salient data privacy issues. One of the issues that needed to be addressed was the updating of the foundational Data Protection Act of 1992. The latter had been drawn up in the early 1990s and would need revision to take account of the specificity of the internet challenge, which by the late 1990s was in full swing. After various calls from the FDPC, and a 1998 parliamentary motion to specifically address the 'online' challenge, the Swiss federal authorities began the process of revising the 1992 Privacy act for the digital age.[109]

To this end, the federal council announced its plans and the different issue areas that needed to be addressed.[110] In particular, it noted issues related to the division of competencies between the Confederation and the Cantons in the area of data privacy and the fact that there were significant variations among the cantons with regard to the implementation of the landmark 1992 privacy act. For instance, not all the cantons had yet appointed data protection authorities. Further harmonisation measures would also be required, especially to deal with 'online transactions' -the subject of the 1998 parliamentary motion.[111] At the same time a further enhancement of the FDPC's regulatory powers was envisaged. Initiated in September 2001, the consultation process, which involved all the major stakeholders including the cantons, political parties and private organisations, revealed a number of serious policy divergences[112]. In fact, the FDCP itself acknowledged that

[108] A list of recommendations and special reports on privacy issues, especially related to the internet can be found at the website of the Federal Data Protection Commissioner at http://www.edoeb.admin.ch/

[109] See the Parliamentary Motion 98.3529 Liaisons "on-line". Renforcer la protection pour les données personnelles

[110] See the Dipartimento federale di giustizia e polizia,(2001) Procedura di consultazione, *Avamprogetto e rapporto esplicativo in merito alla revisione della legge federale sulla protezione dei dati*, available at http://www.ofj.admin.ch/etc/medialib/data/staat_buerger/gesetzgebung/datenschutz.Par.0012.File.tmp/vn-ber-i.pdf

[111] See the Parliamentary Motion 98.3529 Liaisons "on-line". Renforcer la protection pour les données personnelles

[112] See the report by the Dipartimento federale di giustizia e polizia, (2002) Compendio dei risultati della procedura di consultazione concernente la revisione parziale della legge federale. sulla protezione dei dati (LPD), available at www.bj.admin.ch/themen/datenschutz/ve-ber-i.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

'The draft revision has also provoked some criticism insofar as the supervisory role of the Swiss Federal Data Protection Commissioner in the private sector is concerned. The fear is that the SDPC could interfere in every individual case. However, such an interpretation goes against both the spirit and the letter of the proposals that have been made. What is more, the SDPC does not have the resources to do so.'[113]

Enhancing the supervisory powers of the FDPC was therefore off the agenda. It is important to note how limited these powers were in the first place. The 1992 Act created the office of the Federal Data Protection Commissioner, as an essentially supervisory body rather than an office with regulatory powers. Given the tensions that existed between the different levels of government, the creation of a powerful regulatory agency would not have been acceptable to the cantonal authorities. Thus, although the office formally has a number of tools at its disposal, such as conducting investigations, in reality it has only limited possibilities for intervention. The Commissioner can only submit a number of 'suggestions' (*Empfenhlugen*) and decisions can only be taken by the Court and/or Federal Council. Moreover, where private persons are concerned, the procedure is initiated through cantonal authorities.[114] Thus, the FDPC's input is rather limited to issuing critical statements on data protection issues and making recommendations through the publications of its annual reports. It has not been surprising therefore that the FDPC has been at the forefront of raising awareness among policymakers and the general public with regard to internet related privacy challenges. Especially prominent among its concerns have been the issues of email surveillance at the workplace and Spam. On the former, since this is an issue that is directly within its policy remit, the federal supervisor has issued a series of recommendations.[115] It has also been very active on spam although, as of 2005, Switzerland still did not have any specific laws or anti-spam measures. However, as a result of the FDPC's public awareness campaigns, and a

[113] See the Federal Data Portection and Information Commissioner's 12th annual report 2004/2005, also available at http://www.edoeb.admin.ch/dokumentation/00445/00509/00510/00813/index.html?lang=en

[114] Interview with the Cantonal data protection commissioner, 30/06/2005

[115] See for instance the section on *La surveillance du courrier électronique et d'Internet sur le lieu de travail* in the report by the Préposé fédéral à la protection des données et à la transparence (2001), 13e Rapport d'activités 2001, available at http://www.edoeb.admin.ch/dokumentation/00445/00509/00514/index.html?lang=fr

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

parliamentary motion[116] in 2000, a revision is being undertaken that will implement the tougher opt-in regime.[117] Although the FDPC has been active in drawing attention to the issue, the revision as currently envisaged will grant supervisory powers to the State Secretariat for Economic Affairs. The latter will also be responsible for cross-border enforcement for individuals and for companies.

Despite the rather limited powers of the federal supervisor, data privacy issues have managed to generate a series of tensions among the distinct levels of government. The relations have been especially strained between the federal supervisor and the cantonal data protection authorities. For instance, even though supervision of the private sector is a federal competence, there are a number of grey zones. In particular, the health and financial sectors are areas where data privacy issues have generated competency clashes among the different levels of government.[118] The cantonal authorities, especially those that are better resourced such as Zurich, are averse to giving up any powers in the data privacy domain. At the same time, the FDPC has been quick to point out cantonal divergences. For instance, the FDPC has argued that although the cantons have enacted data protection legislation, 'not all of them have introduced an independent control authority. In addition, the efficiency of the legislation varies enormously as a result of the structures and means respectively available. The degree of data protection differs at times both from canton to canton and from the cantonal to the national level'.[119] In fact this was one of the issues that the revision of data protection laws was supposed to address.

In view of the competing interests between the cantonal data protection authorities and the Federal supervisor, the cantons pre-emptively created an

[116] See the parliamentary motion 00.3393 Mesures 'antispamming. Multipostage abusive.

[117] For further information see the planned amendments to the Telecommunications Law and Law on Unfair Competition www.admin.ch/ch/f/ff/2003/ index0_49.html

[118] See for instance the section on *Transfert de données médicales par Internet* in the report by the Préposé fédéral à la protection des données et à la transparence (2001), 8e Rapport d'activités 2005/2006, available at http://www.edoeb.admin.ch/dokumentation/00445/00509/00514/index.html?lang=fr

[119] See the Federal Data Protection Commissioners 9th Annual Report, available at http://www.edoeb.admin.ch/dokumentation/00438/00465/00845/00849/index.html?lang=en

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

inter-Cantonal association of data protection commissioners in 2000. Known as the DSB+CPD, its function was to coordinate cantonal strategies in the area of data privacy and exchange views. From the cantonal perspective this made sense given the fact that they were dealing with the same types of problems.[120] During the pre-parliamentary phase, for instance, the Cantonal data protection authorities have a role to play in scrutinising federal legislation when it touches upon data privacy issues, and where they can put forward their positions. Thus, there was no point in every Canton conducting the same exercise. It would be easier to do this together within the DSB association. This was despite the fact that the federal supervisor was engaged in the very same process. Typically, a Working Group within the DSB would prepare a position, which was then passed back to the Cantons. The process ensured that the Cantons acted as a united force and, to this end, the DSB served as platform for putting forward the Cantonal policy viewpoint.

Initially, the Federal Supervisor participated in the inter-cantonal association. However, after a number of policy disagreements, the membership was effectively terminated. Among the many differences was a clash over roles, and in particular, how messages concerning data privacy were communicated to the public. Given its rather limited powers, communicating with the media and the press was one of the FDPC's most important policy tools. It was increasingly frustrated therefore when cantonal authorities would communicate directly with the media on issues that it felt were clearly federal in scope[121]. In addition, the inter-cantonal association started to publish its own reports on data privacy, sometimes critiquing the FDPC position. For instance, the inter-Cantonal association also published its own guide to internet data privacy even though this was a policy domain in which the FDPC had been making numerous recommendations over the years.[122] Another sore point was the issue of political representation at, for instance, international conferences. Some of the better-resourced cantons also wanted, and indeed, participated in the international agenda-setting forums.

[120] Interview with former President of the DSB+CPD 30/06/2005
[121] Interview with official from Federal Data Protection Commmission 25/11/2005
[122] See for instance DSB+CDT report on Sécurité et outils modernes de communication, available at http://www.dsb-cpd.ch/f/publikationen/depliant_securit%e9_f.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

As of 2005, and a full seven years after the 'online transactions' parliamentary motion, the revision of the privacy act has yet to be agreed, let alone implemented. Throughout the revision process, cantonal interests appear to have been better represented during the drafting process since they can have considerable influence inside their administrations. Indeed, they can have a greater impact than the federal supervisor has on the federal administration.[123] This is despite the fact that the FDPC has a consultative role and can issue opinions where legislation has privacy impact. Unfortunately, the FDPC only gets to give its opinion rather late in the decision-making process and, since 9/11, is generally always on the defensive.[124]

This brings us neatly to one of the biggest tensions in the data privacy sphere in Switzerland. It is less about clashes between privacy advocates on competence issues, than it is about differences with the security advocates represented in the police and justice department. The big tension on the legislative front is increasingly with the police department. Further measures to enhance law enforcement's investigative and surveillance powers, especially with regard to internet communications, are currently being negotiated by two federal agencies (communications and police/justice departments) and will constitute the new policy battleground. Although no new policy initiatives are expected until 2006, further inter-departmental battles over legislation in this domain, and its data privacy impact, are likely to ensue.[125]

4. Comparative review of data privacy

Before proceeding to compare policy dynamics, there is one important dimension to identify. This relates to the significant extra-terrirotorial effects of the EU's 1995 data protection directive which has produced interaction effects

[123] Interview with official from Federal Data Protection Commmission 25/11/2005
[124] Interview with official from Federal Data Protection Commmission 25/11/2005
[125] See the Communication by the Dipartimento federale dell'Ambiente, dei Trasporti, dell'Energia e delle Comunicazioni DATEC, *Il Consiglio federale favorevole a uno sviluppo della sorveglianza del traffico delle telecomunicazioni*. Berna, 29.03.2006.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

among the three units of analysis. This is mostly as a result of certain provisions in the EU's data protection rules that prevent the transfer of data to third countries that have inadequate privacy safeguards. According to some authors, this has resulted in a 'trading up' of data privacy standards at the international level[126]. In the Swiss case, the issue is rather straightforward since, from an EU perspective, Switzerland has adequate data privacy safeguards.[127] The problem was with regard to what EU policymakers viewed as inadequacies or gaps in the US self-regulation regime. To iron out these difficulties, a compromise known as the Safe Harbor Principles was negotiated so that transfers of personal data between the EU and the US were not interrupted.[128] Despite the extra-territorial impact of the EU's data protection regime on both the US and Switzerland, its effects have not altered the policy dynamic which is the subject of this inquiry, (that is the vertical interactions among levels of government and the power capabilities of central level agencies).

The internet's rapid commercialisation in the mid-1990s and the consumer privacy concerns it generated as well as, more recently, the increasing importance attached to the timely access of online traffic data by law enforcement, became the subject of increased political contestation in each of the three polities. These controversies have activated similar policy dynamics in the three federal systems. Put simply, the policy issue has mobilised a number of privacy proponents who have clashed with security advocates. Civil liberties groups and ISPs have generally opposed the enhanced surveillance measures, such as data retention requirements, that have been promoted by security advocates. This has been because of their impact on citizens' privacy or due to the cost burden it imposes on providers. This dynamic has been similar across the cases. One notable difference, however, is the fact that in

[126] Shaffer, G (2000), Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards, *Yale Journal of International Law*, Vol. 25, pp. 1-88.

[127] On Switzerland see the European Commission's Decision 2000/518/EC of 26.7.2000 - O. J. L 215/1 of 25.8.2000

[128] For a detailed discussion on this issue see Heisenberg, D. (2005). See also Long, Willaim and Pang Quek, Marc (2002) Personal data privacy protection in an age of globalization: the US-EU safe harbour compromise. Journal of European Public Policy 9:3 pp 325-344.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the EU and the Swiss cases, the most influential privacy advocates have been the data protection authorities. The latter operate at multiple levels of government and include the federal level data protection commissioners/supervisors and the associations of intercantonal/intergovernmental data protection authorities. In the US, on the other hand, civil liberties groups have tended to perform the privacy advocacy role. Occasionally, they have been supported in their efforts by federal agencies such as the FTC, but this has generally not been the case. Connected to this is another notable difference in political actors' mobilisation. In the US, important federal actors, backed by industry, initially resisted calls for the implementation of a comprehensive data privacy regime. Only when the proliferation of inconsistent state regulations started to produce negative impacts on major industry players did the latter shift their initial policy preferences. This is in direct contrast to the EU and Switzerland where a legislative approach has been favoured from the start. The argument advanced by a leading authority in the data privacy area is that differences in processes of interest intermediation account for the diverging US and European approaches to data privacy. While privacy advocates played a very significant role in Europe, in the US, by contrast, business interests were consulted almost exclusively and the administration's position reflected their preferences.[129]

As to the security advocates one can identify within the three federal polities a similar coalition of law enforcement agencies as well as interior and/or justice departments operating at all levels of political authority. Although security advocates had been active well before the spate of terrorist attacks, the political context since has been considerably more favourable for implementing enhanced security measures. Nonetheless, we can identify some notable differences with regard to the way in which executive authority has been wielded in this area. For instance, in the US, the federal administration has been able to implement surveillance measures without going through lengthy consultation processes. Such expedited processes are

[129] See pp10 of the monograph by Heisenberg, D. (2005).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

significantly more difficult to undertake in the EU and Switzerland where, in addition, the sub-units are formally involved in the consultation procedures. What is notable about the US from a comparative perspective is the degree to which many actors who are excluded –or whose interests are not taken on board during the legislative drafting process- subsequently mobilise through the courts.

4.1 Intensity of vertical interactions

The mobilisation of political actors has generated a similar policy dynamic within the three federal polities in terms of increased vertical interactions among the distinct levels of government. Furthermore, the intensity of these vertical interactions has been similarly high across the cases. In the US, despite the fact that a self-regulation framework was adopted at the federal level, the states have pursued their own measures in relation to data privacy regulation in the private sector. The absence of federal measures has led to a patchwork of competing and inconsistent regulations at the state level. This has provoked a major policy u-turn among the business community now in favour of a comprehensive federal regulatory regime. Vertical tensions between federal and state legislators have been especially prominent around the issue of spam. Here, the federal level has implemented a weak form of regulation that has effectively annulled some of the more restrictive regulatory measures that had been implemented by the sub-units, most notably in California. A similar dynamic is now evolving with regard to the private sector backed initiative to enact a comprehensive federal privacy regime. In view of the fact that most states have already enacted data privacy legislation, and that these vary considerably in scope and across domains, new federal measures will tend to trigger further vertical policy dynamics. This has already occurred in relation to the regulation of the new so-called IP services such internet telephony, where federal agencies (i.e. the FCC) have been quick to assert their regulatory jurisdiction in the area.

On the question of government initiated surveillance of cyberspace, although the US administration has been able to implement a series of federalising

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

measures, the political backlash has been significant. Important constitutional questions concerning federalism are raised as a result. That is the potential clash between the constitutional principle of supremacy and the Supreme Court's anti-commandeering jurisprudence. The latter prohibits the federal government from commandeering local and state level law enforcement officials.[130] It is particularly pertinent to the anti-Patriot Act local and state level measures. Given the heightened political context and the ongoing constitutional challenges, this can only add to the vertical interactions as important political actors resort to the Courts or pass anti-Patriot Act measures.

In the EU the first stages of increased vertical policy interactions took place around the foundational data protection directive. It was the direct result of fears among EU policymakers that diverging approaches to the regulation of data privacy among the member states could provoke distortions to the internal market. To this end, the high protection member states feared that they could be put at a competitive disadvantage by the member states that lacked a comprehensive privacy regime. The problem was framed in terms of the potential distortions to the emerging information society in the absence of EU level harmonisation. The increasing vertical interactions around the issue of data privacy resulted in the establishment of a comprehensive EU data protection regime. But this was only an interim solution, with the increasing importance attached to citizens' electronic data the related question of law enforcement's access to traffic data become a highly politicised issue. Here the vertical interactions have taken the form of a protracted competency battle between proponents of supranational first pillar initiatives versus member-state driven third pillar proposals. Although tensions persist, and various developmental trajectories can be identified, the general direction is a rather clear one. It involves increasing vertical interactions between the centre and the sub-units to negotiate a common set of EU level rules, whether through the first or third pillar, in areas that go to the very core of member state sovereignty in matters of internal security. During the past decade, the risks

[130] For a detailed discussion on this issue see Althouse, A. (2004), The Vigor of Anti-Commandeering Doctrine in Times of Terror, 69 *Brooklyn Law Review* 1231, at 1232-1233.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

associated with technological advance for the integrity of the internal market has remained one of the dominant justifications for greater EU level policy action and has served as the basis for the harmonisation of rules governing data protection. Furthermore, data privacy has now also been recently enshrined in the EU treaties.

As in the case of the EU, the development of a comprehensive data privacy regime in Switzerland has activated significant vertical interactions between levels of government. The cantons are crucial players in this domain and can mobilise significant political resources to prevent federalising measures. Developments in the Swiss data privacy domain were initiated by certain sub-units and, as in the EU, with the passing of federal-level data protection rules, a host of new privacy advocates were created. Nonetheless, with regard to data privacy in the private sector, a federalisation was achieved and this has generated considerable tensions among levels of government. Recently, with the launching of the consultation process for updating the foundational act, competency clashes have been re-activated with the sub-units mobilising against further federalisation measures. This is despite the fact that notable divergences still persist among the sub-units with regard to the implementation of the foundational act. In addition, significant tensions have arisen in certain grey areas where the public and private domains intersect. On the other hand, with regard to surveillance issues, the national scandal in which the federal police force was almost disbanded has ensured that overt federalisation measures would not be possible within the Swiss political context. This came to the fore during the consultation process for updating electronic surveillance measures where overall, and from a comparative perspective, a rather weak arrangement has been implemented. Another development, and one that parallels EU developments, is the fact that the new Swiss constitution includes provisions on data privacy and the secrecy of communications.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

4.2 Power capabilities of the centre

We now turn our attention to the power capabilities of the centre where we find considerable variance among the three systems. Although a self-regulation framework has been favoured in the US, this does not mean that federal agencies were not empowered with significant regulatory and enforcement powers. In this sense it is possible to make the argument –as many analysts have done- that despite the absence of a comprehensive data privacy regime at the federal level, US regulatory agencies are nevertheless endowed with sufficient regulatory capabilities for rule enforcement. In the consumer data privacy domain this is most clearly the case in relation to the FTC's enforcement powers. It has managed to acquire jurisdiction over website privacy policies and has pursued a successful enforcement strategy. Moreover, it is presently doing the same with regard to the spam issue, both nationally and internationally. In this sense, and especially from comparative perspective, the FTC chairman's argument about the need for more enforcement rather than new rules is certainly on the mark. In the area of government sponsored surveillance the FBI's enhanced monitoring capacities in cyberspace as a result of 9/11 has been well documented. What is important to note from comparative perspective, however, is the degree to which this federal policy actor is equipped with the resources and the investigatory powers to undertake surveillance measures both within the sub-units themselves and, increasingly, at the international level. The other significant development is the power of federal agencies, such as the FBI and the FCC, to mandate government regulations for the design of network infrastructures. The FBI's calls for greater interception capabilities in relation to IP services, and the FCC's supporting role, are provoking the latest enforcement controversies that will increasingly be fought through the Courts.

The significant power capabilities of federal agencies in the US can be contrasted with the development of multi-tiered, but fragmented, structures in the EU and Switzerland. This model is characterised by generally weak enforcement powers and this applies equally to both the EU and Switzerland. In the EU, despite the harmonisation of the substantive rules governing data protection and, increasingly, the development of an EU level regime to

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

regulate law enforcement agencies' access to internet data for internal security purposes, no central level agencies have been endowed with significant enforcement powers. Agencies have certainly been created, most notably the Federal level EU Data Protection Supervisor and the more powerful, but intergovernmental, association of Data Protection authorities. Similarly, in the area of spam an intergovernmental organisation has been established. Nonetheless, all of these agencies have very limited enforcement powers, and at best serve to coordinate the exchange of information and best practices among the sub-units, or issue policy opinions rather than take autonomous policy measures in the area of data privacy enforcement. Where it exists, enforcement is executed by the member state authorities. Although comprehensive statutory provisions exist at the EU level, there is no federal agency with the power capabilities to engage in rule enforcement and this generates patchy and fragmented enforcement patterns as the Commission is always quick to note. The only way to address the resultant enforcement gaps is to further harmonise the rules governing enforcement procedures among member state authorities. For the moment, and in the absence of central enforcement agencies, this is the incremental policy route being adopted in the EU.

In many respects, the Swiss and EU cases virtually reproduce the same multi-tiered and fragmented organisational structures. In fact it is possible to argue that the controversies between the federal agency and the sub-unit authorities have been even more conflictual in Switzerland than in the EU. Indeed, the role of the federal data protection commissioner in Switzerland has generated significant policy disagreements. Despite the weak enforcement powers of this office, one of the surprising outcomes is the fact that the cantons have created a competing association to articulate their own policy preferences. To endow the office with further powers has also been prevented by cantonal mobilisation during the consultation process. A fragmented policy context in which a multitude of privacy advocates operating at multiple levels of governmental authority, each striving to guard their prerogatives, has prevented the centralisation of enforcement powers around a federal unit. The latter's enforcement powers are thus restricted to making 'suggestions' that

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

are decided at a higher (politicised) level. A similar outcome is detectable with regard to the surveillance unit. Not even located within the federal police department, it merely serves to streamline the procedures for issuing interception orders and has no investigatory powers. The process is largely controlled by the cantonal authorities which issue the interception orders and are subsequently provided with the relevant communications data. Thus far, and from comparative perspective, the Swiss have implemented rather weak measures which are mostly related to email communications. The ongoing policy battle in Switzerland will be between the vertically fragmented privacy advocates and the security advocates operating within the police and justice departments. Whatever the outcome of these ongoing policy negotiations, a high profile federal unit capable of undertaking extensive surveillance measures like the FBI appears not to be an option within the Swiss political context.

Table 1: Data privacy outcomes

	Intensity of vertical interactions	***Power capability of centre***
US	High	High
CH	High	Low
EU	High	Low

The findings in the data privacy policy domain are summarised in table 1 above. It simply notes that, as expected, the politicisation of this policy area would generate an increase in levels of vertical interactions among levels of government usually in response to federal solutions offered by the centre. What differs when a comparative perspective is adopted is the degree to which the power capabilities of the centre vary markedly between the cases. Whereas powerful federal agencies are created or empowered in the US, the

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

structure of federalism in Switzerland and the EU prevents this type of policy trajectory.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 6: Copyright

Long before the invention of computers and the internet, intellectual property (IP) issues (which include copyright) had been a subject of politicisation. The first efforts to address the problem date back to the 15th century, although the origins of current international efforts were initiated in the late 19th century. More recently, with the creation of the World Intellectual Property Organisation (WIPO) in the 1970s, a new forum has been created for promoting the establishment of an international copyright regime. Over the past two decades, the WIPO has served as a prominent focal point for updating copyright laws. Since much of the current copyright law originated in an analogue world (e.g. cassettes and video recorders), a new regime needed to be crafted for taking account of digital technology (e.g. CD or DVD burners or PC's), which now permitted unlimited copies to be produced with no loss of quality. But this was only part of the problem. In addition, the regulatory challenge was seriously compounded by the fact that the internet could now serve as the major channel for the distribution of digital content on a global scale.[1] It is this reality that largely explains the vigorous demand on the part of rightholders for protective regimes.

In updating copyright laws for the internet era, policymakers have had to address three major issues. The first relates to certain technological measures that can serve as a shield for content owners to protect their works and even as a means for content owners to extend their rights. For instance, certain technological measures or devices can prevent users from accessing or copying digital content without permission from copyright owners. There is a downside however, since the technological measures that the content owners are implementing can limit 'fair uses' of a work such as making a copy for private use.[2] The question of 'fair use' by individual consumers, or by institutional consumers such as universities and libraries, has generated

[1] For an authoritative overview of the copyright challenge from historical perspective see Sieber, U. (1998), Legal Aspects of Computer-related Crime in the Information Society. COMCRIME Study.

[2] The 'fair use' issue is analysed in-depth by Samuelson, P. (1994), Copyright's Fair Use Doctrine and Digital Data, *Communications of the ACM* vol. 37, no. 1

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

intense policy battles. Connected to this is the issue of so-called anti-circumvention devices. Since experts can crack the protection codes without much difficulty and make the software to do this freely available on the internet, content owners have tried to legally prohibit the circumvention of their technology. The issue of anti-circumvention devices has also been one of the major areas of conflict in the updating of copyright laws.

A second issue is related to Digital Rights Management (DRM). A good example of the latter is Apple's highly successful i-Tunes, which is based on a DRM business model that offers a simple means for acquiring copyrighted content via the internet. Contrary to the collective management model whereby general tariffs or taxes are applied to products or licenses, DRM's can allow for a more exact accounting mechanism targeting the individual user. But this DRM model can challenge well established copyright traditions such as the collecting of royalties by national corporate entities known as 'collecting societies'. Since these 'collecting societies' wield a monopoly in their respective territories, their function has become politicised, especially in those polities where they play an established policy role.

Lastly, the proliferation of so-called peer-to-peer networks has offered internet users the possibilities to share vast amounts of copyrighted material for free. These networks have become the focal point for an unprecedented distribution of pirated content on a global scale. It is fair to say that, since they emerged in the late 1990s, the entertainment industry has been fighting a relentless battle to take down peer-to-peer networks.

The combined effect of these challenges has mobilised a range of private actors with conflicting functional interests as well as territorial actors with diverging cultural traditions into pursuing political action. This has left policymakers with a difficult balancing act that, in effect, seeks to broker a compromise between a set of actors wishing to create new rule structures that extend their existing rights to the new medium and a constellation of policy actors that have been mobilised to resist them. In addition, because of the cross-border nature of the problem, the regulatory challenge can pose

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

significant difficulties for federal polities in view of their multiple and overlapping jurisdictions. This can be especially difficult for policy enforcement aspects. The traditionally segmented criminal justice systems of federal systems can, in this sense, provoke significant enforcement gaps.

1. The United States

The power to regulate copyright was accorded to the federal level in the first Article of the US Constitution[3] signed in 1787. Consequently, copyright has evolved as an almost exclusively federal competence. Despite the burgeoning federal copyright law, this did not mean that no role had been left to the states in the copyright domain.[4] For example, copyright law at the state level was used to protect works from their creation until they were published and numerous other state law doctrines could be used to protect copyrightable subject matter.[5] In response, over the last century, an evolving and complicated jurisprudence of the Supreme Court[6] sought to deal with the question of the supremacy of federal law in relation to copyright and, in particular, the extent to which federal copyright law preempts state law. With the most comprehensive overhaul of the copyright domain, which took place some thirty years ago via the 1976 Copyright Act, Congress finally addressed most of the issues related to the preemption of state law.[7]

Before proceeding to the policy responses generated by the current internet challenge, it is vital to note how the legislative process in the copyright domain had come to play itself out. During the last century, and in particular throughout the post-war period, the legislative process in the area of copyright in the US has come to exhibit some very specific features. Most noteworthy

[3] Article I, section 8 states that 'The Congress shall have power .... To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries'.

[4] This is discussed in detail by Halbert, D. J. (1999), *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*. Quorum Books Westport, Connecticut. See especially p. 13.

[5] See Goldstein, P. (1989) *Copyright*. Little Brown and Company. See especially pp 471.

[6] Ibid., pp 471-472 and 495-500.

[7] Amongst the most important aspects of the 1976 act was the extension of the term of protection to life of the author plus fifty years and the extension of copyright protection to unpublished works, an area that had previously been protected by state law.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

amongst these has been the tendency for federal policymakers to delegate the legislative drafting procedure to affected industry groups.[8] A leading academic authority in the field, Jessica Litman, has offered the most succinct description[9]

> About 100 years ago, Congress got into the habit of revising copyright law by encouraging representatives of the industries affected by copyright to hash out among themselves what changes needed to be made and then present Congress with the text of appropriate legislation. By the 1920s, the process was sufficiently entrenched that whenever a member of Congress came up with a legislative proposal without going through the cumbersome pre-legislative process of multi-party negotiation, the affected industries united to block the bill. Copyright bills passed only after private stakeholders agreed with one another on their substantive provisions. The pattern has continued to this day.

The 'industry-negotiated and industry-drafted legislation approach' to copyright resulted in a series of (usually) negative consequences. Firstly, the laws tended to be long, complex and littered with numerous exceptions. This was not surprising since the main objective of the bargain was to resolve the immediate concerns of the industry players at a given policy juncture. Secondly, nascent industries tended to be excluded from the negotiating table. These features of delegated policymaking, whereby federal policymakers essentially left it to the copyright affected industries to negotiate amongst themselves a consensus on legislation, were repeated in the policy battle that erupted in the early 1990s to craft a new copyright regime for the digital age.

The first steps in responding to the internet challenge coincided with the inauguration of President Clinton, who quickly established an "Information Infrastructure Task Force" in February 1993 to formulate the incoming administration's policy towards the National Information Infrastructure (NII) as the internet was then dubbed. An IP Working group, chaired by a former

[8] Samuelson, Pamela (2002), Toward a 'New Deal' for copyright in the information age. *Michigan Law Review* 100, 1488-1505.
[9] See Litman, Jessica (2001), *Digital Copyright*. Prometheus Books, p 23.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

copyright lobbyist,[10] took a lead on the issue and its policy recommendations eventually formed the basis of a controversial White Paper published two years later.[11] Its starting point was the need for enhanced protection for copyright holders. In the absence of such protection, there would be no incentive for the content industry to make their work available and, consequently, the NII would not be realized. The White Paper boasted about the openness of its consultation process and the degree to which interested parties had contributed to the proposals.[12] Although the process may have been open, in the sense that parties were given an opportunity to comment, the fact remained that the White Paper remained remarkably faithful to the interests of the content industry, thereby following a well established historical pattern.[13]. This was evidenced by the degree of hostility to the proposals by a broad coalition of industry groups as well as by an alliance of 100 law professors who sent an Open Letter to the President.[14] Notwithstanding the hostility to the proposals, in 1995 implementing legislation was introduced in Congress.[15] However, given the critical reaction, and the mobilisation of interest groups it prompted, an easy legislative ride did not emerge. Indeed, it was to take a further three years of hard fought battles before a version of this legislation was eventually signed into law.

[10] The role of copyright lobbyists is discussed by a leading US copyright professor in Samuelson, P. (1996) The Copyright Grab, Wired, Archive 4.01 - Jan 1996. Also available at URL: http://www.wired.com/wired/archive/4.06/romer_pr.html

[11] See the Information Infrastructure Task Force, Working Group on Intellectual Property Rights, Intellectual Property and the National Information Infrastructure: A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights (July 1994). Available at: http://palimpsest.stanford.edu/bytopic/intprop/ipwg/).

[12] See page 5 of the Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (September 1995). Also available at: http://www.uspto.gov/web/offices/com/doc/ipnii/

[13] As Litman (2001), points out "[t]he substantive recommendations…were essentially unchanged." pp94.

[14] The Open Letter refers to the White Paper's suggestions and interpretations of current law as having a "radical quality" (p 60). The Open Letter was sent to the Vice-President, the Commerce Secretary, two senators and a representative.

[15] S. 1284 & H.R. 2441 104th Cong , September 28th and 29th respectively (1995). The Register of Copyrights noted that the bills adopted verbatim the legislative proposals set out in the White Paper. For a discussion see Peters, M (1996) The National Information Infrastructure: A Copyright Office Perspective. *Columbia-VLA Journal of Law & the Arts*. Vol 20 pp 349.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Immediately on the release of the White Paper, an opposition group called the Digital Future Coalition (DFC) was formed.[16] It was broad based and included membership of some twenty-seven different organisations,[17] which formed a common front to oppose the White Paper recommendations and the legislative proposals.[18] The leading ISPs were battling against being held liable for copyright infringements committed by their subscribers. The White Paper, however, had clearly rejected their calls.[19] The regulatory model envisaged –and backed by the content owners- was one in which information intermediaries, such as ISP's, would play an important policing role in cyberspace.[20]

Another problematic issue concerned the so called anti-circumvention devices. This triggered what one leading scholar referred to as the *Hollywood versus Silicon Valley* battle.[21] The former were pushing for the strongest possible ban on the use of circumvention devices. These devices could undo the technological protections that the content industries were planning to introduce. The Silicon Valley coalition[22] opposed this provision and drew attention to the negative impact it would have on, amongst other things, lawful reverse engineering, computer security testing, encryption research and public access to information.[23]

[16] For further information see their website at http://www.dfc.org/

[17] The group included libraries, ISPs, telephone companies, software and hardware manufacturers, consumer electronic companies, civil rights groups and consumer protection organisations as well as archivists and scientists.

[18] See for instance their Open Letter of 9 November 1995 available at ftp://www.arl.org/copyright/nii/dfc/dfc

[19] White Paper at page 117 noting that "they…are in the position to know the identity and activities of their subscribers and to stop unlawful activities…they are in a better position to prevent or stop infringement than the copyright owner. Between these two relatively innocent parties, the best policy is to hold the service provider liable."

[20] See White Paper page 124 "Service providers should have incentive to make their subscribers more aware of copyright law and to react promptly and appropriately to notice by copyright owner that infringing material is available on their systems".

[21] Pamela Samuelson that it would not be much of an oversimplification to say that this was a battle between Hollywood and Silicon Valley. See Samuelson, P. (1999), Intellectual Property and the Digital Economy: Why the Anti-circimvention Regulations Need to be Revised, *14 Berkeley Technology Law Journal.* 519 pp 523-24 and 542-543

[22] The coalition included leading technology companies, library associations, educational institutions and other non-profits groups

[23] See the authoritative account provided by Lessig, L. (1999), *Code and other laws of cyberspace*. New York: Basic Books.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Between 1995 and 1996 a series of congressional hearings took place in which representatives of the main industry players, civil liberties groups and educational establishments on the one hand, and the content industries on the other, battled over the question of anti-circumvention devices and ISP liability.[24] By the summer of 1996, Congressionally sponsored negotiations between the copyright industry and the ISPs over the liability issue had broken down.[25]

At this point, a surprising change in strategy was adopted. Whilst some of the core White Paper recommendations were meeting staunch opposition in the domestic legislative process, the US WIPO delegation, headed by the Chairman of the Working Group that produced the White Paper, succeeded in having the core of the White Paper recommendations taken up by the draft Copyright Treaty.[26] The draft Treaty was to be considered by the WIPO Diplomatic Conference scheduled for December 1996.[27] Concerns that international negotiations were being used as a tool to bypass the domestic legislative process were quickly put before Congress.[28] In the end, the Copyright Treaty adopted in December 1996 was shorn of the most controversial aspects of the White Paper recommendations.[29] The fact that the core White Paper recommendations did not make their way into the international Copyright Treaty did not mean that the battle between its supporters and detractors was over. The following year, new legislative proposals – this time to implement the WIPO Copyright Treaty which the US delegation had signed- were re-introduced in Congress. The new proposals retained the broad anti-circumvention provisions and made no concession on the critical issue of ISP liability however. Another round of Congressional

[24] All the testimony is available at: http://judiciary.house.gov/legacy/courts.htm

[25] This is discussed in detail by Litman (2001) pp 128.

[26] Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference, WIPO Doc. CRNR/DC74 , August 30th 1996, available at http://www.wipo.int/documents/en/diplconf/msword/4dc.doc

[27] The WIPO agenda of the US is traced in detail by P.Samuelson, (1997b) The U.S. Digitial Agenda at WIPO, *Virginia Journal of International Law*, 37 at pp 431. Samuelson points out that draft treaties were largely modelled on US digital agenda proposals.

[28] This was expressed forcefully in the testimony of E. Black in February 1996 before the Subcommittee on Courts and Intellectual Property. See testimony available at: http://judiciary.house.gov/legacy/courts.htm

[29] See especially Litman (2001) at pp 129-130.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

hearings took place during 1997-1998 in which two different versions of the legislation emerged (one by the House and the other by the Senate). As a result of the bicameral policymaking differences in this area, an informal conciliation procedure, known as a House-Senate Conference Committee on the DMCA was convened, and within a few months a final version of the DMCA was finally adopted in October 1998.

The core aspects of the DMCA as enacted marked a contrast from the initial proposals. It included certain 'safe harbour provisions' that shielded ISPs from liability, provided that they take down allegedly infringing material if they receive an infringement complaint (this would later prove to be an important weapon in the enforcement battle that followed the DMCA). A number of narrow exceptions to the anti-circumvention provisions were also included. Overall, despite the making of such concessions, there is little doubt that the final product remained heavily skewed in favour of the dominant interests of copyright holders[30]. In this sense, the DMCA followed the long established patterns of delegated legislative policymaking and bargaining noted by Litman at the beginning of this section.

The seven years since the DMCA came into force –until the end of 2005- have been witness to very significant developments in copyright enforcement strategies as content owners and, in particular, the recording industry, have used all the tools at their disposal to battle against infringing activity on the internet. One of the major players in the battle was the Recording Industry Association of America (RIAA) – the main representative of the US recording industry. In 1999 the online trading of music files through "peer-to-peer" networks exploded with creation of Napster. The latter was a company that essentially distributed software that enabled individuals to find and share copyrighted content such as music on the internet. The main point to underline is that Napster had a tremendous mobilising effect on the recording

[30] The DMCA has come in for fierce critique from leading US copyright scholars. The closest to a defence from a leading US copyright scholar is provided by Ginsburg, J. (2002), How Copyright Got a Bad Name for Itself. *Columbia Journal of Law and Arts* 26 : 61 who is willing to state that the DMCA, whatever its many imperfections, endeavours to foster a digital environment in which enhanced security encourages the digital release of works, and limitation on service provider liability promote their broad circulation.'pp 73

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

industry. Within a few months of Napster's creation the RIAA had already brought an action against it for copyright law infringement. Napster lost cases before the district court in mid 2000 and its appeal in early 2001.[31] It was held liable for the direct infringement of copyright law by its users, even though it had tried to argue, unsuccessfully, that it was essentially similar to an ISP, i.e. an information intermediary. Taxonomy mattered here, since ISP's were shielded from liability under the DMCA [32].

Apart from its wider impact on social and political consciousness, the Napster decision had tremendous regulatory implications. One legal commentator asserted that '[b]y placing the burden on copyright owners to identify potential infringers, Napster and the DMCA unwittingly expanded the reach of private regimes of copyright enforcement'.[33] This is indeed what happened and the subsequent strategy of private interests (e.g. the recording, motion picture and software industry) has been to employ twenty-four hour automated software that search websites, chat rooms and peer-to-peer file sharing sites for copyright violations. Since the DMCA provided a procedure for copyright owners to inform ISPs of infringing material, and with the new software employed by the content industry, a decentralised enforcement regime developed in which the software automatically generated notices of allegedly copyright infringing material which were served to the ISPs.[34] In this fashion the DMCA, combined with technological developments, opened up the door to ISPs being bombarded by the recording, motion picture and software industry.[35] The onus was then on the ISPs to determine whether to preclude access to the material, and thus benefit from the safe harbour provisions, or risk liability themselves. Given the incentive structure in place, it was not

[31] See A & M Records Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[32] For a detailed discussion of the Napster case see Spitz, D. and Hunter, S. D. (2005), Contested Codes: The social construction of Napster. *The Information Society*, 21: 169-180.

[33] See Katyal, S. (2004), Privacy vs. Piracy. *International Journal of Communications Law and Policy*. Special issue on Cybercrime, Issue 9, pp1-126

[34] The RIAA pointed out in late 2002 that it has stepped up enforcement of the illegal downloading of copyrighted works by significantly increasing the number of "takedown" notices sent to organizations or ISPs where copyrighted works are being offered Press Release Dec 11 2002 available at http://www.riaa.com/news/newsletter/121102_3.asp

[35] As of mid 2002 the RIAA's software robot alone had served over one million copyright violation notices to ISPs. For a discussion see Katyal (2004).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

surprising that the ISPs were likely to err on the side of caution in order to protect themselves from liability.

The RIAA also stepped up its enforcement campaign by seeking to force ISP's to disclose the identity of subscribers that it alleged were infringing copyright rules through the use of peer to peer file sharing software. The RIAA, in essence, sought a very expansive reading of the relevant DMCA rules so that it could discover the identity of individuals simply on the basis of an allegation of copyright infringement without even having to file a lawsuit. Until it was checked by a Court ruling in 2003, the RIAA embarked on a subpoena spree seeking the identity of thousands of individuals.[36] Not surprisingly, consumer privacy concerns became widespread and by September 2003, Senate hearings had been held and federal legislation was proposed to address such concerns.[37] Nothing came of the proposals, but the Court ruling in December of 2003 brought to an end the expedited subpoena spree strategy of the recording industry. Nonetheless, the Court decision did not actually prevent the RIAA from suing individuals if it instituted a lawsuit with all the due process requirements that this entailed. Although this was a lengthier process for gaining the identity of particular individuals, once it had obtained users identities it could then institute lawsuits against individuals for copyright infringement. Ever since, this has been one of the core enforcement strategies of the RIAA and every month it files somewhere in the region of seven hundred lawsuits seeking the identity of individuals from ISPs as well as many lawsuits against individuals whose identities have been obtained in this fashion.[38]

[36] The district court ruling went into effect in June 2003 and by mid September the recording industry alone is alleged to have issued well over 1600 of these subpoenas. See the testimony of M. Barr (on behalf of Verizon) available at http://commerce.senate.gov/hearings/testimony.cfm?id=919&wit_id=2581

[37] S. 1621 108th Cong , September 16th (2003). Commerce Committee Hearing, 'Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace', September 17 2003, available at http://commerce.senate.gov/hearings/witnesslist.cfm?id=919 and Subcommittee on Investigations Hearing, 'Illegal File Sharing on Peer-to-Peer Networks and the Impact of High Technology on the Entertainment Industry', September 30 2003, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_senate_hearings&docid=f:90239.pdf

[38] On this strategy see the RIAA v. The People: Two Years Later, by the Electronic Frontier Foundation (2005) and available at http://www.eff.org/news/archives/2005_11.php#004116

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Alongside the strategy of suing individuals, epitomised by the RIAA, the content industry did not relent in its attack on technology companies that distribute peer-to-peer file sharing software. Leading motion picture and recording industry representatives brought a crucial case in late 2001, which resulted in the Supreme Court's landmark Grokster decision in 2005.[39] The same content industry actors, while pursuing the litigation route, also pushed for new legislation[40] that would achieve the same aims –namely, to hold companies developing peer-to-peer file sharing software liable when their software is used for copyright violation. In June 2005 the Supreme Court ruled in favour of the content industry. One of the indirect consequences of the Grokster decision was that the restrictive legislative proposals were dropped. A bargain of sorts had been struck. Nonetheless, the decision added a new weapon to the armoury of the content industry to the effect that technology companies could now be liable for copyright infringement by third parties.[41]

The other dimension to the enforcement strategy relates to public measures and, in particular, the expanding role of centralised enforcement by federal investigative agencies. This has resulted in a mutually reinforcing alliance.[42] Given the challenges of new technologies and the rapid growth of the of the piracy problem, the DOJ has made the protection of IP rights a law enforcement priority. It has argued that an effective response to these problems requires specialized expertise that can no longer rely on traditional approaches to law enforcement.[43] Federal investigative agencies are therefore 'assisting' state and local police investigations.

---

[39] See the decision of July 2005 Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. 04-480

[40] It was known as the Induce Act

[41] Initial reactions portrayed it as a big victory for the recording and motion picture industry but many leading legal scholars consider the decision to constitute a victory for the technology industry albeit a defeat for the particular software distributors involved. That said, in the wake of the decision it seems that copyright owners have become even more assertive in protecting their rights and the RIAA for one served prominent peer to peer software distributors with letters, known as 'cease and desist letters', threatening them with legal action if they do not stop inducing infringement though also expressing a willingness to engage in settlement negotiations.

[42] This alliance is discussed in detail by Birnhack, M and Elkin-Koren, N (2003) The Invisible Handshake: The reemergence of the State in the digital environment. *Virginia Journal of Law and Technology* 8:6

[43] Deputy Assistant Attorney General Laura H. Parsky Remarks before the 'The Major Challenges of Intellectual Property Protection' Conference in Rome, Italy, October 14, 2004 available at http://www.usdoj.gov/criminal/cybercrime/parskySpeech.htm

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Since the early 1990s, successive US administrations have supported the development of such specialized federal agencies for IP enforcement operating within the individual states. A crucial step had already been taken in 1991, when in response to the growth of computer crime, a Computer Crime Unit (CCU) was established within the criminal division of the DOJ. Initially it constituted no more than a handful of lawyers who prosecuted IP violation cases. By 1996, however, it had become the specialised Computer Crime and Intellectual Property Section (CCIPS) of the DOJ and its staff has since been dramatically increased. This unit of the Justice Department is a highly specialized investigative team focusing exclusively on computer and IP crime. The prosecutors are charged with developing and implementing the DOJ's overall anti-piracy strategy throughout the country, as well as internationally. Additionally, in 2001, specialized units known as Computer Hacking and Intellectual Property (CHIPS) units with specially trained personnel to work with local and state police in the investigations of IP offences were also created. The first of these was launched in a US Attorneys Office in California and dealt with the Silicon Valley region. The efficacy of this initial unit was such that within a year the Attorney General announced the creation of nine new units in core high tech industry areas.[44]

Despite the fact that the focus of the CHIPs unit's efforts expressly included copyright violations, it appeared that the core concern here was not copyright infringement but, rather, computer security breaches. The motion picture and recording industry promptly pushed for a re-prioritisation of copyright and, in a Congressional hearing, underlined the need to re-prioritise IP enforcement so as to make it the top priority within the specialised investigative units.[45] The RIAA, alongside the MPAA, called for more funds to be devoted to the federal enforcement of copyright law.[46] In other words, the motion picture and music industries were seeking to make sure that the new CHIP units catered to their needs in the wake of the explosion of peer to peer file sharing. Within a short

[44] See Attorney General Ashcroft Remarks, July 20, 2001 available at: http://www.usdoj.gov/criminal/cybercrime/chipagsp.htm

[45] See testimonies during House Appropriations Committee, April 23 2002, the RIIA's testimony is available at: http://www.riaa.com/news/newsletter/042402.asp

[46] See testimony by J. Valenti on behalf of MPAA, and MPAA Press Release April 23, 2002 available at http://www.mpaa.org/jack/2002/2002_04_23a.htm

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

space of time, the DOJ set up in 2004 a high level IP Task Force to examine the IP enforcement efforts and to explore methods to strengthen protection as well as making legislative and regulatory recommendations. In the meantime, Congressional testimony saw the software and movie industry both welcome the increased efforts by the DOJ, whilst also stressing the need for increased funds for FBI investigations.[47] The Task Force's report, released later that year, called for the creation and expansion of the existing specialised investigative units, and to encourage victims of IP offences (i.e. the content industry) to cooperate in (i.e. to help coordinate) criminal investigations. [48] By the end of 2005, most of the high-level Task Force's recommendations had been implemented. It included the doubling of specialised CHIPs units,[49] and the sponsoring of new legislative proposals that would increase law enforcement's investigative powers, such as the interception of communications in relation to IP infringement offences.[50]

2. The European Union

Community level actions in the copyright domain began in the late 1980s with the adoption of a landmark Green Paper.[51] Framed exclusively in terms of the challenge of new technologies, it helped mobilise a powerful lobby of private sector actors who, over the course of the following two decades, would actively seek new policy measures to protect (or extend) their rights in the emerging European digital marketplace. Initial measures should be seen in the context of the early 1990s, when the dominant focus of EU policymakers was on the implementation of the 1992 Single European Market programme. Given the growing development of a European marketplace around the internal market programme, it was becoming increasingly clear that effective policy action in the copyright domain would have to be coordinated at the EU

[47] See the Senate Appropriations Committee Hearing April 29, 2004: testimony of respectively R. Holleyman and J. Valenti available at: http://appropriations.senate.gov/hearmarkups/topics.cfm?code=hearings

[48] Report of the Department of Justice's Task Force on Intellectual Property, October 2004, pages 19-28 available at http://www.usdoj.gov/criminal/cybercrime/IPTaskForceReport.pdf

[49] The number of investigative units was doubled from 13 to 25.

[50] The proposals are contained in the Intellectual Property Protection Act of 2005

[51] See the 1998 Commission Green Paper, Copyright and Challenge of Technology - Copyright Issues Requiring Immediate Action COM/88/172.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

level. What is notable about the first initiatives, however, was the significant weight attached to the role of technological change and its implications for the internal market. The framing of the copyright agenda in terms of the challenge of new technologies and the internet was not politically neutral. In fact, it was underpinned by a liberalisation agenda that would need to confront powerful member state interests in order to be implemented.

In this vein, the Commission put forward the argument that the new technologies entailed the *de facto* abolition of national frontiers and that, furthermore, the territorial application of member state copyright law had become obsolete.[52] Despite the consultation processes that were launched during the early 1990s,[53] a piecemeal approach was the most EU policymakers could agree on during this early phase. Member state traditions displayed notable divergences between the more French inspired model, where author's rights were defined as moral rights similar to human rights, and an Anglo-Saxon understanding of author's rights, defended mostly in terms of property rights.[54] Given such divergences, a 'sectoral' approach emerged during the early phase that was characterised by its relatively high level of harmonisation, but only on narrow technical matters which were of low political salience. To this end, four sector-specific directives were passed to address copyright issues. [55] The Commission, however, was keen to develop a more *comprehensive* approach. Rather than concentrating on narrow *ad hoc* issues, the comprehensive approach would establish the general framework for copyright regulation in the emerging information society. This had to be shaped at the EU level because 'a response to the challenges of new technology which is *limited* to the Member States of the Community will deal with only part of the problem'.[56] What the Commission and many private

[52] See Copyright Green paper (1988)

[53] See discussion by Burrell R and Coleman A. (2005) *Copyright Exceptions: The Digital Impact*, Cambridge University Press: Cambridge

[54] The differences between the two understandings within an EU policy context are discussed in detail by Littoz-Monnet, Annabelle (2006), Copyright in the EU: droit d'auteur or right to copy? *Journal of European Public Policy* 13:3 438-455.

[55] Copyright directives were passed in the area of 1) software programs 2) rental rights 3) satellite and cable 4) databases

[56] Follow-up to the Green Paper –Working Programme of the Commission in the field of copyright and neighbouring rights, COM (90) 584.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

actors were pushing for was a harmonised EU regime or, as it was later termed, a 'horizontal' approach.

To develop a 'horizontal' approach to copyright at the EU level would generate a considerable politicisation of the issue area which, in turn, was connected to radically different conceptions of IP among the member states. The internet –or rather the emerging information society- was the preferred rhetorical device used by EU policymakers to pursue their harmonisation agenda.[57] A fierce battle between different interest groups concerning the mode of regulation was to ensue. Moreover, for the member states and other parties, the key policy venue and bargaining arena had now shifted to the EU level. Private organisations, especially those that were sufficiently well resourced, launched a multi level approach by developing effective national, EU level and international lobbying strategies. In formulating its policy proposals, the Commission would have to strike a difficult balance between the functional interests of a number of players with widely diverging agendas: from the copyright owners, i.e. the authors and the major content industries, through to the network providers such as the ISP's and telecoms operators who were responsible for the flow of content on the internet, down to the consumers, including private users, the professions and institutional users. In contrast to the less politicised 'sectoral' phase, in trying to shape a new copyright regime for the internet environment, a host of new policy actors (such as ISPs, network providers, technology companies) had been mobilised. Moreover, the new policy actors fundamentally differed in their composition and policy preferences to the '*dirigiste*' cultural lobby of earlier phases.[58] In addition, and to add to the problem, a further balance would have to be struck between differences in member state preferences as to what constituted an appropriate protection regime for their content industries.

The consultation process launched in the mid-1990s by the Commission was to involve the major interests, both functional and territorial, in a bargaining

[57] See for instance the Commission's 1995 Green Paper Copyright and Related Rights COM(95) 382.
[58] Littoz-Monnet, Annabelle (2006).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

process that lasted a further six years.[59] The outcome of this bargaining process was referred to at the time as the most 'lobbied directive' in the Community's history.[60] It also involved inter-institutional battles between all three legislative players at the EU level -the Commission, Parliament and Council- on a number of sensitive provisions with important territorial implications. A first package of policy measures specifically addressing the internet challenge were announced in 1997.[61] The proposals drew immediate criticism from numerous interest organisations, especially the music industry. It wanted a stricter regulatory regime and pursued a unique and extremely sophisticated lobbying strategy. In a blaze of media publicity, the music industry successfully enlisted the help of around 400 pop stars who signed a petition organised by the French recording artist Jean-Michel Jarre. It was presented in 1999 to the European Parliament President, Gil Maria Robles, and the Legal Affairs Committee responsible for reviewing the Commission's proposed copyright legislation. As the music industry's representative, Jarre argued that artists 'must be allowed to use technology to protect our works. The digital era is giving us the systems to do that, but we need the laws to be able to use them. This is why the European copyrights directive is so important'.[62]

In terms of EU policymaking, this was an entirely new lobbying strategy and it was employed to extremely good effect by the music lobby.[63] On the other hand, content users felt that the proposal had been drafted too strongly in favour of copyright holders.[64] According to some copyright analysts,[65] the timescale established by the Green Paper made it almost inevitable that only

[59] The consultation process was launched after the publication of the Commission's 1995 Green Paper

[60] Hargreaves, Deborah (2001). EU and the space cowboys. *Financial Times* February 4, 2001

[61] See the European Commission's Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society, Brussels, 10 December 1997, COM(97) 628, Official Journal C108/6 of 7 April 1998.

[62] See BBC news, Pop stars fight Net piracy, January 18, 1999 available at: http://news.bbc.co.uk/1/hi/entertainment/256516.stm

[63] It was orchestrated by the IFPI according to Littoz-Monnet (2006)

[64] For instance see the comments by the Director of the European Bureau of Library, Information and Documentation Associations (EBLIDA) at the hearing of the European Parliament, Committee on Legal Affairs and Citizen rights, 30 June 1998. Available at http://www.eblida.org/position/EPHearing_Comments_June98.htm

[65] Burrell R and Coleman A. (2005).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

well-informed groups that were already geared up to respond would provide input into the drafting process. Striking a balance between the competing claims had been difficult and the Commission's first proposal appeared too favourable to the well-organised and resourced copyright holders. A new draft,[66] published in 1999, took into account some of the concerns of the content users but, most importantly, incorporated greater flexibility. This new flexibility centred on the degree to which certain 'exceptions' to the new copyright rules were to be left to the interpretation of the member states. Reaching a consensus on the issue of 'exceptions' proved difficult and the Council had to step in and ask national representatives –in the form of the Committee of Permanent Representatives- to study the matter further. A common position was finally brokered by the Council[67] in September 2000. According to two copyright scholars, the final form left in place a fairly generous system of exceptions, not because the EU legislative process had necessarily responded to the needs of users, but rather because member states had been keen to limit disruption to their existing arrangements.[68] To this end, the member states had retained sufficient flexibility to allow them to keep their lists of exceptions more or les intact. Member state divergences were too great to fully harmonise copyright traditions, and given that it touched on sensitive areas, the 'cultural lobby' could mobilise effectively through national governments.[69]

With the compromise agreement in place, it was possible to adopt in 2001 the most lobbied directive in the Community's history[70]. It represented the culmination of EU policymakers' attempts to establish an EU-wide copyright regime to meet the challenges posed by new technologies, and the internet in particular. Despite the exceptions, by harmonising substantive legal rules

[66] See the Amended proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society COM/99/0250 final

[67] Common Position (EC) No 48/2000 of 28 September 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a Directive of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society.

[68] See Burrell R and Coleman A. (2005).

[69] See Littoz-Monnet, Annabelle (2006).

[70] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

among the member states, it provided the general framework for copyright regulation in the EU. At the same time it created a new, and mostly intergovernmental body, known as the 'Article 12 Contact Committee'. Made up of Member States representatives, with participation of the Commission, it would, henceforth, be responsible for dealing with questions deriving from the application and implementation of the directive. Implementation problems surrounding the new copyright rules could be anticipated and, therefore, in order to underscore the importance attached to the new regulatory regime, it was agreed that an expedited implementation schedule should take place within 18 months of adoption.

This has caused a number of problems for some member states largely because many of the difficulties experienced at the EU level were played out again at the domestic level. Not surprisingly, this has led to notable implementation gaps. To address these gaps, the Commission has made recourse to infringement proceedings and has signalled that it would vigorously 'pursue infringement proceedings procedures until all Member States have written the Directive into national law'.[71] By late April of 2005, six Member States had been held to be in breach of their obligations under the Copyright directive.[72] Several Member States were then threatened with further legal action which could have resulted in the imposition of fines by the ECJ,[73] and all but one of them – France - have since transposed the Directive.[74]

An effective copyright regime would of course require more than just the transposition of laws. It would also entail tackling a number of sensitive issues concerning the application and enforcement of the new rules. This raised two major issues: first, the regime for copyright clearance, which would entail

[71] European Commission Press Release Commission moves against 13 member state for failure to implement EU legislation, 14 July, 2003 (IP/03/1005)

[72] Spain, France, Finland, Sweden, Belgium, UK. Cases 31/04, 59/04, 56/04

[73] European Commission Press Release Copyright: Infringement proceedings against France, Finland, Spain and Czech Republic for non-implementation of 2001 Copyright Directive, 13 July, 2005 (IP/05/921)

[74] European Commission Press Release Copyright: Infringement proceedings against France, Finland, Spain and Czech Republic for non-implementation of 2001 Copyright Directive, 13 July, 2005 (IP/05/921)

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

confronting powerful member state organisations; and second, the enforcement of copyright rules, which would raise sensitive third pillar questions relating to the harmonisation of criminal sanctions and penalties and the framework governing enforcement by private parties.

On the first issue, the model of copyright clearance was segmented along national lines and controlled by well organised member state 'collecting societies'. For the Commission, and many content providers,[75] the territorial principle underpinning copyright clearance in the EU served to restrict or distort competition. In practice, this meant that commercial users required a licence from each and every collecting society across the EU. The Commission's aim was to secure an EU-wide copyright clearance model that was, as the Internal Market Commissioner argued, more in tune with the internet age rather than the nineteenth century.[76] However, in order to create an EU level playing field, the Commission would have to confront the vested interests of the powerful collecting societies who, in effect, wielded a *de facto* national monopoly in their respective territories.

Even before the formal adoption of the 2001 EU Copyright Directive, Commission policymakers had clearly signalled that they intended to pursue further EU level coordination in the area of copyright clearance.[77] However, in a pre-emptive move, most of the EU member states' collecting societies signed up in 2001 to a bilateral reciprocal arrangement known as the Santiago Agreements which was notified to the Commission in early 2001. To the Commission this appeared like a cartel that could endanger the roll-out of online services and it therefore issued a formal notice to the relevant parties

[75] See for instance the comments of GSM Europe association during the 2005 consultation process. Available from: http://ec.europa.eu/internal_market/copyright/docs/management/consultation-rights-management/gsme_en.pdf#search=%22european%20commission%20consultation%20GSM%20europe%20comments%20collecting%20societies%20%22

[76] See Speech by European Commissioner for Internal Market 07/10/2005, 'Music copyright: Commission recommendation on management of online rights in musical works' SPEECH/05/588

[77] Meetings took place in Florence (1996), Vienna (1998) and specially convened hearing in Brussels in 2000. In particular, see the Conclusions of the European Commission Hearing on Collective Management, Brussels, 13-14 November 2000, available at http://europa.eu.int/comm/internal_market/copyright/management/hearing-collective-mgmt_en.htm

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

and invited interested third parties to submit observations.[78] Furthermore, the arrangement was still rooted in a territorial principle that effectively granted the same monopoly to the national collecting societies for internet services as they traditionally held in the offline world. The Commission wanted to introduce further competition between collecting societies in order to break up the territorial monopoly. As the Internal Market Commissioner put it 'once upon a time it may have made sense for the member state to be the basic unit of division. The internet overturns that premise'.[79]

On the basis of its investigation and the comments received from third parties, the Commission issued a statement of objections –the first stage in a legal procedure- to the collecting societies in 2004. [80] Alongside the aforementioned legal challenge,[81] the Commission also outlined its policy agenda for an EU-wide licensing arrangement in order to harmonise rules and address the significant divergences among the operational procedures of the national collecting societies.[82] At the same time, it noted its aim to establish external control mechanisms through the creation of specific bodies (i.e. to create a new EU level oversight body).[83] Within the space of a year, however, the Commission's plans for regulatory intervention had to be completely watered down. This was due, in large part, to the successful mobilisation against EU action by the national collecting organisations during the consultation process.[84] The Commission's approach had to be scaled down, and targeted

[78] See the European Commission's 'Notice on the Santiago Agreement' OJ C 145/2 of 17 May 2001.

[79] See Speech by European Commissioner for Internal Market 07/10/2005, 'Music copyright: Commission recommendation on management of online rights in musical works' SPEECH/05/588

[80] See Europa Press Release 'Commission opens proceedings into collective licensing of music copyrights for online use' IP/04/586.

[81] The legal challenge is ongoing, the Dutch and Belgian collecting societies however responded separately to the Commission's 2004 statement of objections by undertaking to address the Commission's concerns. See Notice published pursuant to Article 27(4) of Council Regulation (EC) No 1/2003 in Cases COMP/C2/39152 — BUMA and COMP/C2/39151 SABAM (Santiago Agreement — COMP/C2/38126). OJ C 200, 17.08.2005, p. 11-12.

[82] European Commission Communication on the management of copyright and related rights in the internal market, COM/2004/261

[83] See in particular pp19 of the European Commission Communication on the management of copyright and related rights in the internal market, COM/2004/261

[84]See the results of the consultation exercise and the responses from interested parties available at: http://europa.eu.int/comm/internal_market/copyright/management/contributions_en.htm

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

at a specific challenge, the provision of online music services[85]. Much to the dismay of commercial users,[86] the regulatory discourse and the harmonisation model was abandoned. The national collecting societies had effectively forestalled EU harmonisation attempts, at least for the moment. Indeed, the Commission readily admitted in its paper that 'the CRMs [the collecting societies] and their umbrella orgnisations are *powerful collective actors* who…are effectively engaged in self-regulating their trans-national relationships' (authors italics).[87] For the moment the EU-wide licensing arrangement is predicated on a self-regulation model, in which voluntary codes of conduct are agreed by the respective member state collecting agencies, and where the major regulatory goals are set and monitored by the Commission.[88] For the time being, national collecting agencies have managed to avoid harmonisation measures and control mechanisms that may have led to the creation of a formal EU supervisory agency. On the other hand, the threat of regulation has generated a degree of reform through the use of soft law mechanisms.

The other side of the implementation problem relates to enforcement. This is largely because, in the absence of an appropriate enforcement regime, copyright rules can only be partially effective. In terms of decentralised enforcement by private parties, an important role has been played by the International Federation of the Phonographic Industry (IFPI), an organisation that essentially serves to create, and promote, the rights of the international recording industry.[89] It has a European regional office, located in Brussels, and numerous local offices within EU Member States. Since anti-piracy enforcement is a key aspect of the IFPI's strategy, it has sought to use a

[85] European Commission Staff Working Document, 'Study on a community initiative on the cross-border collective management of copyright', 2005, available at: http://europa.eu.int/comm/internal_market/copyright/docs/management/study-collectivemgmt_en.pdf

[86] For instance see the comments of BSA, as well as other commercial users, on the new approach, available at: http://forum.europa.eu.int/Public/irc/markt/markt_consultations/library?l=/copyright_neighbouring/cross-border_management&vm=detailed&sb=Title

[87] See pp30 of the European Commission Staff Working Document, 'Study on a community initiative on the cross-border collective management of copyright', available at: http://europa.eu.int/comm/internal_market/copyright/docs/management/study-collectivemgmt_en.pdf

[88] See the Commission Recommendation of 18 May 2005 on collective cross-border management of copyright and related rights for legitimate online music services OJ (2005/737/EC)

[89] See http://www.ifpi.org/site-content/about/mission.html

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute
DOI: 10.2870/1208

similar litigation strategy within the EU as it has done in the US in order to clamp down on copyright infringement most notably in the peer to peer context. However, since there is no central EU-level body with which it can cooperate on enforcement aspects, the enforcement strategy is pursued through the individual member states. Essentially, there are two major problems constraining this enforcement strategy: first, the strong data protection rules mean it is more difficult and costly to obtain alleged infringers identities; second, the considerable variation among the member states' investigative and prosecution authorities reduces the effectiveness of this type of enforcement strategy.

On the other hand, enforcement by EU level authorities in the copyright domain raises sensitive third pillar issues for the member states. This is especially the case in areas related to the harmonisation of sanctions and penalties. In fact, this has generated a series of cross-pillar battles that are essentially competency clashes. In many respects, the Commission, with strong backing from the entertainment industries, had already launched its enforcement agenda well before the adoption of the landmark copyright directive of 2001. To justify the need for new enforcement rules the policy discourse was shifted towards framing the threat of piracy as a pan-European problem involving organised criminal groups who exploited the internet for large-scale infringement.[90] It was an internal security problem that, according to the Commission, now threatened the internal market. To make matters worse, the levels of legal sanctions and the severity of the penalties varied considerably among the member states with some not even providing for criminal penalties.[91]

Such divergences were clearly not satisfactory for content owners who wanted stricter EU-level rules. Moreover, they found a valuable ally in the Commission, which was also keen to strengthen its own enforcement powers. The problem was that, apart from raising sensitive law and order sovereignty

[90] See the European Commission's (1998) Green Paper on Combating Counterfeiting and Piracy in the Single Market. COM(98)569.

[91] See pp 18 of the European Commission's (1998) Green Paper on Combating Counterfeiting and Piracy in the Single Market.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

issues, penal sanctions were considered to be outside the scope of the Commission's legislative powers. Still, given the perceived dangers that piracy posed to the internal market, the Commission signalled its intention to take a hands-on approach to the prevention of infringements of Community law.[92]

A consultation process was launched that especially mobilised copyright holders who were keen to strengthen their rights in the digital environment. The culmination of the consultation process occurred at the German Council Presidency of March 1999 where national representatives and interested parties (including industry and other stakeholders) met and endorsed an EU plan for responding to the piracy threat.[93] The outcome was a set of policy proposals to address the enforcement of IP rights. Endorsed in 2003, the new policy initiative tried to juxtapose two sets of issues: first, the link between the disparities in criminal penalties for piracy offences and the distortions this was apparently creating to the EU's internal market; second, the proliferation of new technologies, especially the internet, which the Commission argued were being increasingly used by organised crime groups.[94]

Two provisions in the Commission's proposal were particularly problematic from a competence perspective since they required member states to classify serious infringements as criminal offences punishable by criminal penalties.[95] For the Commission to introduce such provisions into a Community directive was deemed by many Member States to be outside the scope of the first pillar.[96] This is because issues related to the imposition of criminal sanctions were considered to constitute a third pillar competence governed by the intergovernmental method of policymaking. It was not surprising that the provisions would therefore provoke controversy in the Council. The proposal

[92] See the Commission's (1998) Green Paper on Combating Counterfeiting and Piracy in the Single Market.

[93] This led to the Commission's (2000) Communication from the Commission to the Council, the European Parliament and the Economic and Social Committee. Follow-up to the Green Paper on combating counterfeiting and piracy in the single market COM (2000) 789

[94] See the European Commission's Proposal for a Directive on measures and procedures to ensure the enforcement of intellectual property rights COM(2003) 46

[95] See articles 4 and 20 of the Commission's proposals IPR enforcement directive of COM(2003) 46

[96] See the House of Lords Select Committee on European Scrutiny Twelfth Report. Enforcement of intellectual property rights. (a). (24313). 6777/03. COM(03) 46. (b). (25394). Available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmeuleg/42-xii/4217.htm

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

was promptly amended and a more flexible terminology was adopted merely requesting that member states apply 'appropriate' sanctions in cases of copyright infringement. With this amendment in place, the enforcement directive was, for EU standards, swiftly adopted in less than 14 months.[97]

Within the space of a year of the adoption of the enforcement directive, two new proposals to strengthen the enforcement of IP rights were put forward by the Commission. The two, a proposal for a Directive and one for a Framework Decision, were jointly published and represent the EU's new enforcement agenda.[98] The former was geared exclusively to issues related to enforcement. However, it was supplemented by the Framework Decision (governed by the third pillar legislative process) which specified the level of penalties and the rules governing the initiation of criminal proceedings. The framework decision included provisions that would allow for the setting up of a new type of investigation team that would, in effect, enhance copyright owners' access to national law enforcement bodies. Article 4 stated that 'Member States shall ensure that the holders of IP rights concerned, or their representatives, and experts, are allowed to assist the investigations carried out by joint investigation teams'. With such rules in place, representatives of copyright owners, such as the music or film industry, could be allowed to assist in the criminal investigation. It is not surprising that the copyright coalition was firmly in favour of such measures since it meant that copyright infringers, potentially even small scale individual suspects, could be investigated by the police of member states instead of requiring a potentially expensive civil lawsuit. Moreover, it would require further harmonisation at the EU level of both the substantive legal norms concerning criminal offences and penalties, as well as the regime governing the procedural aspects of investigating copyright infringement across the EU.

[97] See Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights

[98] See the Commission's Proposals of 2005 for a Directive and a Framework Decision COM (2005) 276

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

But as a result of a recent groundbreaking ECJ judgment,[99] the Commission has changed tack. The case involved a Commission challenge to a Council framework decision adopted under the third pillar that required member states to impose criminal sanctions for certain environmentally harmful acts. Crucially, the ECJ found the decision invalid because it could have been adopted under the first pillar.[100] The Commission immediately issued a Communication in which it argued that the principles laid down in this case were not specific to the environmental sphere and could be applied to other policy areas (e.g. copyright enforcement) where the closer approximation of criminal penalties was necessary to achieve internal market goals.[101] The judgment itself, as well as the breadth of the Commission reading has not gone uncontested and is causing disquiet among some of the member states.[102] In the meantime, the Commission withdrew its earlier joint proposals (i.e. the first pillar Directive and a third pillar Framework Decision) and re-submitted them as a single amended Directive on criminal measures for enforcing IP rights.[103] What the Commission has done, in effect, is to re-introduce all the core provisions, including the joint investigation teams, under a legislative procedure where it has considerable agenda setting powers. Put simply, the Commission considers the recent ECJ judgment to have provided it with the authority to pursue such criminalization of IP infringement under the first pillar and it has responded accordingly.

[99] The case of Commission v Council (C-176/03), decided on 13 September 2005, involved an action for annulment of Council Framework Decision 2003/80 on the protection of the environment through criminal law. As the House of Lords report points out at para 3 "Until September 2005 it was commonly understood that the Treaty establishing the European Community (the EC Treaty or TEC) conferred no power to define criminal offences or prescribe criminal sanctions."

[100] See C-176/03 Commission v. Council, [2005] ECR I–7879. It is useful to note that eleven member states intervened in support of the council

[101] See the European Commission's Communication on the implications of the Court's judgment of 13 Septmber 2005. COM (2005) 583

[102] See the Report of the House of Lords EU Committee, The Criminal Law Competence of the European Community, July 2006 available at: http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeucom/227/22702.htm. And the hearing before the French Senate in February 2006 available at http://www.senat.fr/europe/r22022006_1.html

[103] See the Commission's Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights COM/2006/168 (2005/0127 (COD))

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

3. The Swiss Confederation

While its European counterparts, such as Britain and France, were busy developing national regulations in the area of IP during the early 19th Century, the idea met with opposition from the Cantons in Switzerland. For almost fifty years the Cantons effectively blocked federalising initiatives until 1883, when the first federal copyright legislation was passed. Shortly thereafter, a federal Institute of Intellectual Property was created and, over the last century, it has acquired considerable agenda-setting powers to become one of the major policy actors in the Swiss copyright domain.

The Swiss Federal Institute of Intellectual Property (known in its German acronym as the IGE) is responsible for all matters relating to IP in Switzerland. Although it is linked to the Federal Police and Justice Department, as an independent agency and relative to others in Switzerland, it is financially and operationally considerably autonomous. Its main task has been to take a lead role in the formulation of IP legislation, a role that would be tested when trying to broker a compromise among the disparate interest groups involved in the updating of Swiss copyright law for the digital era. But the IGE's principal role is to actually supervise the collecting societies of Switzerland.[104] To understand the copyright battles of the last decade in Switzerland, it is imperative to take account of the collecting agencies, and the corporatist type of arrangement that underpins their role in the policymaking domain of copyright.

The collecting societies are functionally organised according to a number of fields (e.g. music, literature, film, theatre) although there is certain segmentation reflecting the distinct linguistic groups. In effect, however, these collecting societies operate with a single voice at the national level despite some historic differences among the distinct linguistic groups. Traditionally they have played the major role in protecting creators' rights by collecting royalty payments. Given their monopoly position, the collecting societies and

[104] For further information see the website of the Swiss Federal Institute of Intellectual Property at: http://www.ige.ch

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the amount of royalties and tariffs that are applicable are all regulated by the federal agency.

With the challenge of updating the Swiss copyright regime, the cosy bargaining model would come under pressure. A disparate range of new policy actors and interest groups, both public and private, were immediately mobilised to address the internet challenge. In fact, some groups began to challenge the corporatist arrangement underpinning the collecting societies' privileges. For instance, between 1998 and 2002, a number of parliamentary interventions and motions had called for a reinforcement of user's rights *vis a vis* the collecting societies.[105]

The other element that needs to be taken into account is that the Swiss delegation signed the WIPO Internet treaties of 1996. Swiss policymakers thus committed themselves to revising their copyright regime. A decade later, the fact that, as of the end of 2005, this has still not been achieved invites explanation. Gradualism and consensus seeking is quite typical for the Swiss policymaking process and its slowness should therefore come as no great surprise. Moreover, the historical track record did not provide optimism for a speedy legislative process. Indeed, the current rules governing the Swiss copyright regime, the Copyright Act of 1993, had been over thirty years in the making leading some copyright commentators to refer to it as the '30 years War'.[106] Thus, it is not at all surprising that the copyright revision for the digital age would be a lengthy policy affair. In addition, the National Assembly had also stipulated that in conducting the copyright revision process for implementing the Internet Treaties, attention should be paid to the European Union Copyright Directive, which was not passed until 2001. The problem, however, was that following the EU model would mean a more comprehensive protection of technological measures because the Directive, much like the US DMCA, went beyond the requirements of the WIPO.

[105] See the following interventions: 98.3389 postulat Widrig; 99.3347 postulat Imhof; 99.3557 postulat Christen; and a parliamentary motion 02.3322 motion Triponez

[106] Lindner, Brigette (2005) Demolishing copyright: The implementation of the WIPO Treaties in Switzerland. *European Intellectual Property Review*, 27(12), pp 481-488. WHAT PAGE

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Following a parliamentary motion in 1997, the IGE set out on preparing an initial draft.[107] By 2000, an informal draft proposal had been sent to all the relevant interest groups, thus initiating the start of the informal consultation procedure. The aim of the proposal was to close certain gaps in the existing copyright law, including issues related to liability and technological measures, so as to make Swiss copyright law WIPO compatible. At the same time, the rules governing the collecting societies were to be amended.[108] According to the federal regulator, the proposals generated substantial conflict among the disparate interest groups, with some groups (mostly the representatives of copyright holders) viewing them as not going far enough while others considered them an unacceptable expansion of property rights (mainly the institutional users and consumer groups).[109] In fact, according to one source,[110] a completely new actor[111] –one that represented consumer groups- was mobilised and emerged as a key player in the collective bargaining process.

In order to find a compromise the IGE director proposed the creation of a number of Working Groups (WG's) to try to reach a consensus. In 2002 four WG's were created to study the problem, with one dedicated to the especially delicate role of the collecting societies.[112] Over the course of the following year, numerous (19) hearings took place and apart from certain rules applying to disabled users, no consensus was forthcoming. The IGE recognised that, on the basis of the WG's sessions, reaching a consensus in the forthcoming formal consultation procedure would be a difficult and arduous task.[113] Over the course of 2003-2004, and after taking stock of its preparatory work over

[107] La protection du droit d'auteur et nouvelles technologies de la communication, Motion 97.3008

[108] See the Circular letter and the summary report of the informal consultation which lists all the participating actors. Available at http://www.ige.ch/D/jurinfo/documents/rs_kon_erg.pdf.

[109] See the IGE's Circular letter for the evaluation of the informal consultation of April 4, 2001. Available at http://www.ige.ch/D/jurinfo/documents/rs_kon_erg.pdf. See also the IGE's summary of the results of the informal consultation, available at http://www.ige.ch/D/jurinfo/documents/rs_kon_erg.pdf

[110] Interview with federal official at the IGE 23/11/05

[111] This was la Fédération des Utilisateurs de Droits d'Auteurs et Voisins.

[112] Groupe de Travail 1, Utilisateurs/societes de gestion.

[113] See the Institut Fédéral de la Propriété Intellectuelle (2003) Révision partielle de la LDA: rapport final sur les travaux des groupes de travail, available at http://www.ige.ch/F/jurinfo/documents/j10301f.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the previous six years, the IGE released a draft law[114] in September 2004, which was sent to the cantons, the political parties and the major interest groups, formally initiating the consultation procedure. Although all parties agreed that the copyright law needed to be modified in view of technological developments, it was far from clear which model the Swiss would pursue. While the entertainment industry was clearly in favour of a regime closer to the EU model, with its rather more generous protections which went beyond the WIPO requirements, consumer groups and public institutional users were concerned about the royalty system and the role of collecting societies. One of the most influential Swiss business lobbies argued that 'the exploitation of works will expand decisively in the digital age. Regulations need to be conformed accordingly and the antiquated royalty systems dominated by monopolies and collecting societies need to be rethought."[115] Moreover, the cantons (as well as communal representatives) appeared to be also worried about the financial implications of the proposed laws. They were particularly concerned about potential increases in the royalties charged by the collecting societies. As the principal paymasters for educational institutions and the cantonal public administration, the cantons would have to incur extra financial burdens[116]. In other words, the cantons were mostly concerned with making sure that, as the largest institutional public consumers of copyright material, excessive royalties were avoided.[117]

While there was an ample consensus on the need for revision of the Swiss copyright regime, the divergences among the collecting societies, institutional users and consumer groups was so great on measures to combat digital

[114] Interview at IGE 23/11/05

[115] See the comments by Thomas Pletscher, Executive Board Member of economiesuisse (the influential Swiss business lobby group) in the specially commissioned report by the Swiss Federal Institute of Intellectual Property (IGE), Copyright in the digital age: Highway or dead-end? pp 11, Available at http://www.swiss-copyright.ch/E/documents/pocketguide_e.pdf

[116] See in particular the comments from the Canton and Republic of Neuchatel, and Canton Vaud. See the Swiss Institute for Intellectual Property, Stellungnahmen betr. Vernehmlassung zur Revision des Urheberrechtsgesetzes
http://www.ige.ch/D/jurinfo/j10301.shtm

[117] See the comments of Dr. Marcel Guignard, Mayor of Aarau and President, Swiss Union of Cities in the specially commissioned report supra note ????

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

piracy that no agreement was possible.[118] At this point, the focus shifted towards simply implementing the basic requirements for ratifying the WIPO treaties. All the problematic issues were taken out of the text – a relatively straightforward task. This would enable Switzerland to ratify the international treaties.[119] It was expected that a text would be agreed in 2006 and the Treaties would enter into force the following year.[120] Addressing the much more contentious issue of revising the copyright regime –which would require reaching a consensus among all the interested parties- would have to wait. No doubt with a notable touch of hyperbole, one copyright lawyer has described the process as follows

> Surrounded by 25 EU Member States which are all obliged to comply with the terms of the Copyright Directive, Switzerland also risks becoming a home for unlawful online services and manufacturing outlets of circumvention tools which would be no longer allowed in the European Union. Can this really be the goal of the Swiss WIPO Treaties implementation?[121]

The other side of the copyright challenge relates to the thorny issue of enforcement. In relation to enforcement, and especially with regard to combating piracy, a number of organisations were created. Already in 1988, a Swiss anti-piracy federation (SAFE) organisation had been founded to represent the copyright holders.[122] An umbrella organisation of the major copyright interests, it focused its attention firmly on prioritising the enforcement agenda of the content industry. More recently, a new public-private organisation (the Swiss Anti-Counterfeiting and Piracy Platform) has also been created. Housed at the IGE, it aims to bring together private and governmental interests at all levels so as to enable the diverse interests to coordinate their strategies.[123]

---

[118] Comunicato per la stampa, Servizio d'informazione, Dipartimento Federale di Giustizia e Polizia, *Prosegue la revisione del diritto d'autore*, Berna 10.06.2005, available at http://www.ige.ch/I/jurinfo/documents/j10308i.pdf

[119] Interview with official from the IGE, 23/11/05

[120] See in particular the Comunicato per la stampa, Servizio d'informazione, Dipartimento Federale di Giustizia e Polizia, *La protezione del diritto d'autore nell'epoca della tecnologia digitale*, Berna, 10.03.2006.

[121] Lindner, Brigette (2005).

[122] Further information is available from the Association Suisse pour lutte contre le piratage, at http://www.safe.ch/

[123] See the Swiss Anti-Counterfeiting and Piracy Platform position paper available at http://www.ige.ch/E/jurinfo/documents/j10718e.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

The need to coordinate was especially relevant because of some gaps in Swiss law related to file-sharing services, such as the peer-to-peer networks. In Switzerland most legal analysts tend to agree that downloaded copyrighted content that is used for making a private copy for personal use is permissible under current Swiss law.[124] What is not permissible, however, is making copyrighted data stored on one's hard disc available to other users.[125] This legal lacuna revealed some of the enforcement dilemmas confronting the content industry in Switzerland since downloading music files from peer-to-peer networks could be construed as legal.

In 2004 the biggest Swiss ISP, in a voluntary collaboration with the music and movie industry association, began to send emails to some of its subscribers that were allegedly illegally sharing music and video files. The content industry employed specialised private companies that were able to track the particular IP number back to a Swiss ISPs.[126] Although the private companies could identify the IP numbers of the alleged infringers, only the ISP's possessed the information necessary to identify the subscriber. The ISPs were unwilling, however, to pass on subscriber identities to the content industry representative, not least because of the bad publicity that this could entail (as it had in the US).

A year later the Swiss branch of the international music association (the IFPI), changed track and employed a much more aggressive strategy. Known as 'game over'[127], it heralded the beginning of the litigation approach to anti-piracy in Switzerland. However, the cooperation of cantonal authorities would be especially useful for effectively pursuing this strategy. This is because the investigation of copyright violation, whether by civil or criminal procedure, is a

[124] Interview 23/11/2005 IGE official

[125] For a discussion see Rohmer, Sandrine and Bloise, Joelle (2003) Le mp3 face au droit d'auteur du point de vue des utilistiers. *Pratique Juridiques Actuelle*, pp 51-57.

[126] Swissinfo, *Cher client, vous n'êtes qu'un pirate!*, January 21, 2004, available at http://www.swissinfo.org/eng/search/detail/Cher_client_vous_n_tes_qu_un_pirate.html?siteSect=881&sid=4652127&cKey=1075317537000

[127] See the Press Release by the Groupe national suisse de International Federation Of Producers Of Phonograms And Videograms, Zürich, le 3 novembre 2005 - L'industrie de disque avertit les pirates de musique moyennant des «messages instantanés», available at http://www.ifpi.ch/f/main_f.html

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

cantonal matter. Furthermore, the ISP's refused to cooperate, and used data privacy rules as a justification for not revealing subscribers' identities.[128] Only a cantonal investigative magistrate could force an ISP to reveal the identity of its subscribers. In 2005, the IFPI therefore began to file civil and criminal complaints in order to get the ISP's to reveal its subscribers' identities.[129] This was a controversial strategy that has generated a storm of criticism.[130] It also raises issues of federalism since there is no federal prosecutor or investigative authority that deals with this. Following the criminal procedure approach is, however, likely to be frustrating in Switzerland, since the cantonal authorities who are charged with investigation are overworked and do not have copyright violation high on their criminal enforcement agenda. Moreover, none of these authorities would actively seek evidence, but, would rather have to be provided with it.[131] The issue of privatised enforcement by specialised IT companies is controversial and raises serious data protection issues, which in Switzerland are taken quite seriously. In this sense, it will be no straightforward task for those private interests seeking to implement their enforcement agenda in the Swiss context with 26 different prosecution and criminal investigative authorities that do not view copyright violation as a major criminal or civil legal issue.

4. Comparative Review

The copyright battles of the last decade exhibit features that suggest a fruitful area of policy inquiry for examining similarities and differences among the three cases. One important point to underline, however, is that in tandem with the bargaining process taking place within the three federal systems, a copyright agenda had already largely been framed at the WIPO level. Negotiated by an epistemic community of policymakers operating at national

[128] Swissinfo, *Piratage sur internet: contrôles renforcés*, June 25, 2006, available at http://www.swissinfo.org/eng/search/detail/Piratage_sur_internet_controles_renforces.html?siteSect=881&sid=6845595&cKey=1151241208000

[129] According to Swissinfo, 70 criminal cases have been filed with the cantonal penal authorities Swissinfo, *Piratage sur internet: contrôles renforcés*, June 25, 2006, available at http://www.swissinfo.org/eng/search/detail/Piratage_sur_internet_controles_renforces.html?siteSect=881&sid=6845595&cKey=1151241208000

[130] See the 'Lettera aperta sulla LDA alle associazioni dei consumatori e dossier sulla LDA'. From the Associazione di Diritto Informatico della Svizzera italiana. Available at http://www.adisi.ch/lda.html

[131] Interview on 23/11/06 with federal judge at IGE.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

and international policy levels, the adoption of the two so-called WIPO internet treaties in 1996, established a set of minimum international standards. Nonetheless, the major policy clashes within each of the federal systems were not so much about the implementation of the international treaties, but rather about how much further the domestic policy measures would go beyond the minimum requirements of the WIPO arrangements.

In this sense actor mobilisation has exhibited notable similarities across the three federal systems, especially in terms of producing a new coalition of policy actors, namely network providers, technology companies, and consumer groups and/or institutional users. In all three systems, the newly empowered actors challenged the more established players, the content owners and their representatives. To this end, the nascent policy players altered the delegated legislative bargaining model whereby interested parties negotiated outcomes amongst themselves. Although this is most obviously the case in the US, it also applies to both Switzerland and the EU. In a nutshell, there were two major factors that explain the successful mobilisation against these well entrenched interests. First, the stakes were much higher given that the focus of the negotiations was not on a narrow area of copyright law. Instead, the outcome of the policy bargain would define access to creative content on the new internet medium for the next generation. Second, despite the well entrenched interests of the strong 'copyright' lobby and their privileged access to policymakers, the competing coalition was also well endowed with political resources. The interaction of these two elements largely explains the intensity of the policy battles in the three federal polities.

At this point it is worth considering the notable dissimilarities between the cases. Especially noteworthy, are the differences in processes of interest intermediation, that is between pluralist and more corporatist processes. The main point to underline in this respect is that it was largely producer interests that determined policy in the US. In Switzerland however, the process has been characterised by a more corporatist bargaining arrangement in which peak associations negotiate amongst themselves with a federal oversight agency (the IGE) playing an agenda setting role and trying to broker a policy

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

compromise among the divergent interests. Also in the Swiss case a major policy role can be attributed to corporate entities such as the 'collecting societies'. Such organisations do not play such an important role in the US policy context. This is in direct contrast to the EU where, as in Switzerland, these national monopolies are influential policy actors. Thus, despite certain pluralist elements, the EU bargaining process was similarly corporatist with the Commission trying to broker a compromise between the divergent functional and territorial interests. The latter in particular added a significant additional constraint to the EU policy process.

4.1 Intensity of Vertical interactions

If we focus on the degree to which vertical policy interactions among levels of government have been activated, a number of considerable differences can be identified across the cases. Whereas in the US, vertical policy dynamics were not present in any significant measure, in the EU, on the other hand, they mattered and had a considerable impact on the final policy bargain. As has already been noted, the US agenda was principally driven by producer interests operating within a pluralist policy process. The sub-units did not act in any corporate sense. The policy battle was overwhelmingly related to the mode of regulation rather than level of regulation. To a certain extent this was similar to Switzerland where vertical interactions among levels of government were also less significant compared to the EU. This is not unrelated to the fact that copyright has been effectively federalised in both the US and Switzerland. Notwithstanding the degree of federalisation, it is notable that in Switzerland the sub-units were still formally involved, and played an active role, during the consultation procedures. Moreover, they had a clear set of preferences with regard to the role of the collecting societies and the resulting financial implications of the emerging policy bargain. Of the two cases the consultation process in Switzerland, which is both more consensus seeking and open to territorial interests, came closest to the EU model.

In the EU, the copyright policy agenda activated intense vertical policy interactions mainly because of the diverging national traditions in this

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

sensitive policy domain. Although a degree of harmonisation was achieved, a rather flexible system of exceptions was left in place to minimise the disruption to member states' existing arrangements. Unlike Switzerland and the US, which have over a century of harmonisation efforts behind them, the EU is still at an evidently earlier stage of copyright federalisation. Nonetheless, the trend is clearly towards a greater degree of federalisation and this will inevitably continue to activate vertical policy dynamics between the member states and the centre. Furthermore, the EU has progressed from its earlier 'sectoral' focus to a more recent 'horizontal' approach with the concomitant politicisation that this implies. To implement the 'horizontal approach', the centre has inevitably had to resort to infringement proceedings against the sub-units to close implementation gaps. At the same time, the centre has launched an enforcement agenda that is triggering further competency clashes, which are coded in terms of first pillar versus third pillar procedural arguments. Throughout, one thing has remained constant, the challenge posed by new technologies for the internal market, especially the proliferation of the internet, has remained the pre-eminent justification for offering federalising solutions.

4.2 Power capabilities of the centre

When our focus is directed to the power capabilities of the centre, further similarities and differences can be identified. This is mostly related to the enforcement aspect of copyright policy, where again some notable divergences can be identified. Whereas, both Switzerland and the US have federal agencies responsible for the supervision of copyright issues (the IGE and the US Copyright Office respectively) there is no similar EU agency. Although both federal agencies play a role in the legislative drafting process, the Swiss agency clearly has a bigger role. Its agenda setting powers are significant although its main task is to supervise the 'collecting societies' who are the major policy actors in this domain. Furthermore, it is the only federal agency in Switzerland that deals with copyright issues and its role is more akin to that of an arbiter over the tariffs set by the collecting societies while acting as an agenda setter during the policy process. In the US, on the other hand, federal agencies have significant enforcement powers and there is no

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

need for a supervisory agency for the collecting societies since they do not play a comparable role in the copyright domain.[132] Thus when it comes to the actual enforcement of copyright and, in particular, the investigation of copyright infringements, US policymakers can draw on a host of federal agencies, especially within the DOJ, that have significant powers to operate nationally and increasingly on the international level. Moreover, these specialised investigative units are expanding across the country both in terms of their investigative powers and their number of offices.

No such units exist in Switzerland. To the extent that enforcement takes place it is conducted through cantonal authorities, and this relates to both the investigation and prosecution of infringements. As revealed by the IFPI litigation strategy, there is no Swiss federal agency to contact or to lobby. Enforcement powers lie with the sub-units, and despite increasing information exchanges between the IGA and other interested parties, this hardly amounts to an enforcement body. This is not dissimilar to the EU context, especially in relation to the comparatively weak power of federal actors. In this sense the Commission plays a similar role to that of the IGA in the copyright domain, as an agenda setter and compromise broker between the divergent interests. With the adoption of the copyright directive, a small and intergovernmental body has been created that may in the future morph into a more influential player. However, for the moment, the Commission's plans to create an EU-level body to supervise the powerful 'collecting societies' did not materialise. Interestingly, had the Commission been successful it would have a created an organisational body similar to the Swiss IGA. Thus the Commission is pursuing its enforcement agenda through the closer approximation of legal norms, rather than through the creation or empowerment of enforcement bodies such as in the US.

[132] There is, however, a US Copyright Office, and although it administers copyright law, it does not play a major role in the policymaking process, as do producer interests.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Table 2: Copyright

	Intensity of vertical interactions	***Power capability of centre***
US	Low	High
CH	Medium	Low
EU	High	Low

The findings in the copyright domain are summarised in table 2 above. It denotes the lower intensity of vertical interactions among levels of government in the US compared to the EU where these have remained rather high. Switzerland has been coded medium given the more active role played by the sub-units during the policy process. With regard to the power capabilities of the centre, federal actors in both Switzerland and the EU play important agenda setting roles and attempt to strike compromise between the differing parties but have limited enforcement power capabilities. Furthermore, in the EU case, the Commission has been prevented from creating a supervisory authority and for the moment has adopted a co-regulation approach to the 'collecting societies'. In the US, federal actors have mostly adopted a 'delegated legislative model' to copyright rulemaking. When it comes to rule enforcement however, the US model has empowered and/or created federal agencies with the necessary capabilities to investigate, prosecute and enforce the copyright regime. For the moment, in the Swiss and EU cases such tasks are performed by the sub-units and it is unlikely that similarly endowed enforcement agencies will emerge at the federal level in the near future.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 7: Cybercrime

Cybercrime merges two little understood spheres -technology and crime- that most lawmakers, officials and the public at large, do not fully understand and therefore tend to fear. Consequently, defining the many types of criminality on the internet has been a notoriously difficult exercise.[1] Although this may well be the case, it is possible, nonetheless, to identify two major elements of cybercrime as it is commonly understood by politicians and the general public. The first concerns the issue of 'illegal and harmful content' and is, essentially, an old problem framed around a new medium. The second area relates to the breaching of an information system's security and constitutes an entirely new crime that increasingly falls within the category of 'cybersecurity'. For the purposes of this enquiry, therefore, cybercrime will be broken down into these two major (and overlapping) areas.

In relation to illegal and harmful internet content it will be necessary, at the outset, to define what is understood, first, by the term 'content' and, second, the types of 'content' that will be the focus of the analysis. By 'content' we are principally concerned with communications, which may be computer images, video, or text messages, that are transmitted over computer networks such as the internet. As to the types of content a three-fold distinction[2] can be made: 1) Content that everyone has a right to (e.g. political information); 2) Content that no one has a right to (e.g. child pornography, and obscene material); 3) Content that some have a right to and others not (e.g. pornographic material that is 'harmful' to minors but legal for adults). The regulatory dilemma concerning type 2 content (such as child pornography) is, to a certain extent, the least problematic in terms of criminalising.[3] Type 3 content, such as adult

[1] Notable exceptions include Sieber, U. (1998), Legal Aspects of Computer-related Crime in the Information Society. COMCRIME Study; and Brenner, Susan W (2004) US Cybercrime Law: Defining Offences, Information Systems Frontiers 6:2, pp115-132.

[2] This is slight adaptation of Lessig, L. and Resnik P. (1999), Zoning speech on the Internet: A legal and technical model, *Michigan Law Review* 98:395-431, who provide a three-fold typology of 'speech'. Interestingly the reference to 'speech' (popular in the US) rather than 'content' (popular in Europe) seems to connote a greater affinity with the print medium.

[3] Although there has been a big debate about AGE, and whether an 'actual' person rather than a 'fictitious' image is involved.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

material that is harmful to minors, can be more problematic from a legal and policy perspective. Lastly racist and xenophobic material, can be viewed as type 1 content (i.e. legal), as is usually the case in the US, or it can be viewed as type 2 content (i.e. illegal) as is usually the case in Europe. Such divergences can generate numerous policy problems both at the international level and, even, within polities. In sum, the internet's spectacular diffusion over the past decade poses an entirely new challenge to policymakers and law enforcement. This is connected to the fact that the web facilitates the dissemination of potentially harmful material on an unprecedented scale. The problem is compounded by certain attributes of the internet's navigation arena, such as its open architecture, its anonymity enhancing features and the absence of any central control mechanism. Furthermore, the international nature of the medium, the widely diverging legal concepts as to what constitutes illegal content or harmful content, exacerbates the regulatory challenge.

Computer crimes and breaches of cybersecurity, such as computer espionage and hacking, on the other hand, represent an entirely new crime. The emergence of high-tech computer crimes can be traced back to the 1970s, before the internet became a tool of mass communication. The issues remain the same however: the unlawful penetration of computer systems and the use of techniques such as 'hacking'. Traditional forms of hacking computer networks and other forms of computer system interference proliferated during the 1980s. Also in the late 1980s, these acts began to be increasingly committed remotely via telecommunications systems. In response, a wave of specific legislation developed in relation to this computer-related crime.[4] With the internet's proliferation the risks and vulnerabilities associated with a growing dependence on information systems have now been amplified to an unprecedented degree. The more the internet becomes the central nervous system of the economy and society, the greater the corresponding reliance on its safe and secure functioning. This new social and economic reality also affects the provision of essential services –such as utilities,

[4] This is discussed in detail by Sieber, U (1998).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

telecommunications, and finance- that are at the heart of a nation's wealth and security. Known as 'critical informantion infrastructures', the policy issue can acquire a national security dimension. This is especially the case in states that perceive themselves to be disproportionately at risk from potential cyberattacks (such as the US). In sum, cybersecurity policy took on a new meaning in the 1990s. However, in addressing the security problem, a whole host of problems are raised, not least the fact that most information infrastructures are owned by the private sector.

There are three overlapping issues that preoccupy policymakers and, in particular, law enforcement agencies in connection with cybercrimes. First, there is the assumption that based on current trends, cybercrimes will continue to increase and, furthermore, that in the near future most crimes will have a cyber component. Second, getting access to data, i.e. through the electronic interception of communication or the search and seizure of computer evidence, will become increasingly important for law enforcement. Third, these problems are exacerbated by the fact that the internet is an international communication medium that transcends territorial and jurisdictional borders.[5] The cybercrime challenge is therefore putting considerable pressure on the hitherto neat compartmentalisation of criminal justice systems, especially in federal polities, where law enforcement has been a jealously guarded competence of the sub-units.

In this chapter a slightly different format will be followed according to which the US and EU cases will be contrasted before analysing the Swiss case. For both the US and the EU cases it is possible to make a distinction between 1) illegal and harmful content and 2) cybersecurity issues. The policy dynamics around these two issue areas have been sufficiently different to present these two areas as separate sections. In Switzerland, on the other hand, both issue areas have been addressed simultaneously. Thus, in order to present the case studies more coherently I will address the two issue areas separately for the US and the EU, and contrast the policy response in each polity before

[5] See Speer, D. (2000), Redefining Borders: The challenges of cybercrime, *Crime, Law & Social Change* 34: 259-273.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

proceeding to analyse the Swiss case in a single section. This format is better suited for capturing the policy dynamics in the three polities.

1. The United States: Illegal and harmful content

The starting point for any discussion on regulating illegal internet content in the US is the Constitution and, in particular, the First Amendment. The latter focuses on freedom of speech values and has been at the core of the US debate. Given that lawyers, academics and other parties have been arguing endlessly over its meaning, it is perhaps not so surprising that the arrival of the internet would test the scope and application of this cherished value[6]. By the mid-1990s the internet had become the focal point for a heated policy debate concerning the new medium's potentially negative effects, especially on children. Heightened media attention to the availability of sexually explicit material to an audience of children and adolescents generated what some scholars have referred to as a classic 'moral panic'.[7] It followed a high profile obscenity case in 1994 where a Californian pair was convicted for, amongst other things, posting visual images online of child pornography and acts of bestiality on the internet.[8] Interestingly, they were convicted in Tennessee, not in their home state California, bringing to the fore the issue of computer related inter-state communications and the applicability and jurisdiction of state criminal law.

The topic of rampant online pornography soon became the subject of articles by major newspapers and magazines.[9] It was also at around this time that a

[6] For instance the noted media law scholar Barendt states that 'rarely has such an apparently simple legal text produced so many problems of interpretation" pp48. See Barendt, E (2005) *Freedom of Speech*, 2nd edition. Oxford: Oxford University Press.

[7] See in particular Zimmer, Eric A and Hunter Christopher D. (2001) Risk and the Internet: Perception and Reality in Strate, Jacobson and Gibson Eds. Communication and Cyberspace: Social Interaction in an Electronic Environment. 2nd ed. Hampton Press.

[8] United States v. Robert A. Thomas and Carleen Thomas, No. CR-94-20019-G (W.D. Tenn. 1994), appeal in United States v. Thomas, 74 F.3d 701 (6th Cir. 1996) which affirmed the district court.

[9] The most high profile article was a lead story in *Time* magazine, Philip Elmer-DeWitt, 'On a screen near you: Cyberporn', Time (July 3rd 1995), available at: http://alumni.media.mit.edu/~rhodes/Cyberporn/time.html Other examples include: The New York Times see Lewis, P. H. (1995, March 26). Despite a new plan for cooling it off, cybersex stays hot. (National), pp. 1, 10. The Wall Street Journal see Sandberg, J. (1995, February 8). Electronic erotica: Too much traffic. pp. B1, B9 and Newsweek see Levy, S. (1995b, July 3). No place for kids? A parents' guide to sex on the net. 126(1), 46-50.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

number of organisations began lobbying the US Congress for legislation to protect minors.[10] But, in formulating a regulatory response, federal policymakers would need to take account of US constitutional restraints.[11] Within two months of the conviction federal legislators had already introduced proposals to regulate content on the internet. The first area to receive regulatory attention was content that is harmful to minors. In February 1995, a Democratic Senator introduced the first piece of US federal legislation proposing to regulate harmful internet content, subsequently known as the Communications Decency Act (CDA).[12] Essentially, the legislative proposals had three elements: first, to expand current laws to cover the internet; second, to expand criminal liability for content carried over computer networks to ISPs; and third, to grant new enforcement powers to one of the independent regulatory agencies (the Federal Communication Commission). The bill immediately mobilised a disparate range of interest groups, especially civil liberties groups and Internet Service Providers (ISPs), against the proposed measures.[13] Exactly one year after it was first put forward in the Senate, the CDA was added to the landmark 1996 Telecommunications Act.[14]

Ever since the bill had been placed on the legislative agenda, a powerful opposition group representing a broad spectrum of interest groups had been forming. As soon as it was signed into law, the CDA became the subject of two legal challenges from civil liberties groups and private sector organisations.[15] The two actions were subsequently consolidated as the

[10] This is discussed in detail in Sutter, G. (2000) Nothing new under the sun: Old fears and new media. *International Journal of Law and Information Technology* 8(3).

[11] See for instance chapter 12 of Lessig, L. (1999) *Code and other laws of cyberspace*. New York: Basic Books.

[12] The most detailed account is available in Cannon, R. (1996), The legislative history of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway. *Federal Communications Law Journal*. 49(51).

[13] Critics included the American Family Association, American Online and People for the American Way.

[14] The bill that was eventually passed did, however, include some notable changes. In particular, the enforcement role originally envisaged for the FCC became instead the jurisdiction of the Department of Justice, notably expanding the power of the latter in this area . See especially Cannon pp 59-64.

[15] One was led by the American Civil Liberties Union (ACLU) and including amongst others Human Rights Watch; the Electronic Privacy Information Centre; the Electronic Frontier Foundation; the Journalism Education Association; the National Writers Union. The other challenge was brought by a different group of some twenty-five plaintiffs led by the American Library Association, and including amongst others leading internet service providers; booksellers, journalists, newspaper editors, press photographers, publishers and writers associations, Microsoft and Apple Computers.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

landmark *ACLU v. Reno* case. At stake was how the Internet should be categorised: as a print medium or as a broadcast medium. The answer to this question would have enormous ramifications for the regulation of the internet. The CDA clearly favoured the 'broadcast' model while civil liberties argued in favour of the alternative 'print' model. In June 1997, the US Supreme Court ruled in a landmark case, the first of its kind relating to federal attempts to regulate the internet, that various provisions of the CDA were unconstitutional.[16] The Court stated that the CDA placed an 'unacceptably heavy burden on protected speech' that 'threatens to torch a large segment of the Internet community'.[17] As a unique and wholly new medium of worldwide communication, the Court argued that the internet is entitled to the highest constitutional protection and that it should enjoy the same protection as the print medium.[18] Federal lawmakers' first attempt to regulate harmful content on the Internet had thus conspicuously failed at the first hurdle.

Regulatory actions were not only pursued at the federal level however. Indeed, in reacting to the cyberporn scare many states had enacted similar versions of the CDA. Here, once again, the role of the federal courts would prove decisive. In a case brought before a Federal Court by the American Libraries Association against the State of New York, the court took a decision that effectively struck down New York's 1996 indecency law, which had been adopted in the wake of the CDA.[19] What is revealing in this context is not so much the fact that the federal court found that the state legislative measure had violated first amendment freedom of speech values, but rather that it violated the 'commerce clause' of the US constitution. On the former point, the Supreme Court had already declared federal regulatory attempts as unconstitutional on 'first amendment' grounds. This could, at least in theory, be redressed by passing less restrictive measures. The violation of the 'commerce clause' added an entirely new dimension to state-level attempts to regulate internet content however. In explaining its decision against the state

[16] The Court found that the Act was both overbroad and vague and therefore unconstitutional. In particular see the Opinion of Justice Stevens in *Reno v. American Civil Liberties Union*, 52 U.S. 844 (1997)

[17] See Justice Stevens Opinion (*ibid*)

[18] See Justice Stevens Opinion

[19] American Library Association v. Pataki, 969 F.Supp 160 (S.D.N.Y. 1997)

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

of New York, the federal court was drawing on a doctrine that prohibits states from regulating in ways that unduly burden interstate commerce[20]. By invoking this doctrine the federal court established the basis for the judicial pre-emption of state law in this area. To this end, the federal court argued that 'regulation on a local level…will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities'. Furthermore, the Court famously concluded that 'the unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes'.

Two legal scholars have argued that this reasoning threatens to invalidate nearly every state regulation of internet communications[21]. Since the *Pataki* decision (as the New York case is known), and based on the same reasoning, various other federal circuit courts have ruled that comparable state initiatives were unconstitutional for breach of the interstate commerce clause as well as the first amendment.[22] In one such case the court went as far as to say that "[w]e think it likely that the internet will soon be seen as falling within the class of subjects that are protected from State regulation because they 'imperatively demand a single uniform rule'.[23]

Despite such rulings, legislators at the state level have persisted in their attempts to regulate internet content. Most recently a Pennsylvanian law, passed in February of 2002, which required ISP's to block access to a given site that contained child pornography or face criminal charges, was challenged on first amendment and commerce clause grounds.[24] The same coalition of organized civil liberties groups mobilized to mount a legal

[20] It is known as the 'dormant commerce clause' and is a judge-made doctrine that can serve to preempt state laws. For a discussion in relation to internet content see Goldsmith, J. and Sykes, A. (2001), The Internet and the Dormant Commerce Clause, *Yale Law Journal* 110 pp 786.

[21] Ibid., pp 786-787

[22] ACLU v. Johnson, 194 F.3d 1149 (10th Cir. 1999) (New Mexico state law); Cyberspace Communications, Inc v. Engler, 142 F. Supp. 2d 827 (E.D. Mich 2001) (Michigan State Law); American Booksellers Foundation v. Dean, 342 F.3d 96, 104 (2d Cir. 2003) (Vermont state law); Southeast Booksellers Association v. McMaster, 282 F. Supp. 2d 389 (D.S.C. 2003) (South Carolina state law); PSInet, Inc. v. Chapman, 63 F3d 227 (4th Cir. 2004) (Virginia state law)

[23] The case is known as *Dean*. See the American Booksellers v. Dean. For a fuller discussion see Pann, C (2005) 'The Dormant Commerce Clause and State Regulation of the Internet: Are Laws Protecting Minors from Sexual Predators Constitutionally Different than those Protecting Minors from Sexually Explicit Materials?' Duke Law & Technology Review

[24] See the Internet Child Pornography Act 18 Pa. Cons. Stat. § 7330 (2002)

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

challenge.[25] And again, in September of 2004, the court ruled in favour of the coalition by finding such state initiatives to be unconstitutional.[26] Emboldened by their successes, civil liberties organizations have gone on to challenge other state laws, most recently a Utah law passed in 2005, on both first amendment and commerce clause grounds.[27]

In view of the difficulties facing state-level legislators on account of the commerce clause, the onus was on federal policymakers to come up with a set of regulatory measures that would stand the first amendment test. Within a few months of the Supreme Court decision against the earlier federal measures (the 1996 CDA), an amended version had already been introduced. The new legislative measures, known as the Child Online Protection Act (COPA), were proposed in April 1998 and signed into law by the President within six months. As with the CDA, access by civil liberties groups had been restricted during the key policy formulation stages and the proposed bill was attached to legislation that was guaranteed to pass. The new regulatory measures represented a watered down version of the earlier CDA, one that crucially, did not impose liability on content providers who were simply involved in the transmission of data (e.g. telecommunications carriers, ISP's and search engines). In this regard, the ISP's had successfully lobbied to avoid liability for third party content.

Nonetheless, despite the modifications, COPA mobilized the same influential coalition of free speech advocates and private sector actors against renewed regulatory efforts by federal policymakers to protect minors from online pornography.[28] The new law, which was never actually enforced, was challenged on First Amendment grounds even before it came into effect. A convoluted litigation process ensued that thus far has included two further Supreme Court decisions, the second of which was handed down in June of 2004 and, essentially, prevents the federal government from enforcing

[25] The challenge was brought about by the CDT and the ACLU in 2003.

[26] Centre for Democracy and Technology v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004)

[27] The King's English v. Shurtleff. The complaint filed is available at: http://www.cdt.org/headlines/786

[28] It was headed by the ACLU and included amongst others the American Book Sellers Association; the Electronic Frontier Foundation and the Electronic Privacy Information Centre

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

COPA.[29] In short, some ten years after Congress first enacted its ill-fated CDA, and after protracted and on-going litigation, its second attempt remains unenforceable. As one legal scholar has argued, 'few decisions show so well the lengths to which the US Supreme Court will go in the context of the Internet to protect speech, which in other contexts has been treated as of 'low value'.[30]

An area in which the federal and state level governments have had more success has been where they have targeted schools and libraries in receipt of public funding. An example is offered by the Childrens' Internet Protection Act[31] (CIPA) of 2000. While the problem remained the same -how to reduce children's exposure to harmful material on the Internet- the method differed in that the new measures obliged sub-state actors to implement the regulations. CIPA was an attempt to achieve federal policy objectives by requiring schools and libraries that receive specific federal funds to certify that they have in place a 'Safer Internet Policy'. The latter comprises the use of technological filters that block access to illegal content such as obscenity and child pornography. It is noteworthy that even prior to the CIPA being signed into federal law, several states had already enacted laws mandating filtering measures in either public schools, libraries or both and many other states had bills pending.[32] By 2005, over twenty states had their own state level internet filtering laws,[33] and at least five other states appear to have bills pending.[34] The majority of these laws simply require school boards or libraries to adopt

[29] The litigation history runs as follows: A preliminary injunction was granted by a federal district court in February 1999 in the case of ACLU v. Reno, 31 F. Supp. 2d 473 (E.D. Pa. 1999). This was affirmed by the Court of Appeals for the Third Circuit in June 2000 in ACLU v. Reno, 217 F. 3d 162 (3d Cir. 2000) but was reversed by the Supreme Court in Ashcroft v. ACLU, 535 U.S. 564 (2002). After further rounds it eventually resulted in the Supreme Court decision of June 2004 in ACLU v. Ashcroft 124 S. Ct. 2783 (2004).

[30] Barendt (2005), p461.

[31] See the *Childrens' Internet Protection Act* of 1999 S. 97, 106th Congress.

[32] On the early state legislative measures see R. Peltz (2002) Use "The Filter You Were Born With": The Unconstitutionality of Mandatory Internet Filtering for the Adult Patrons of Public Libraries 77 Washington Law Review 397, at 434-435.

[33] See *Children and the Internet: Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries*, National Conference of State Legislatures available at http://www.ncsl.org/programs/lis/cip/filterlaws.htm

[34] Georgia, Florida, Illinois, Iowa and Kansas. See the table of state laws available at http://www.safelibraries.org/statecipalaws.htm#examples

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

so-called 'safer internet policies', but some states also require publicly funded institutions to install filtering software.

The constitutionality of both the federal level CIPA and the proliferating state-level measures was questionable. Thus, it was no great surprise that CIPA (the federal law) was soon the subject of a new legal challenge by the civil liberties coalition[35] and that this would have important implications for the initiatives being pursued at the state level. The prospects for a positive outcome did not appear promising. Even before CIPA's enactment, a 1998 Federal Court decision had declared that the mandatory filtering of all library computers violated, *inter alia*, the first amendment and was thus unconstitutional.[36] Initially declared unconstitutional and in violation of the first amendment by a lower court,[37] the CIPA went all the way to the Supreme Court in 2003.[38] This time, however, the highest federal court ruled in favour of the federal measure. The stakes were high indeed, since a negative verdict would have seriously eroded state level authority's competencies within their own public administrations. In the wake of the Supreme Court's decision in 2003, it appears that state-level measures on filtering are in principle constitutional. There is thus a varied approach to internet filtering laws in the US, depending on whether the public authority in question is federal, state or local.

The analysis thus far has focused on issues related to harmful internet content, questions of liability, and the use of filtering technologies by public authorities. But there is still another issue –that of 'illegal content' - which needed to be tackled. Fortunately, the latter is not protected by the First Amendment and is therefore unambiguously prohibited. Even here though, controversies have arisen that further illustrate the structuring effect of US constitutionalism. A notable and early example is provided by the 1996 Child

[35] Two of the staunchest critics of CIPA during the legislative development stage, the American Library Association (ALA) and the ACLU (alongside a broad coalition of groups) brought legal challenges against CIPA.

[36] Mainstream Loudoun v. Board of Trustees of the Loudoun County Public Library, 24 F. Supp. 2d 552 (E.D. Va. 1998). For discussion see http://www.cato.org/pubs/scr/2003/publiclyfunded.pdf

[37] American Library Association v. United States, 201 F. Supp. 2d 401 (E.D. Pa. 2002)

[38] United States v. American Library Association, 123 S. Ct. 2297 (2003).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Pornography Prevention Act (CPPA).[39] Prior to 1996, federal law prohibited interstate distribution of child pornography though it required that the offending material depict an *actual* child engaged in sexually explicit activity. This legal lacuna acquired a heightened significance with the increasing availability of technology,[40] such as computer-generated imaging software, that could now effortlessly produce fictitious children's images. The response to this new development, at the height of the moral panic in the US, was the CPPA.

Having been largely excluded from the legislative process, civil liberties groups and the adult content industry were immediately mobilised and challenged the federal measures in multiple state jurisdictions. It resulted in another Supreme Court ruling against the Department of Justice (DOJ) in which the CPPA was found to be unconstitutionally overbroad with regard to virtual child pornography created without real or identifiable minors.[41] This decision, *Ashcroft v. Free Speech Coalition,* generated an unprecedented torrent of criticism.[42] Within a fortnight of the decision, a legislative response had been drafted by the DOJ[43] and a hearing was convened by the judiciary committee to address the decision.[44] The National Center for Missing and Exploited Children testified that 'the Court's decision will result in the proliferation of child pornography in America, unlike anything we have seen in more than twenty years…[and] as a result of the Court's decision, thousands of children will be sexually victimized'.[45] In fact, the critical reaction was such

[39] See 18 U.S.C. S 2256

[40] This is discussed in detail as is the federal response in Mota, S (2002) 'The U.S. Supreme Court Addresses the Child Pornography Prevention Act and Child Online Protection Act in *Ashcroft v. Free Speech Coalition* and *Ashcroft v. American Civil Liberties Union*' (2002) 55 *Federal Communications Law Journal* 85, at 88.

[41] See Ashcroft v. Free Speech Coalition 535 U.S. 234 (2002).

[42] The Attorney General was quoted, on the morning of the decision, as stating that "This morning the United States Supreme Court made our ability to prosecute those who produce and possess child pornography immeasurably more difficult". See "Supreme Court strikes down ban on "virtual child porn", CNN, April 18, 2002 available at http://archives.cnn.com/2002/LAW/04/16/scotus.virtual.child.porn/ .

[43] Child Obscenity and Pornography Prevention Act of 2002, H.R.4623, 107th Cong. (2002).

[44] 'Hearing to address the April 16, 2002 Supreme Court decision in *Ashcroft v. the Free Speech Coalition* as well as other threats against the protection of children' before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee, 107th Congress (May 1st, 2002) available at: http://judiciary.house.gov/legacy/crime.htm

[45] Testimony of E. Allen available at http://judiciary.house.gov/legacy/allen050102.htm . Testimony later repeated before a Senate judiciary committee hearing, "Stopping Child Pornography: Protecting

DOI: 10.2870/1208

that some legislators tried to alter the US Constitution. A joint resolution was proposed in 2002, albeit unsuccessfully, to add a new constitutional amendment (known as "the Brown Amendment") clarifying that neither the US Constitution nor any State constitution was to be construed as to protect child pornography whether actual or virtual.[46] Following the outcry against the Supreme Court's decision, a number of legislative proposals were swiftly introduced that have since appeared to have overcome the first amendment constraint.[47] Typically, it was achieved by adding provisions concerning illegal internet content to a an entirely different act that, in this case, had as its key aim the expansion of the US's child alert system.

In view of the failed attempts to oblige information intermediaries to police the internet through liability provisions, the federal government adopted a more collaborative approach with the ISPs on the specific issue of child pornography.[48] Federal measures had already been passed in 1999 that established criminal offences and initiated a 'zero tolerance' policy for possession of child pornography.[49] Moreover, the measures included a novel approach whereby ISP's would report child pornography on their sites to a 'Cyber Tipline', at the National Center for Missing and Exploited Children (NCMEC). This information is subsequently forwarded to the relevant law enforcement agencies. This novel 'hotline' approach received strong support from the state and federal governments but, most importantly, did not raise first amendment concerns.[50]

---

our Children and the Constitution", October 2nd 2002, available at http://judiciary.senate.gov/hearing.cfm?id=485

[46] H.R.J. Res. 106, 107th Cong. (2002).

[47] See the *PROTECT* Act of 2003.

[48] A zero tolerance policy was first announced by the CEO of AOL, Steve Case, at The Internet Online Summit: Focus on Children, on December 2, 1997. He announced that 'I'm pleased to report that the leading Internet service providers, represented by the Commercial Internet exchange Association, the Interactive Services Association, and the Association of Online Professionals, are today reaffirming in the strongest terms our "Zero Tolerance" policy against child pornography…we will not allow this valuable new medium to be exploited by child pornographers or child predators." Speech available at:
http://www.cybercrime.gov/zero.htm

[49] See the Protection of Children from Sexual Predators Act passed in December 1999.

[50] In a speech the Vice President Gore grandiosely announced his expectations of the hotline approach as 'a warning to criminals and a promise to parents: There are Internet police for those activities that are illegal, and they will capture and punish those who would use the Internet to harm and hurt our children. Together, these new initiatives [hotlines] will make a significant difference in the ability of parents and law enforcement to work together to keep our children safe on the

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Curtailed in many of its earlier legislative ambitions, the federal administration adopted a 'hotline' approach and this was supplemented with more traditional forms of investigatory policing. Key amongst these was the FBI's Innocent Images National Initiative (IINI). Launched at the height of the moral panic in 1995, the IINI was an intelligence driven investigative initiative to combat the proliferation of child pornography that had been facilitated by computer networks. In order to activate federal competencies, it focused on major *interstate* producers and distributors of child pornography as well as those in possession of child pornography. Interestingly, the Innocent Images Unit was also able to use undercover investigative methods with agents posing as children or as adults with an interest in child pornography. According to the FBI's own figures, between the fiscal years 1996-2005 there was a 2026% increase in the number of IINI cases opened (113 to 2402) by the FBI.[51]

After the initial focus on child pornography, federal policymakers' attention has now shifted to also encompass obscenity. This has therefore broadened the scope and the fight against illegal internet content. Further interagency collaborations have resulted, especially between the FBI and the DOJ's Child Exploitation and Obscenity Section (CEOS), both of which have concentrated their investigations on major producers and interstate distributors of obscenity. More recently, the DOJ has created a high-level Obscenity Prosecution Task Force in 2005 that is dedicated to the investigation and prosecution of distributors of hard-core pornography.[52] Having put the fight against child pornography at the top of the FBI's investigatory agenda, the scope is being presently broadened to include obscenity. This is not the case for racist and xenophobic content however. First Amendment provisions make it extremely difficult to criminalise racist and xenophobic content in the US, since it can be regarded as a form of political expression. As a result, the vast majority of racist material on the Internet could not be the subject of criminal sanctions. In

---

Internet.Remarks by vice president Al Gore at the Internet/outline summit, Renaissance hotel, Washington, DC, December 2, 1997 available from http://www.cybercrime.gov/gore-sp.htm

[51] See FBI's statistics on IINI cases available at http://www.fbi.gov/publications/innocent.htm

[52] See the Taskforce's website at: http://www.usdoj.gov/criminal/OPTF/index.html

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

other words, the US government is forbidden, in most cases, from taking any legal action to suppress or regulate the expression of racist views. There are, of course, exceptions but these are strictly limited to cases where hate speech crosses the line and become threats or harassing speech directed at individuals.[53]

2. The European Union: Illegal and harmful content

The constitutional battles over illegal and harmful internet content unfolding in the US during the mid-1990s were being closely monitored by policymakers on the other side of the Atlantic. When in 1997 German prosecutors held the general manager of *Compuserve* (an American internet service provider) responsible for trafficking in pornography and neo-Nazi propaganda,[54] EU policymakers took note. Events in Europe had potentially grave implications for the internal market. If member states adopted diverging approaches to the regulation of internet content, distortions to the internal market could be created.[55]

In 2000, further unilateral member state attempts to regulate racist internet content appeared when three anti-racist and Jewish associations successfully filed a complaint against *Yahoo*! before a French Court for hosting online auctions of Nazi memorabilia.[56] French law prohibited the exhibition of objects that incite racial hatred. The French courts decided to hold Yahoo! responsible and gave it three months to block French users access to the US auction site.[57] Given these very high profile cases of unilateral regulation of racist internet content –and the dangers it could pose to the EU internal

[53] For a critical stance on the US approach to anti-hate speech see The Anti-Defamation League at: www.adl.org

[54] See the Local Court Munich v. SOMM, Felix Bruno, Munich File No.: 8340 Ds 465 Js 173158/95 the German Court of Appeal in 1999.

[55] For a detailed discussion see Goldsmith, J. (2000a), Unilateral Regulation of the Internet: A Modest Defence. *European Journal of Internation Law*; 11(1):135-148; and Mayer, F. (2000). Europe and the Internet: The Old World and the New Medium. *European Journal of International Law*; 11(1):149-169.

[56] For a discussion see Goldsmith, J. (2000b). Yahoo! Brought to Earth. *Financial Times*. November 27; and Akdeniz, Y. (2000) Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance ded Paris (The County Court of Paris), Interim Court Order, 20 November, *Electronic Business Law Reports*; 1(3):110-120.

[57] Eaglesham, J. (2001), "Yahoo! Bans hate propaganda," *Financial Times*, January 3, 12.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

market for online services- a number of policy actors began to direct their lobbying efforts onto the EU policy stage. They were able to count on a sympathetic Commission, which was actively seeking to minimise the potential for regulatory and intra-EU conflicts in what was perceived to be an area of vital economic competitiveness: the market for digital content.

The Commission had actually given much thought to the issue of illegal content, and the dangers posed by unilateral member state regulation of online services, well before the French *Yahoo!* case. Its first initiatives in the area of illegal and harmful content therefore need to be seen in the context of widespread public and political concern about the spread of certain types of content, especially pornography, which were proliferating at an accelerating rate on the new medium during the mid-1990s. EU policymakers' main fears were that this could provoke member states into pursuing uncoordinated regulatory action, generating new barriers to the flow of information services in the EU, and adversely affecting the environment for commerce[58]. With the German and French attempts at regulatory unilateralism these fears appeared well-grounded.

In the mid-1990s, well before the internet had become a 'hot' political issue in most member states, the Commission put forward its policy agenda to address the challenge of illegal content. Towards the end of 1996 two, more or less complementary foundational policy statements were agreed. The Commission's *Communication on illegal and harmful content*[59] and a *Green Paper on the protection of minors and human dignity.*[60] These were important policy statements which defined the EU agenda for the following half a decade. In both documents the Commission voiced its concerns with the German *Compuserve* case and was blunt about the dangers of German standards of morality being exported[61]. The *Communication* had been

[58] See Benkler, Y. (2000), Internet Regulation: A Case Study in the Problem of Unilateralism. European Journal of Internation Law; 11(1):171-185.

[59] European Commission. Communication on Illegal and harmful content on the Internet. 1996; COM(1996)0487

[60] European Commission. Green Paper on the Protection of minors and Human Dignity. 1996; COM(1996)0483.

[61] See the 1996 Communication

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

sponsored by DG XIII (Telecommunications) and was rather optimistic about the possibilities of using new technologies (such as filtering and rating technologies) to address the new perceived dangers. At the same time it also fervently promoted self-regulation as the most appropriate regulatory mode. This was not altogether surprising given that it emanated from one of the more free market oriented DG's within the Commission, one that had already achieved a notable degree of success in liberalising the telecommunications sector. To a large extent DG Telecommunications (now known as DG Information Society) was attempting to recreate its earlier success in the now rapidly emerging internet policy domain. At the same time, it was more receptive to the interests of the commercial network providers and this was notably reflected in the policy measures it proposed.

On the other hand, the *Green Paper on the Protection of minors and Human Dignity*[62] was the result of a separate initiative from DG X (Education and Culture), one that was more open to civil society organisations. It took a broader perspective and presented the content issues as part and parcel of a wider regulatory challenge. The Green Paper was rather optimistic about finding legislative solutions to the problems of internet content. Indeed, it identified types of content which

'may be banned for everyone regardless of the age of the potential audience or the medium used. Here it is possible, irrespective of differences in national legislation to identify a general category of material that violate human dignity, primarily consisting of child pornography, extreme gratuitous violence and incitement to racial or other hatred, discrimination, and violence'.[63]

What remained clear throughout this initial phase is that it would be up to the member states to enforce the law on illegal content. Despite the Green Paper's optimism about finding legislative solutions, there were serious divergences concerning certain acts that were punishable in some member states and not in others. This was less the case for child pornography than it

[62] See the European Commission's Green Paper on the Protection of minors and Human Dignity COM(1996) 0483
[63] See 1996 *Green Paper*

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

was for the dissemination of racist material. On this latter issue, member states rules varied significantly and this would pose numerous problems in later policy stages. Indeed, variation was most marked between the UK on the one hand, and France and Germany, which had stringent rules, on the other.

During this initial phase, a consensus of sorts emerged on how to address the problem of illegal and harmful content: 'self-regulation' on the part of content and access providers and, for internet users, the promotion of new technologies. On the latter point, the priority was to enable users (e.g. parents) to deal with harmful content through the development of technological solutions (especially filtering and rating systems) and in fostering the use of such technologies in a context of self-regulation.[64] The technology panacea appeared particularly appealing in the EU context since it could potentially avoid governmental regulation. Moreover, it could reduce the even greater danger of unilateral intervention by the member states. But there was also another reason why the technology solution was being promoted. Put simply, it was in order to avoid the situation of having to rely on rating systems developed for the US, where a different approach to content rating could emerge reflecting US values.[65]

The 1996 initiatives had therefore set out a two-fold strategy of private sector leadership via self-regulation on the one hand, and support for technical solutions on the other. During the early days of the internet's proliferation this was probably as much as could be expected in terms of EU level policy action. By the late 1990s, however, a second phase could be discerned and it involved two distinct policy methods. One was promoted by the Council and was 'top-down' in nature, while the other, sponsored by the Commission's DG Telecommunications, focused on a series of 'bottom-up' measures. To implement the former, a consultation process was launched which brought

[64] The Communication in particular, included sophisticated diagrams on the operation of blocking technologies and third party labeling services.
[65] See in particular the Green Paper.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

together national representatives, consumer and industry groups.[66] The most relevant findings from the consultation process were the points of divergence among the member states and the fact that those that were most concerned with illegal content were northern EU member states.[67] Significant differences existed among the member states' organizational structures, and this would affect their capacity to design and implement self-regulation instruments. Differences in member state priorities were also prevalent, with some targeting child pornography while others were concerned with violence in new media.

In light of the above divergences, and in view of the findings from the consultation process, a greater coordination of national responses was to be pursued through the pooling of experience at the European level. These conclusions were important because they marked an evolution from the self-regulatory rhetoric of the 1996 initiatives, towards a co-regulatory model. In this new approach public authorities would set out the overall policy goals and leave it to the stakeholders to agree on appropriate solutions.[68] The preferred method to achieve these EU policy goals at this stage was through a non-binding legal instrument -a member state driven Council Recommendation.[69]

In 1998, a Council Recommendation on the protection of minors and human dignity[70] was adopted. It constituted the first legislative attempt at the EU level, albeit a 'soft' one, that specifically targeted illegal and harmful internet content. The Council called for the setting up of 'hotlines' for handling

[66] See European Commission Directorate General X. Commission Working Paper on the Protection of minors and human dignity in audiovisual and information services: Consultations on the Green Paper. 1997; SEC (97) 1203.

[67] European Commission Directorate General X. Commission Working Paper on the Protection of minors and human dignity in audiovisual and information services: Consultations on the Green Paper. 1997; SEC (97) 1203.

[68] Cowles, M. G. (2001), *Who are the Rule-Makers of E-commerce: The case of the Global Business Dialogue on E-Commerce*. Washington DC: American Institute for Contemporary German Studies.

[69] The Recommendation, which is a legal act under Article 249 (ex-article 189) of the Treaty, aimed to provide guidelines for national legislation. The important note is that a Recommendation expresses the views and preferences of EU institutions on desired actions, but is not binding on the Member States.

[70] See the Council Recommendation of 24 September 1998 On the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

complaints and encouraged industry to agree on basic common rules for dealing with complaints, such as the exchange of information between operators and the procedures for responding to complaints. It also called on the member states to create representative bodies in order to foster cooperation among the national complaints handling systems at the European level. With the Council Recommendation self-regulation was no longer solely in the hands of the private sector.[71] Public authorities would establish the context in which self-regulation was to take place by setting out the conditions for the set up, drafting, implementation and evaluation by all the relevant actors.[72] The major ISPs would, in this way, work together with representatives of consumers, civil liberties associations, privacy authorities and especially with official authorities in charge of the prosecution of crimes.

While the Council driven instrument had a 'top down' flavour, i.e. establishing general guidelines for national frameworks of self-regulation, the DG Telecommunications initiative had a distinctly 'bottom up' approach. Known as the Safer Internet Action Plan[73], it was intended to complement the Council instrument and covered the period 1999-2004. It focused specifically at the R+D level and aimed to provide incentives for industry players to develop and implement a system of co-regulation. This was to be achieved in two principal ways: First, by providing EU funding for the creation of a European network of hotlines. These were reporting mechanisms which would allow members of the public to report illegal content. The reports would then be passed on to the appropriate body for action (e.g. police authorities or ISPs). It was deemed an effective way to restrict circulation of illegal material while leaving responsibility for investigation and prosecution firmly with member state law-enforcement authorities.[74] Second, the development of filtering and rating systems was to be encouraged. To this end, the programme not only aimed to

[71] For a detailed discussion see Cowles, M. G. (2001).

[72] See Udekem-Gevers, Marie and Poullet Yves. Concerns from a European user empowerment perspective in internet content regulation: An analysis of some recent statements. ECLIP II. No date.

[73] See Decision No 276/1999 EC of the European Parliament and of the Council adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.

[74] See Annex 1 of Decision.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

demonstrate the potential of filtering and rating systems, but to promote this in such a way that the technological solutions reflected European values.

In parallel to EU funded R+D programmes, the interests of industry were also safeguarded by the adoption of DG Internal Market's landmark e-commerce directive in 2000.[75] Negotiated over a three year period, the e-commerce directive aimed to reduce regulatory uncertainty for the uptake of e-commerce. However, what was at stake during the negotiations of the directive was the tricky question of the liability of ISPs for content passing through their networks. The issue was especially pertinent given that the German and French court cases had effectively held information intermediaries liable for content passing through their networks. In passing the e-commerce directive, business interests had successfully lobbied the Commission and the Council for an exemption from liability in cases where service providers played a passive role as mere conduits of content.[76]

In many respects, by 2000 much of the policy agenda of the mid-1990s had been operationalised and, most importantly, the thorny question of liability had been resolved. However, there had been a notable shift from self-regulation towards a second phase characterised by a form of co-regulation. This was especially the case with the new Council instrument. Yet for all intents and purposes, the model still displayed an overwhelming belief in the superiority of industry self-regulation and a rather naïve faith in technological solutions. Implementation also tended to be patchy, for instance, not all member states yet participate in the EU funded networks.[77] This was no doubt due to the non-binding nature of the instrument. Still, as the Commission readily admitted, the Safer Internet Programme of 1999-2004 was one of its major policy actions in the field. Moreover, without EU funding the pan-European

[75] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[76] The directive also limited service providers' liability for other intermediary activities such as the storage of information.

[77] The network of EU funded hotlines is knwn as INHOPE. See http://www.inhope.org/

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

network would not have been set up.[78] With the EU's imminent enlargement an extension of the programme was agreed through to 2008. Now referred to as the Safer Internet Plus Programme,[79] its funds have been doubled and it now constitutes the EU's main attempt to foster 'hotlines', while promoting R+D initiatives to address harmful content through filtering and labelling technologies.

Coinciding with the new millennium a third and rather more ambitious phase has been recently pursued. The latest approach to illegal internet content, however, needs to be viewed through the wider prism of changes in the field of EU police and judicial cooperation. The new direction represents a notable change in emphasis from the earlier self-regulation and co-regulation strategy, towards what can be viewed as a third mode of regulation, which is aimed at enhancing the investigative powers of law enforcement agencies and cooperation among judicial authorities across the EU. More importantly, backing and support has been provided at the highest political level, the European Council. Following an initiative from Austria, the first area to receive attention was child pornography.[80] The initiative specifically addressed the issue of online child pornography and called for the reinforcement of the investigative powers of law enforcement authorities and greater cooperation between member states to facilitate the effective prosecution of child pornography offences. Six months later the Austrian initiative was formerly approved as the Council Decision of 2000 to combat child pornography on the internet.[81]

This was one of the first ever uses of the new Council Decision –an instrument that had been created by the 1997 Treaty of Amsterdam. It is noteworthy that the new instrument was explicitly targeted at the perceived

[78] See the European Commisssion 'Proposal for a decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies' COM/2004/91.

[79] See Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies.

[80] See Initiative from the Republic of Austria with a view to adopting a Council Decision to combat child pornography on the Internet (1999/C 362/06).

[81] See the Council Decision to combat child pornography on the Internet (2000/375/JHA).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

social risks of the internet. The Council Decision –which can be used for strengthening cooperation among law enforcement agencies- now *obliged* member states to set up specialised units within law enforcement authorities. These were to have the necessary expertise and resources to be able to deal swiftly with information on suspected production, processing, distribution and possession of child pornography.[82] Member states were to ensure enhanced cooperation for facilitating the investigation and prosecution of offences concerning child pornography on the Internet through these units on a 24 hour contact point basis.[83] Moreover, greater coordination with Europol, which should be kept informed of suspected cases of child pornography, was also explicitly called for.[84]

In order to cement the latest approach to illegal content on the internet, the Commission put forward its policy agenda in the form of a landmark communication specifically dedicated to 'cybercrime'.[85] Published in January 2001 under the responsibility of DG JHA, it set out an ambitious agenda which included calls for new legislative proposals to approximate member state criminal laws and the creation of an EU Cyber Crime unit. The latter –which has since been established at the EU's Joint Research Centre[86]- would deal with, amongst a number of other issue, the question of illegal content. As promised, the *Cybercrime Communication* spawned various proposals[87] for a greater harmonisation of criminal laws. The most important thing to note about these proposals was that they were driven by the Council and DG JHA.[88] The first to emerge, passed in the same month as the Communication, was a new proposal for harmonising EU member states criminal laws on child

[82] See Article 1 (2) of the Decision.
[83] See Article 1 (3) of the Decision.
[84] See Article 2 (3) of the Decision.
[85] See the European Commission's Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer related crime of 2001 Jan; COM(2000) 890.
[86] As of 2005 and three years after its establishment the EU Cyber crime Forum has certainly not become the coordination mechanism that was anticipated by the Cybercrime communication. For further information see: http://cybercrime-forum.jrc.it/default/
[87] Framework Decisions have been proposed to 1) combat child pornography,2) racism and xenophobia, and 3) network security.
[88] Interview with European Commission official at the Joint Research Centre 23/05/04.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

pornography.[89] While the earlier Council Decision of 2000 had set up specialised units and greater cooperation among judicial and police authorities, the new initiative went much further in the area of criminal law. Framed rather broadly, it aimed to combat the sexual exploitation of children as well as addressing child pornography[90]. Adopted in December 2003, the new framework decision has effectively harmonised at the EU level what constitutes a child pornography offence, the penalties for such conduct, and the criteria for settling jurisdictional conflicts among the member states.[91]

Unlike child pornography, the subject of racism has been rather more controversial. There is less common ground in this area and the divergences are wider among the member states. Notwithstanding these differences, the Commission put forward its proposals in 2001 for a closer approximation of penal laws relating to racist and xenophobic offences.[92] As was the case with online child pornography, one of the chief motivations for the new initiative was the Internet's role in facilitating the dissemination of racist and xenophobic content. The medium had become a 'cheap and highly effective tool for racist individuals or groups to spread hateful ideas' and the Commission acknowledged its ambitious aim 'to ensure that racist and xenophobic content on the Internet is criminalized in all Member States'.[93] Notwithstanding these declarations, attempts to bring about greater approximation of criminal laws on racism and xenophobia have stalled in the Council and, to date, given the greater divergences in this area, no consensus has yet been reached in the negotiations. This offers a stark contrast to the harmonisation of penal laws pertaining to child pornography, and the creation

[89] See the Commission's Proposal for a Framework Decision on combating the sexual exploitation of children and child pornography COM (2000) 854 final.

[90] See the Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography.

[91] This was achieved by defining the key terms such as 'child', 'child pornography' and 'computer system'. With regard to the later, for instance, it defined as an offence the production of child pornography whether undertaken by a computer system or not. In other words it resolved the controversial issue of whether the material in question involved a real child or fictitious computer image.

[92] See the European Commission's Proposal for a Council Framework Decision on combating racism and xenophobia COM(2001) 664 Final.

[93] See the Explanatory Memorandum of the proposal.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

of specialised units for coordinating policy, all of which have now been implemented at the EU-level.

3. The United States: Cyersecurity

Our attention can now be focused on a distinct set of cybercrime issues that are not connected to illegal and harmful content and are increasingly referred to as cybersecurity. Two major issues around which the cybersecurity policy agenda has centred have been 1) the updating of computer crime laws and 2) the protection of critical information infrastructures. In the decade 1995-2005, it is fair to say that both areas have been effectively federalised. In relation to computer crime, a major piece of legislation was introduced in the mid-1980s to address the emerging phenomenon. The debate at the time centred on whether computer crime was nothing more than traditional crime committed with new high-tech devices or whether it required innovative law enforcement techniques and new laws designed to address the resultant abuses.[94] In the mid-1980s, federal policymakers adopted the latter view and enacted legislation to address crime in the electronic environments known as the *Computer Fraud and Abuse Act* of 1986.[95] It is important to note however, that consistent with the US version of federalism and its multiple and overlapping jurisdictions, each state had different laws and procedures pertaining to the investigation and prosecution of computer crimes.[96] On the other hand, as a result of the above act, the FBI was able to set up a specialized computer squad that subsequently began to play a prominent role in the area of computer crime.[97] Having obtained a particular expertise in dealing with and investigating hacker intrusions and data theft, the FBI was well placed to acquire a prominent role in dealing with the issue of cybersecurity when it exploded in the mid-1990s.

---

[94] See in particular the Computer Crime and Intellectual Property Section of the US Department of Justice. The National Information Infrastructure Protection Act of 1996: Legislative Analysis. Available at: http://www.cybercrime.gov/1030_anal.html

[95] See the *Computer Fraud and Abuse Act* 1986 (US) 18 USC 1030.

[96] National Conference of State Legislatures has a database with all the individual state level statutes in the area of computer crime. See database at: http://www.ncsl.org/programs/lis/cip/computercrimes.htm

[97] For further information see the federally funded Computer Emergency and Response Team, CERT Coordination Center (2004) *How the FBI Investigates Computer Crime*, available at http://www.cert.org/tech_tips/FBI_investigates_crime.html

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

With cybercrime incidents and computer intrusions on the rise[98] during the 1990s, it was increasingly felt by the DOJ that new legislation was required.[99] From a legal perspective, however, federal activity was restricted to computers used by the federal government –consistent with the traditional dual criminal justice system under which federal crimes were narrowly defined and limited to only protecting special *federal* interests. With the implementation of the 1996 *National Information Infrastructure Protection Act* this was changed. With its strong national security overtones, the title of the Act was instructive and gave a sense of urgency to a problem that was now not limited to individual computers (whether federal or not) but, instead, to a *national* infrastructure. As a result, cybercrimes were now federalised under one statute and this was achieved by introducing the term of a 'protected computer' instead of the more restrictive 'federal interest computer'. The new definition, based on an expansive reading of the interstate commerce clause, increased the federal scope of the law to encompass any computer connected to the internet.[100] Consequently, new powers were conferred to executive departments, such as the DOJ, which assumed supervisory responsibilities over the federalised crime, as well as to federal agencies such as the FBI, which was charged with the investigation of such crimes. The individual states, however, also received federal support since the FBI has field offices in the individual states and many of these now included specialized cyber squads called Cyber Action Teams. The latter were to provide expert assistance to law enforcement agents at all levels and could assist local and state agents in cybercrime investigations.[101]

[98] For instance, the federally funded Computer Emergency and Response Team reported a 498% increase in the number of computer intrusions between 1991 and 1994.

[99] See in particular 'The National Information Infrastructure Protection Act of 1996: Legislative Analysis by the Computer Crime and Intellectual Property Section of the US Department of Justice. Available at: http://www.cybercrime.gov/1030_anal.html

[100] This is addressed in detail by Brenner, S. (2004). On the interstate commerce clause see Brickey, K. (1996), The commerce Clause and Federalized Crime: A tale of two thieves, 543 *Annals of American Academy Political and Social Science* 27.

[101] CERT Coordination Center (2004), *How the FBI Investigates Computer Crime*, available at http://www.cert.org/tech_tips/FBI_investigates_crime.html

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Other complementary measures, such as the establishment of a special 'hotline', were also pursued. In June 2000, the FBI, in partnership with another federally funded organisation that supports state and local law enforcement efforts,[102] set up a national Internet Fraud Complaint Centre. Crimes could now be reported online with analysts reviewing and researching each of the complaints and disseminating the information to the appropriate federal, state, local, or regulatory agencies for criminal, civil, or administrative action. The unit –as with most other hotline mechanisms- could not conduct its own investigations but instead, reviewed complaints and referred them to the appropriate agency.[103] However, the FBI was not the only federal agency taking initiatives in the area of internet-related crimes. Another federal agency that acquired important competencies in the area of cyber crime was the United States Secret Service (USSS). The latter's role has gradually evolved from protecting the integrity of the nation's financial payment system to include, more recently, dealing with computer or cyber facilitated criminal activity.[104] This new competence was formalised in 1995 with the establishment of a nationwide Electronic Crimes Task Force (ECTF), based in New York, and specifically focused on helping companies improve their cybersecurity.[105]

At the same time as moves were being made to federalise computer crime and empower federal agencies in relation to its investigation, a set of parallel initiatives were undertaken in the interconnected policy area of cybersecurity. In fact, throughout the 1990s, US administrations had been concerned with the protection of the nation's so called 'critical information infrastructures'.[106] Of particular concern was the threat posed by hackers, who were very much an unknown and unpredictable element. The preferred approach was to establish a policy framework which would provide the security forces and/or

[102] See the National White Collar Crime Center, http://www.nw3c.org/

[103] Investigation and prosecution was therefore at the discretion of the receiving agencies. For further information see the http://www.ic3.gov/faq/

[104] For further information see the USSS website at: http://www.ustreas.gov/usss/

[105] The number of cities with an Electronic Crime Task Force has now been expanded from one (New York) to thirteen, thereby covering most major US cities. See the Electronic Crimes Taskforce website: http://www.ectaskforce.org/Regional_Locations.htm

[106] See the Congressional Research Service. Critical Infrastructure: A primer. 1998 Aug 13; CRS 98-675. Available at: http://www.fas.org/irp/crs/98-675.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute
DOI: 10.2870/1208

law enforcement agencies with mechanisms to detect and track actions at an embryonic stage of an attack.[107] Given that the US perceived itself to be disproportionately at risk from such attacks, it has been the first nation to seriously address the problem as part of a coherent policy strategy. At the same time, addressing the problem provided the opportunity for a variety of federalising initiatives.

Both the Clinton and the Bush Administrations put a lot of effort into thinking about cybersecurity and creating new agencies and institutions with responsibility for the nation's critical information infrastructures. During the early 1990s the debate concerning the protection of critical information infrastructures was characterized by competing interests. Military and national security interests, in particular, sought to expand their powers in the new post-Cold war security context. They propagated alarmist warnings about the potential dangers of an 'electronic Pearl Harbor' and used concepts such as 'cyberwar' and 'information warfare'.[108] The terminology was politically and normatively loaded in favour of viewing the issue from a defence lens. Framing computer and network security in terms of a national security threat offered many advantages, not least a greater scope for secrecy and less public scrutiny. The problem, however, was that there was no clear threat, at least in terms of classical conceptions of a military threat. Thus, although there was an important social construction of a potential 'electronic Pearl Harbor' or 'cyberwar' –fanned by prominent media coverage, which to all intents and purposes has persisted to this very day- US military and intelligence interests largely failed in the securitization of cybercrime.[109] However, this did not mean that the federal government was necessarily blocked, but that a different policy model was followed instead.

[107] See *ibid*.

[108] One of the best accounts of the role of discourse in setting the critical infrastructure protection agenda is provided by Bendrath, R. (2001), Cyberwar debate: Perception and politics in US critical infrastructure protection. *Information and Security*, 7.

[109] See in particular Green, Joshua. *The Myth of cyberterrorism*. The Washington Monthly Online. 2002

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Under the rubric of 'critical information infrastructure protection', a series of policy initiatives were promoted by the Executive which have resulted in a federalization of cybersecurity. A crucial juncture occurred in 1996, when President Clinton established a special commission[110] to study the vulnerability of key US infrastructures and to formulate a comprehensive national policy to address new threats such as cyber attacks. The Commission did not come out in favour of a 'national security' approach, but, instead, favoured a public-private partnership. Two years after setting up the Commission, President Clinton ordered the federal government to implement a framework with the private sector to secure the nation's vital information networks, 90% of which were privately owned and operated. At the same time, he called on the federal agencies responsible to develop a coherent national cyberspace protection plan by 2000. This was implemented through the adoption of two Presidential Decision Directives (PDD's) in May 1998.[111] The PDD's have since formed the basis for all subsequent policy initiatives in the area of cybersecurity. Most significantly, a host of federal oversight agencies were created by the PDD's.[112] But because of the tensions and overlapping interest among federal departments, namely: defense, law enforcement, and commerce, a complicated three-fold organisational structure was created.[113] Of the three federal agencies involved, it was the FBI that was to take the initial lead role. This was partly for historical reasons, especially in view of the FBI's expertise acquired in the area of computer crime during the 1990s. Moreover, the FBI had already hosted two groups involved in infrastructure protection,[114] both of which were already located at

[110] The President's Commission on Critical Infrastructure Protection (PCCIP) was established in July 1996 by Presidential Order 13010

[111] See Presidential Directive 62 (PDD-62) on Combating Terrorism and Presidential Directive 63 (PDD-63) on Critical Infrastructure Protection.

[112] Detailed information on the Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, White Paper, May 1998 is available at http://www.mipt.org/pdf/ClintonPolicyCIP_PDD63.pdf

[113] It included a prominent role for security interests, exemplified by the role of a National Coordinator at the National Security Council. The interests of the law enforcement community were satisfied by housing the National Infrastructure Protection Centre at FBI headquarters. While a Critical Infrastructure Assurance Office was also created and housed at the Department of Commerce with the aim of coordinating information sharing with the private sector.

[114] This was the Computer Investigation and Infrastructure Threat Assessment Center, and the interim Infrastructure Protection Task Force.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

FBI headquarters.[115] It was thus well placed to take a lead in this issue area. In short, one of the major reasons why the overt military perspective was abandoned was due to the prominent role of other government agencies – especially law enforcement- and the influential position of the private sector, which largely owned most of the critical information infrastructures.[116]

In sum, on the eve the terrorist attacks of 9/11 many elements of cybercrime had been effectively federalised. Furthermore, federal agencies had been appropriately empowered to deal with the problem. Nonetheless, most of the work would still be conducted at the state level with federal agencies providing assistance although they could still conduct their own operations within the states. A federalisation in the area of cybersecurity had been achieved, though, at the organisational level, the structure was horizontally fragmented among various federal agencies. Following the terrorist attacks of 9/11, two major policy responses, one legislative (the USA Patriot Act of 2001) and the other organisational (the creation of a new Department for Homeland Security), were promptly implemented with considerable implications for the area of internal security in general, and the issue of cybercrime in particular. The former considerably enhanced the FBI's investigative powers in cyberspace, while the latter represented the biggest reorganisation of the US government in over fifty years.[117]

The Patriot Act constituted a controversial piece of legislation that was pushed through Congress with unprecedented speed. Although 9/11 was not the 'electronic Pearl Harbor' that US policymakers had repeatedly warned against, it nevertheless facilitated the implementation of certain policy 'solutions' that had been 'in the air' during much of the 1990s.[118] One of the most revealing aspects of the Patriot Act was the degree to which it impacted

[115] For a discussion of the FBI's role, see EPIC 'Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructures Protection'. 1998. Available at: http://www.epic.org/security/infowar/epic-cip.html.

[116] Bendrath, R. (2001).

[117] Clarke, J, (2004), The United States, Europe, and Homeland Security: Seeing soft security concerns through a counterterrorist lens, *European Security*, 13: 117-138.

[118] In relation to the policy debate in the late 1990s see O'Neil, M and Dempsey, J (1999) Critical Infrastructures Protection: Threats to Privacy and Other Civil Liberties and Concerns with Governments Mandates on Industry. *Depaul Busienss Law Journal* . 1999; 12:97.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

on cybercrime. The threat of terrorism was used to justify increased penalties for minor and mid-level computer crime, which, although containing a criminal element, bore absolutely no relation to terrorism. In this vein, the Patriot Act greatly expanded the provisions of the *Computer and Fraud Abuse Act* of 1986 especially in relation to the maximum penalties for cyber trespassing offences and by ensuring that violators need not have intended to cause general damage or harm.[119]

In the aftermath of 9/11, a radical reorganisation of federal agencies responsible for the cybercrime also took place. In early 2002, the FBI centralised all its efforts in the cyber domain within a single division. It did so primarily in order to consolidate what had been a historically fragmented approach to cybercrime. The FBI's new Cyber Division brought together all its efforts to conduct criminal investigations of crimes that occur over the internet or involve computers or networks within a single department.[120] Although many criminal investigations would still be operated from the field offices located within the states, major cases were to be managed directly from headquarters.[121] This constituted a big change for the FBI since, historically, the field offices had run cases.[122] In addition, the Cyber Division expanded its specialized cyber squads[123] at most FBI field offices and its Regional Computer Forensic Laboratories throughout the country to *assist* state and local law enforcement.[124] It also incorporated within its headquarters the 'hotline' unit (the Internet Fraud Complaint Center) whose remit was now expanded to cover *all* areas of internet crime. Accordingly, the unit was now renamed in 2003 -the Internet Crime Complaint Center (IC3) - to denote its new expanded comptencies[125]. However, despite the consolidation of the

[119] See in particular Brenner (2004).

[120] Statement of Steven M Martinez, Deputy Assistant Director, Cyber Division, Concerning Computer Provisions of the USA Patriot Act before Subcommittee on Crime, Terrorism, and Homeland Security Committee on the Judiciary, House of Representatives, April 21, 2005.

[121] Kane, Margaret, 19/06/2002, The FBI's cybercrime battle, CNET News.com http://news.com.com/The+FBIs+cybercrime+battle/2008-1082_3-937420.html

[122] See Statement of Steven M Martinez *ibid*.

[123] These are the mobile Cyber Action Teams (CATS) which assist with specialized expertise on matters related to cyber crime not just in the US but around the globe.

[124] Statement of Steven M Martinez above.

[125] For more information see the Internet Crime Complaint Centre at http://www.ic3.gov

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

FBI's cybercrime efforts, it was to lose its lead role in the area of critical information infrastructure protection. This now went to the newly created Department of Homeland Security. Interestingly, at the same time as he established the Department of Homeland Security, President Bush created a new and high profile post.[126] Formally known as the 'Special Advisor to the President for Cyberspace Security', but more commonly referred to as the 'Cyberspace Czar', the new post was at the highest political level, the White House.

In many respects, the creation of the new DHS in January 2003 represented a consolidation of efforts in the cybersecurity domain after almost a decade of activity, spanning various departments and countless organizations (according to an official count over 50 organisations).[127] All federal efforts related to critical information infrastructure protection were incorporated within a new cabinet-level directorate.[128] Created in June 2003, it now served as a national focal point for cyber security making it the single largest computer security organization the U.S. government has ever had.[129] But as one FBI official argued, the new department handles only intrusion cases, as for all other cybercrimes, the new agency would not have any impact, since this was within the FBI's policy remit.[130]

With new criminal legislation in place, new enforcement powers for policing, and internal security issues refocused within a new executive department, the only remaining issue to address was the private sector. In late 2001, the newly appointed Cybersecurity Czar began what became a year long campaign to address the cybersecurity dilemma and formulate a 'National Strategy to Secure Cyberspace' (the National Strategy). The National

[126] See Executive Order 13231 of October 16, 2001.

[127] For instance the Government Accounts Office Report 'Critical Infrastructure Protection: Significant challenges need to be addressed' (GAO -02-961 T) found that over 50 organizations, including five advisory committees, six organizations in the executive office of the president, 38 executive branch organizations and three other organizations are involved in critical information infrastructure protection.

[128] This is the Department of Homeland Security's "Directorate of Information Analysis and Infrastructure Protection".

[129] Fitzgerald, M. (2003), *Homeland Cybersecurity Efforts Doubted*, SecurityFocus, 2003-03-11.

[130] See Statement of Steven M Martinez *ibid.*

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Strategy became the focal point for the Bush Administration's efforts in the field of cybersecurity.

Initially, there were high hopes for the National Strategy to address the country's post-9/11 cybersecurity problems. A set of recommendations for the national cyberspace strategy were proposed[131] with early drafts including proposals to require ISPs to include firewall software, and that government agencies should use their power as a major purchaser of computer software to push vendors to improve the security of their products, as well as initiatives to impose legal liability for failure to meet basic security standards. These proved unacceptable to business and one of the most notable features of the evolution of the National Strategy is how, over the course of the year, the plans became progressively watered down. The quiet release of the National Strategy stood in contrast to the Administration's original plan to release the draft at a high profile event.[132] In a further twist, two weeks before the release of the National Strategy, the Cybersecurity Czar, by far the most enthusiastic promoter of regulatory intervention, resigned from his post. The final outcome of the plan, approved in February 2003, was a watered down version that contained no legislation and proposed no government mandated regulation.[133] Instead, the final document directs the government to lead by example by tightening the security of *federal* information systems.

Despite its weak regulatory character, the National Strategy reveals some major insights on the US administration's thinking on how to resolve the nation's cybersecurity dilemma that marks a significant policy evolution. With regard to private industry, policy is increasingly promotional in character and predicated on a voluntary public-private partnership. In this regard, private industry, and the information technology sector in particular, have been largely successful in two main respects. First, they have conspicuously avoided the spectre of government mandated regulation –which was a real

[131] See the President's Critical Infrastructure Protection Board, *The Draft National Strategy to Secure Cyberspace*, September 2002.
[132] See Krebs, Brian. White House Releases Cybersecurity Plan. Washingtonpost.com. 2003 Feb 14.
[133] See the President's Critical Infrastructure Protection Board, The National Strategy to Secure Cyberspace, February 2003. Available at, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

threat during the Cybersecurity Czar's year long campaign to address the cybersecurity problems. Second, they have attracted considerable federal R+D funds for cybersecurity related programs. These are not inconsiderable sums with, for instance, over 4 billion US dollars allocated to cybersecurity for a single year's federal budget.[134] While the self-regulation contours are noticeable, there was also a policy evolution in terms of the scope of the problem. In this sense the title, 'National Stategy to Secure Cyberspace', is indicative and represents an evolution towards a broadening of the problem, from what was initially a security concern about 'critical information infrastructure', to one that encompasses all of cyberspace. In other words, it is no longer just a defense issue, everyone is now implicated all the way down to the home user.

4. The European Union: Cybersecurity

As in the US, computer security had been slowly advancing on the European policy agenda since at least the late 1980s. It first appeared on the EU policy radar screen in 1987 when the Commission's Legal Advisory Board drew attention to the threat.[135] However, for the greater part of the 1990s, cybersecurity issues were not the subject of any specific policy measures or actions at the EU level. Instead, the issue formed an indirect component of two major policy fields in which the EU was becoming increasingly active: the regulatory framework for telecommunications and the data protection regime.[136] Still, this did not amount to a cybersecurity policy although it did display a disposition, on the part of EU authorities, to use regulatory mechanisms to achieve certain policy goals. Thus until the late 1990s, issues related to cybersecurity were dealt with indirectly at the EU level.

---

[134] This was for the federal budget year of 2003. This figure simply dwarfs any comparable R+D subsidies from the EU and its member states. The sum of 4.2 billion dollars for cybersecurity research is arrived at in a study compiled by Thierer, A.D., Crews Jr., C.W., and Pearson T. (2002), Birth of a digital new deal. *CATO Policy Analysis* No 457. 2002 Oct 28.

[135] The Commission Legal Advisory Board requested a report on the issue in December 1987, see *Sieber/Kaspersen/Vandenberghe/Stuurman*, The Legal Aspects of Computer Crime and Security, 1987.

[136] From the early 1990s onwards central provisions concerning the security of network operations were part of the EU framework for telecommunications (the Liberalisation Directive 90/388/EC; Interconnection Directive 97/33/EC and the Voice Telephony Directive 98/10/EC) and the 1995 Data protection directive 95/46/EC.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

To understand how the issue of cybersecurity became the subject of increasing EU policy attention it is necessary to take into account growing concerns about the phenomenon of organised crime. Since the early 1990s member states had been intensifying cooperation between their law enforcement and judicial services in the fight against organised crime.[137] Within this context, an influential community of security experts was able to explicitly link the issue of computer security to that of organised crime.[138] Their first success came with the Action Plan to combat organised crime, which was endorsed by EU leaders at the European Council of Amsterdam in 1997.[139] More specifically, the Action Plan included a request for a study to be commissioned on computer related crime. Known as the COMCRIME[140] study, it was undertaken by a leading criminal law scholar and computer crime specialist and its findings were presented to the Commission the following year. The study drew attention to the risks and vulnerabilities of the emerging information society and the need for an urgent EU level response.[141] In this incremental fashion, it is fair to say that, by the late 1990s, cybercrime was slowly advancing onto the EU policy agenda. In particular the Commission, with political support from the Council and the law enforcement communities, was increasingly articulating the case that cybercrime required an EU level coordinated response.

Following the entry into force of the Treaty of Amsterdam in May 1999, and a specially convened summit at Tampere in the same year, a vigorous new drive was undertaken at the EU level in the fight against organised crime. In particular, the 1999 Tampere Summit was a landmark event not only because EU leaders devoted the entire summit to questions of justice and home affairs but also because, for the purposes of the present analysis, EU leaders specifically included cybercrime (referred to as high-tech computer crime) in

[137] See for instance Walker, Neil (2003) The Pattern of Transnational Policing. Neburn, Tim ed. A Handbook of Policing. London: Willan Publishing.

[138] Interview with European Commission official at the Joint Research Centre 23/05/04.

[139] See the European Council conclusions, 16, 17 June Amsterdam, 1997 available at: http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/032a0006.htm

[140] Sieber, U. Legal Aspects of Computer-related Crime in the Information Society . COMCRIME Study. 1998.

[141] See Comcrime Study pg 3.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

their list of priority areas.[142] However, apart from a set of grandiose political declarations at the highest political level, nothing in terms of actual policy initiatives had yet been put forward. In the meantime a series of initiatives were implemented, usually prefixed with the letter 'e'. The most notable of these were the eEurope initiatives, launched by the Commission President, Romano Prodi, in December 1999.[143] The Commission President had identified 10 priority areas for action with ambitious targets to be achieved through joint action by the Commission, the member states, industry and civil society.[144] Noticeably absent from the eEurope action plan was any reference to cybersecurity. With very high profile denial-of-service attacks against Yahoo, CNN, eBay and other e-commerce web sites in February 2000 and with the outbreak in of the 'I love you" virus in May 2000, all of which mobilised business interests, this startling omission was redressed. The initial 10 key targets were swiftly revised and a comprehensive eEurope 2002 Action Plan[145] was adopted around three main objectives,[146] one of which was the goal of achieving *secure* internet infrastructure.

The eEurope Action Plan was an example of a new mode of governance known as the 'open method of co-ordination'.[147] It identified the increasing threat caused by disruptions such as viruses and denial of service attacks and listed a set of targets to be achieved in this area. It was hoped that greater policy coordination in the area of cybersecurity could be achieved through this co-regulatory approach. Sponsored by the market-friendly DG Information Society, the plan argued that 'the market should, as far as possible, be left to

[142] See Presidency Conclusions of the Tampere European Council of 15 and 16 October 1999, available at http://ue.eu.int/Newsroom/LoadDoc.asp?BID=76&DID=59122&LANG=1

[143] See the eEurope initiative, available at http://europa.eu.int/information_society/eeurope/news_library/pdf_files/initiative_en.pdf

[144] See Rapid Press release Prodi launches "eEurope" Initiative to accelerate Europe's transformation into an Information Society IP/99/953.

[145] See the eEurope Action Plan 2002 available at: http://europa.eu.int/information_society/eeurope/action_plan/pdf/actionplan_en.pdf

[146] These were 1) a cheaper, faster and **secure** Internet; 2) Investing in people and skills and 3) stimulate the use of the Internet.

[147] An analysis of the 'OMC' that is relevant to this argument is offered Scharpf, Fritz W. (2001), European Governance: Common Concern vs the Challenge of Diversity. Jean Monet Working Papers. (No. 6/01 Symposium: The Commission White Paper on Governance).

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

define the adequate security level for user needs'.[148] Within the space of a year, however, this market-friendly discourse was abandoned in favour of a more regulatory and legislative approach. The landmark Tampere Summit of 1999, with its focus on organised and transnational crime, had already provided the Commission with a political mandate and a green light to put forward legislative proposals. Having been deemed a priority issue by successive European Council Summits,[149] cybercrime could be said to be now firmly on the EU policy agenda. A general policy dealing *exclusively* with the issue was not yet in place though. With the adoption in January 2001 of the DG JHA sponsored Cybercrime Communication,[150] cybercrime received a major political impetus. Although the document did not contain any specific legislative proposals *per se,* it has since defined the EU cybercrime agenda by providing an outline of how EU policymakers would tackle network security issues and by listing the forthcoming EU level actions.

Nonetheless, during the consultation process that followed the Commission's cybercrime communication, its proposals were heavily criticised by business organisations.[151] According to these interests, the Commission had disproportionately focused on illegal content issues, which, while important, did not address the fundamental issues of growing dependence on the safety and reliability of the information infrastructures. Business organisations were particularly keen to make a distinction between a) security offences and b) content offences. For them it was clear that the security dimension, i.e. hacking, denial of service attacks and cyber piracy, should take precedence over the content issues, such as child pornography. They viewed the latter as a traditional crime which merely used a new medium.[152] The private sector

[148] See pp 10 of the eEurope Action Plan 2002 available at: http://europa.eu.int/information_society/eeurope/action_plan/pdf/actionplan_en.pdf

[149] See for instance Recommendation 7 on cybersecurity of the Prevention and control of organised crime: A European Union strategy for the beginning of the new millennium. (OJ 2000 C124, 3.5.2000)

[150] European Commission Communication Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer related crime. 2001 Jan 26; COM(2000) 890.

[151] See the response to the European Commission's 2001 Request for comments on the Cybercrime Communication, available at:
http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Comments/index.htm

[152] See *ibid.* the comments by ICL. They pointed out that the word 'child pornography' appeared more than fifteen times and stated that they 'reject absolutely the implication that child pornography is

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

was much more concerned with dealing with the new threat of cybercrime and, in particular, the security of information infrastructures. Largely as a result of these reactions, it would be necessary, henceforth, to distinguish between content issues on the one hand, and cybersecurity issues on the other. This sentiment was echoed by the European Council at its summit meeting of March 2001 where EU leaders called on the Commission to 'develop a comprehensive strategy on security of electronic networks including practical implementing action'.[153] The outcome of this specific mandate from the member states, as well as the increasing calls from the private sector, resulted in the implementation of a new cybersecurity strategy at the EU level.[154]

As noted above, issues related to network security had been taken up in many previous initiatives. Rather than being appended to broader notions of 'organised crime' or, even, 'cybercrime', the Commission's network and information security proposals of 2001 constituted the first policy actions to *exclusively* address the issue of cybersecurity.[155] Sponsored by DG JHA, the policy agenda set out an ambitious plan that would require new legislation on network security at the European level. Moreover, EU policymakers also proposed to create a new EU independent agency to monitor cybersecurity. What is of most interest in relation to the EU's new cybersecurity policy was not so much the progress made on defining network and information security and the overview of the threats, but rather its strategy. In a nutshell it consisted of three elements: 1) more EU level coordinated action; 2) an enhanced regulatory framework within the data protection and telecommunications regime (i.e. first pillar activities) and greater police and judicial cooperation (i.e. in the third pillar); 3) the acknowledgement that

---

a computer-related crime any more than that it is a camera-related crime, a postal service-related crime or a video-related crime…the domination of child pornography within the Communication dangerously distorts any balanced appraisal of computer-related crime.'

[153] Conclusions of the Presidency, European Council Stockholm Summit 15 and 16 June 2001 available at:
http://www.europarl.eu.int/summits/pdf/sto1_en.pdf

[154] The new approach was formulated in the European Commission's Communication. *Network and Information Security: Proposal for a European approach*. COM (2001)0298.

[155] See the *Proposal*

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

serious market imperfections exist in the domain of cybersecurity and that, on this basis, leaving cybersecurity to the market was simply not an option.[156]

On the eve of the 9/11 attacks in 2001, it was thus possible to discern a new EU policy on cybersecurity. Spearheaded by DG JHA, it offered a stark contrast to the 'softer approach' of the eEurope action plans. With the 9/11 attacks, however, an entirely new urgency was attributed to the issue of cybersecurity and, as in the US, numerous proposals were put forward to combat terrorism by EU policymakers. But in addressing the terrorist threat, a much broader net was cast. In relation to cybersecurity, this took the form of an explicit link being drawn between terrorism and the cyber threat. For instance, one of the outcomes was the speedy adoption of a Framework Decision to combat terrorism[157] (just nine months after the attacks) which included new definitions for terrorist offences and established common criminal sanctions. Among the list included in Article 1 (d) was the terrorist offence of causing extensive destruction to infrastructures such as information systems.[158] Security advocates were now increasingly making the link between, not just organised crime, but also terrorism and the new cyber threat.[159] Although much work had been done earlier, the terrorist attacks were to significantly alter the security environment. In particular, the newly expanded DG JHA was able to capitalise on the window of opportunity that had presented itself to pursue its agenda for strengthening EU level cooperation on internal security issues. Six months after the 9/11 attacks, sufficient consensus had been reached among the relevant stakeholders, and the Council, for the Commission to release its legislative agenda for the cybersecurity domain.

The first part of the strategy to be implemented was in the traditionally less sensitive first pillar. In 2002, data protection and telecommunications issues were brought together under a single and comprehensive regime with major

[156] See the *Proposal*

[157] See the Council of the European Union. 'Framework decision on combating terrorism'. 2002/475/JHA.

[158] See the Council of the European Union. 'Framework decision on combating terrorism'. 2002/475/JHA.

[159] Interview with European Commission official at the Joint Research Centre 23/05/04.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

cybersecurity implications.[160] The new regime now obliged all electronic communication providers to ensure the confidentiality of data and protect communications from unlawful interception. The strategy pursued in the third pillar area of police and judicial affairs represented a more radical regulatory turn however. In April 2002, the Commission announced its proposals for harmonizing EU criminal laws with regard to attacks against information systems.[161] New measures were needed because the threat of intentional attacks against information systems now constituted a 'threat to the achievement of a safer Information Society and an Area of Freedom, Security and Justice, and therefore require a response at the European Level'[162]. Also a new rhetorical device was introduced that, up until this point, had been conspicuously absent in EU policy discourse –the spectre of cyberterrorism. EU policymakers now argued that 'more serious attacks [on information systems] could not only lead to serious financial damage but, in some cases, could even lead to loss of life (e.g. hospitals systems, air traffic control systems etc)'.[163] Furthermore, the Commission identified significant enforcement gaps among the member states that it argued could act as a barrier to effective police and judicial co-operation in the area of cybersecurity.

In early 2005, a Framework Decision on attacks against information systems was finally adopted.[164] As a result of the latter there will be a greater harmonisation of criminal laws among EU member states in the area of cybercrime. The new EU rules explicitly deal with the vulnerabilities of information systems and cover most forms of cybercrime such as hacking, denial of service and virus attacks –i.e. the three most common forms of cybercrime. Moreover, sanctions were harmonised which include penalties of at least one year for cybercrime offences. This would bring into play the instruments of European police and judicial cooperation and, in particular, the

[160] See the European Commission's Privacy and Electronic Communications Directive 2002/58/EC.

[161] See the European Commission's Proposal for a Council Framework Decision on attacks against information systems. 2002, COM (2002) 173.

[162] See pp1 of the Explanatory Memorandum in the European Commission's *Proposal for a Council Framework Decision on attacks against information systems.* 2002, COM (2002) 173.

[163] See pp4 of the Explanatory Memorandum of the European Commission's *Proposal for a Council Framework Decision on attacks against information systems.* 2002, COM (2002) 173.

[164] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

DOI: 10.2870/1208

new European arrest warrant.[165] In another significant development, the new measures ensured that criminal liability would also extend to legal persons, such as corporations, with the result that a company could be held liable if an offence resulted from a lack of supervision. This gave the Framework Decision potentially very broad liability scope, especially with regard to companies.[166] On the whole, the business community had been quite receptive to the Commission's draft. However, they were particularly critical of the liability provisions.[167] But since the initiative was taken under the intergovernmental third pillar not only industry, but also the European Parliament, played a more peripheral role during the drafting process.

In order to supplement the first and third pillar legislative measures noted above, a new independent EU agency was also created.[168] It was supposed to help the member states in their efforts to deal with cybersecurity issues. The independent agency's ultimate aim is to be able to prevent and respond to major network and information security incidents. The problem at the EU level is that the member states are at very different stages of their work in dealing with cybersecurity issues, and, furthermore, these asymmetries have been amplified since enlargement. Interestingly, in order to justify EU action in the area of cybersecurity, and find a legal basis for the creation of the new independent agency, the Commission made recourse to an internal market argument. It argued in its proposal that 'the introduction of technically complex requirements for security in networks and information systems at Member State level and Community level could hamper the deployment of the Internal Market principles'.[169] Greater EU-level coordination through an independent agency is therefore being promoted to ensure that interoperable security solutions are developed among the member states in such a way that these

[165] See the opinion of the Rapporteur Charlotte Cederschiold in the European Parliament Report on the commission proposal for a Council framework decision on attacks against information systems A5-0328/2002.

[166] For a related discussion see Mazumdar, A. (2003), EU Council Agrees to Move forward with proposals to harmonize computer crime laws. *Computer Technology Law Report* . Mar 21; 4(6).

[167] See for instance the Business Software Alliance comments on the proposed framework decision at http://global.bsa.org/uk/policyres/EUPolicy/BSA_Framework_Decision_Cybercrime.pdf

[168] See pp 3 of the European Commission's Proposal for a regualtion eEstablishing the European Network and Information Security Agency COM(2003) 63 final.

[169] See pp 3 of the European Commission's Proposal for a regualtion eEstablishing the European Network and Information Security Agency COM(2003) 63 final.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

do not pose barriers to the functioning of the single market. However, this has led to conflict between the Commission and the UK. The latter has challenged the legal basis on which this agency was created, i.e. the internal market justification. At issue was the Commission's recourse to Article 95, a legal basis in which QMV applies, rather than Article 308 where unanimity would have applied.

Although the response of the Court of Justice is still pending, the Advocate General's opinion has supported the UK position.[170] The fledgling agency has thus commenced its operational functions with an important Court case looming. Despite such politicisation, the new agency has begun to work closely with the member state regulatory authorities all of which are at very different stages and levels of preparation in the cybersecurity domain. Nonetheless, it is important to note that the agency's main role will be advisory since it will not have any regulatory powers. Essentially, its task will be to collect and analyse data, conduct major risk assessments, and deliver opinions to the Commission with the ultimate aim of enhancing cooperation among the member state regulatory agencies and other parties concerned with cybersecurity. The European Network and Information Security Agency (ENISA) became operational in 2004 and, as with most other EU decentralised agencies, is located outside Brussels.

The EU has also recently stepped up its efforts in the area of critical infrastructure protection following growing calls by member state leaders. These developments are especially noteworthy given the national security implications of the policy area. The impetus came after the terrorist attacks on the Madrid transport network in March 2004. At this point the EU leaders who gathered for the traditional June Summit explicitly called on the Commission to prepare proposals for protecting critical infrastructures.[171] The plan, put forward by the Commission in October 2004, sets out an agenda for EU-level

[170] See Advocate General's opinion in case c-217/04 of 22 September 2005.

[171] See the European Council's Conclusions 17/18 June, 2004 available at http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/81035.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

actions to protect critical infrastructure.[172] The *Communication* warned of the increasing dangers of terrorist attacks on Europe's critical infrastructures, especially its transport and communications network. It also drew attention to the threat of cyberterrorism which could now be used in combination to physical attacks.[173] Presently, an EU policy that will involve the development of a 'horizontal plan' known as a European Programme for Critical Infrastructure Protection (EPCIP) is being developed. Given the growing security concerns, intensive interactions among Commission officials and national representatives from security agencies were conducted throughout 2005. The key focus for EU level action is on those areas which have the greatest 'transboundary' effects. And it is here where the communications and information infrastructure, arguably the most 'transboundary' of all the critical infrastructures listed, plays a crucial role.[174] In terms of present EU policy actions it is also the most developed. Not only has a specialised independent EU agency (ENISA) already been created to deal with cybersecurity, but EU funds are being directed to addressing the threat. For instance, an EU sponsored Taskforce on Critical Information Infrastructure Protection[175] was created in April 2005 to bring together experts from the 25 member states to combat perceived cybersecurity threats. Although the EU's policy on critical infrastructure is evidently at an embryonic stage, and the impetus is notably intergovernmental, the trend is clearly one towards much greater coordination at the EU-level.[176] It is a significant development given that this policy area brings to the fore some of the most sensitive questions concerning national security.

[172] See page 3 of the European Commission's Communication on Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final.

[173] See page 3 of the European Commission's Communication on Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final.

[174] The latest plans on EU-level actions are detailed in the Commission's Green Paper on a European Programme for Critical Infrastructure Protection COM (2005) 576, it has been further endorsed by the Council Decision C/2005/3179.

[175] The taskforce is funded by the IST priority, 6th Framework Programme, and is called C12RCO, (IST-2005-15818).

[176] Interview with official working on Critical Infrastructure Protection within the Joint Research Centre of the European Commission, 24/06/05.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

5. Switzerland: Cybercrime

In the case of Switzerland, the cybercrime problematique has emerged mostly as a single issue area. Unlike with the US and EU cases, where it is analytically more useful to distinguish between the two overlapping domains of illegal content and cybersecurity, in Switzerland policymakers addressed the issues simultaneously under the category of 'cybercrime'. Therefore, for the purposes of coherency the analysis that is presented below follows the same format.

In Switzerland over the past decade, the increasing internationalisation of crime, and the emergence of the cybercrime threat, has put a considerable strain on the extremely decentralised law enforcement set-up. Law enforcement, and in particular the investigation and prosecution of crime, is a cantonal competence. Essentially, there are no federal investigative units, and the cantons guard their prerogatives in this domain with great zeal. There is one area however, where, in response to international pressures, certain investigative procedures have been federalised. This is in the very narrow area of 'organised crime'. Thus, although a federal police office exists it resembles an administrative unit and its remit is strictly limited to only investigating 'organised crime'. Furthermore, the strict and very narrow definition of organised crime contained in the Swiss Penal Code, effectively ensures that most instances of these crimes are, in any case, investigated by the Cantons.[177] In view of such constitutional constraints, and the extremely decentralised nature of the Swiss law enforcement and justice system, it comes as no surprise that cybercrime, given the intensive resources required to mount successful investigations and prosecutions, would pose problems for a system characterised by significant variation among the 26 police corps and prosecuting authorities (one for each canton).

Realising the challenges posed by the internet during the mid-1990s, federal policymakers took a series of initiatives. Following a request by internet access providers, an interdepartmental Working Group comprising the most relevant federal departments and agencies was formed in September 1995.

[177] Interview with crime analyst in Geneva 22/05/04.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Under the lead of the police and justice department, its remit was to study the major challenges posed by the internet's proliferation for the Swiss policy context, especially with regard to criminal law.[178] It focused on various forms of internet abuse -subsequently referred to in Swiss policymaking circles as cybercriminalité or Netzwerkkriminalität. Among their primary concerns was the issue of illegal content (pornography, especially child pornography and racist material) and the connected question of the responsibility and liability of internet providers for the availability of such illegal content on their networks. The issue of liability was problematic and the Working Group recommended a code of self-regulation among the ISPs. What was most surprising about these initial discussions was the fact that the role of the cantonal authorities in the fight against cybercrime was not even mentioned.[179] Within a few years, however, this anomaly would be more than compensated for.

Growing concerns about the internet as an easy channel for disseminating illegal content and the lack of resources among cantonal police forces, led the Intercantonal association of prosecuting authorities to ask the federal police department in 1998 to create an embryonic internet monitoring unit. Known as 'Internet-Monitoring', it was rather misleadingly referred to in the media as an 'internet police force'.[180] Essentially, it was a pilot project that involved two part-time agents who monitored illegal online activities with a focus on racist and xenophobic material. Most importantly, it created no new federal competencies, i.e. investigation and prosecution stayed with the cantons. By the end of 1999, however, and after only two years in operation, the experiment was terminated.

---

[178] See the Office fédéral de la Justice, Berne, mai 1996, Le Nouveau Média Interroge Le Droit, Rapport d'un groupe interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet, available at http://www.ofj.admin.ch/etc/medialib/data/kriminalitaet/gesetzgebung/netzwerkriminalitaet.Par.0012.File.tmp/rf-internet-f.pdf

[179] For instance, see the final report of the Working Group. Office fédéral de la Justice, Berne, mai 1996, Le Nouveau Média Interroge Le Droit, Rapport d'un groupe interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet, available at http://www.ofj.admin.ch/etc/medialib/data/kriminalitaet/gesetzgebung/netzwerkriminalitaet.Par.0012.File.tmp/rf-internet-f.pdf

180 The association is actually known as the Cantonal conferece of prosecuting authorities. Also see article in the NZZ "Schweizer Polizisten auf Patrouille im Internet; Schwierige Ermittlungen im globalen Dorf", 27.2.1998.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Over the course of the late 1990s, much of the debate focused on the responsibility of ISP's for illegal content distributed on their networks. However, by framing the policy debate in terms of ISP liability, attention inevitably gravitated towards the issue of illegal content, such as pornography or racist material, rather than computer crimes. In the same year as the federal police initiated its 'internet-monitoring' pilot, a letter was sent to all the ISP's inviting them to block access to potentially offending sites.[181] In the letter, the federal police argued that the ISPs could be made liable for the transmission of illegal racist content over their networks. This generated a great deal of controversy,[182] not least because the law was not clear on the issue of liability. Furthermore, the ISPs doubted the technical feasibility of undertaking such a filtering task. As a result of the controversy a more cooperative approach was eventually agreed. A contact group between the federal authorities and the various national ISPs was established to discuss legal and technical preventative measures, including the blocking of websites with the offending (illegal) content, and measures for self-regulation among the ISPs.[183] The arrangement was soon tested when in 1999 the cantonal prosecution of Zürich asked an ISP to communicate the identity of a person offering child pornography over the internet.[184] The ISP refused and this ultimately ended up before the Supreme court.[185] The latter confirmed that, based on the existing telecommunication law, the ISP had to give this information to cantonal prosecutors. The case also highlighted the increasing need for international cooperation in this area (it had originated from a tip-off from German authorities)[186] and brought to the fore the problematic question

[181] See the Avis de la Police fédérale, avril 2000, *La responsabilité pénale des fournisseurs de services Internet*, available at http://www.rhf.admin.ch/themen/netzwerkkrim/2000-05-15-internet-isp-f.pdf

[182] See NZZ article "Bundespolizei bekämpft Rassismus im Internet; Ein Schnellschuss sorgt für Kopfschütteln, 31.7.1998.

[183] Schwarzenegger, Christian (2002) Computer Crimes in Cyberspace, A comparative analysis of criminal law in Germany, Switzerland and Northern Europe, Jusletter available at http://www.weblaw.ch/jusletter/jsp?ArticleNr=1957

[184] See NZZ article "Aus dem Bundesgericht; Kinderporno im Internet; Swiss Online zur Auskunftserteilung verpflichtet", 12.12.2000.

[185] Decision 1P.608/2000 from 7.11.2000.

[186] See NZZ article "Das ist nur die Spitze des Eisbergs; Staatsanwalt Andreas Brunner zur Kinderpornographie", 2.10.2002.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

of investigative procedures in Switzerland's extremely decentralised policy context.

Following the multiple interactions between distinct federal agencies, the courts, and the interdepartmental working groups, by the end of the 1990s, the Parliament also became an arena for political contestation on the issue of cybercrime. A 1998 parliamentary motion[187] had already called for further clarification of the liability issue, implicitly arguing that voluntary codes of conduct, or self-regulation on the part of ISPs was insufficient. Such a move would require a modification of the penal code however. On this point the Federal Council disagreed and preferred to adopt a wait and see approach on the question of ISP liability.[188] This strategy was not unconnected to the fact that the EU was in the very process of passing legislation (its e-commerce directive) precisely on this issue.

As a result of the increasing politicisation of cybercrime, a number of initiatives were submitted and these became the subject of further parliamentary discussion.[189] In particular, a parliamentary initiative[190] by the canton of Geneva in 2000, framed in terms of paedophilia and chid pornography, called for the re-establishment of the disbanded 'internet-monitoring' unit and a greater coordination among the levels of government. In parallel, a more detailed call for a federalisation of cybercrime by a parliamentarian in the same year led to a number of developments. Known as the Pfister motion,[191] it drew explicit attention to the broad issue of cybercrime, which went *beyond* illegal content and also included the security of information networks. Furthermore, it explicitly argued that responsibility for cybercrime should not be left to the cantons, the federal police should

[187] 98.3467 Motion, Criminalité sur Internet. Responsabilité du fournisseur d'accès.

[188] See the Avis du Conseil fédéral du 30 novembre 1998, which is available at http://www.parliament.ch/afs/data/f/gesch/1998/f_gesch_19983467.htm

189 The following parliamentary interventions can be mentioned in this regard: motion, legal affairs Commission of the National Council (01.3012), interpellation, Tillmanns Pierre (00.3235), motion, Commission 00.16 of the National Council (00.3206), interpellation, Freund Jakob (00.3059), cantonal initiative of Geneva (00.314), motion, von Felten Margrith (98.3467), motion, Jeanprêtre Francine (97.3487), postulat, legal affairs Commission of the National Council (96.3005).

[190] See the 00.314 - Initiative cantonale. Lutte contre la pédophilie.

[191] See the 00.3714 motion, Cybercriminalité. Modification des dispositions légales.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

intervene.[192] It was followed by an additional initiative (known as the Watermann motion) the same year calling for greater centralisation in view of the fact that the 'investigation of crimes committed on the internet is laborious…and there are a number of cantons lacking the human resources and an adequate infrastructure for effectively investigating these crimes. The fact that there are 26 different criminal procedural codes and police forces is an obstacle for conducting effective investigations'.[193] The initiative called for a centralisation, at the federal level, of the investigation and prosecution of cybercrimes. At the same time an active lobby group was created, the Marche blanche. Formed in 2001, it immediately began lobbying parliamentarians for tougher legislation, which included further centralisation of investigative procedures in the fight against child pornography.[194]

As a result of these high profile calls for parliamentary action in the area of cybercrime, a series of consultation processes and working groups were established to study the matter further. Nonetheless, the scope for the federalisation of cybercrime appeared remote. Despite the numerous parliamentary initiatives that, since at least 1996, had called for further centralisation, the Federal Council was adamant that 'a centralisation of investigative competencies [in the domain of cybercrime] would represent a fundamental *mutation* of the Penal system'.[195] Moreover, the parliament had also rejected efforts to federalise competencies for cybercrime.[196] Although a federalisation of investigative competencies had been blocked, new federal measures on substantive criminal law were, nonetheless, passed. To this end,

[192] In fact the motion argued that in relation to cybercrime 'Cette responsabilité ne doit pas être abandonnée exclusivement aux cantons. La Police fédérale doit être en état d'intervenir'.

[193] Author's translation. See Parliamentary initiative 01.3196 *Améliorer la procédure de lutte contre la cybercriminalité*, Déposé par Aeppli Wartmann Regine.

[194] A list of sponsored parliamentary motions can be found on its website http://www.marche-blanche.ch/interventions.php

[195] Author's translation, see the Avis du Conseil fédéral du 12 septembre 2001, available at http://www.parlament.ch/afs/data/f/gesch/2001/f_gesch_20013196.htm

[196] For an overview of the different positions and the bargaining process see the Conseil des Etats, Rapport de la Commission des affaires juridiques du 2 mai 2002, 00.314 n Lutte contre la pédophilie, 01.3012 n Lutte contre la pédophilie, 01.3196 n Améliorer la procédure de lutte contre la cybercriminalité, available at http://www.parlement.ch/afs/data/f/bericht/2000/f_bericht_s_k25_0_20000314_0_20020502.htm#5

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the Penal code (Art. 197 Penal Code) was amended so that possession of child pornography would be punishable with up to 1 year imprisonment.[197]

Between the late 1990s and 2004, federal policymakers undertook a number of measures to examine the competency problem in relation to cybercrime. Given the controversies surrounding the area, the calls for greater legal clarity on cybercrime issues, and the numerous parliamentary initiatives, a high profile Commission of Experts on cybercrime was set up.[198] The latter was mandated with further studying the competency question, namely the issue of cantonal versus confederation powers in relation to criminal investigative procedures. In its final conclusions, the Commission sided with the earlier Watermann initiative in calling for a federalisation of cybercrime.[199] The aim was to make cybercrime a federal competence, as was already the case for 'organised crime'. While the Commission had been deliberating over possible policy solutions a major international event was to highlight the difficulties and inefficiencies of the highly fragmented Swiss penal system.

In the summer of 2002, the biggest international child pornography investigation to date was launched, and it included the participation of Swiss law enforcement agencies. Known as Genesis, it involved the cantonal penal authorities in collaboration with the federal police force and was the subject of intense media attention. According to those who wanted to federalise cybercrime competencies, the Genesis operation revealed the inadequacy of the fragmented Swiss penal system. Within a month, and in a glaze of publicity, a policy entrepreneur had already tabled a new motion calling for a federalisation of investigative procedures for child pornography. Having had her earlier attempt to federalise the broader area of cybercrime rejected, Watermann now re-framed the challenge in terms of the evils of child

[197] For a discussion see Schwarzenegger, Christian (2002) Computer Crimes in Cyberspace, A comparative analysis of criminal law in Germany, Switzerland and Northern Europe, Jusletter available at http://www.weblaw.ch/jusletter/jsp?ArticleNr=1957

[198] See the Expert Commissions report, Rapport de la commission d'experts <Cybercriminalite>, Département fédéral de justice et police, Berne, Juin 2003.

[199] See pp 73-75 of the Expert Commissions report, Rapport de la commission d'experts <Cybercriminalite>, Département fédéral de justice et police, Berne, Juin 2003.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

pornography, and the accompanying need for federalisation.[200] In this sense, Genesis had a huge impact on public opinion in Switzerland and put the issue of child pornography issues firmly in the public spotlight. Moreover, it revealed the ongoing and very public disagreements about the assignment of prosecution competencies between the Confederation and the cantons that had occupied federal policymakers between 1998 and 2003.

Despite the public disagreements on federalising cybercrime, an Inter-Cantonal initiative had already managed to find an interim solution. On behalf of a call from the InterCantonal association of police chiefs in 2000, a Working Group (known as BEMIK) was established to examine the problems of cybercrime.[201] On the basis of its work, the federal department of justice and police, and the cantonal penal authorities came together the following year and set up a national Coordination Unit for Cybercrime Control (CYCOS) within the federal office of police. The problems in setting up this unit exemplify the Swiss cybercrime problematique.

In view of the serious institutional constraints for dealing with the cybercrime challenge –namely fragmented penal competencies- it would be necessary to develop other mechanisms. Thus, the Inter-Cantonal Working Group on cybercrime formulated a series of proposals, mainly centred on harmonising law enforcement techniques. However, it also recommended the creation of a 'cybercrime unit'.[202] The difficulty was in trying to set up a unit which did not infringe upon the investigative authority of the cantons, but at the same time reduced the inefficiencies resulting from information and investigative asymmetries among the 26 different authorities.[203] The result was the creation of a cybercrime coordination unit, CYCOS, which would deal with reports of internet crime, and act as a legal clearing house (i.e. check whether the subject matter was illegal or not and conduct nationwide analyses). By

[200] See the parliamentary initiative 02.452 Mise en place d'un service central en matiére de pédophilie sur internet.

[201] The association is known as Conference of Cantonal Police Commanders of Switzerland.

[202] For an overview see the website of the Swiss Coordination Unit for Cybercrime Control http://www.cybercrime.admin.ch/

[203] Interview with official at the the Swiss Coordination Unit for Cybercrime Control on 23/06/04 at Berne.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

delegating some of the costly manpower and specialised activities to the new unit, the cantons, and in particular those that are smaller and less well resourced, were able to free up resources while still maintaining their full investigative authority.

The federal cybercrime unit therefore has no investigative authority, this lies firmly with the Cantons who are the only ones that can investigate crimes on the internet. Thus, the cybercrime unit created no new federal competence while also serving to assist the cantons. It was an appropriate policy solution. By creating a coordination unit with a reporting mechanism (i.e. a hotline) for the public side, the inefficiencies of burdening the individual cantons with requests that require costly manpower resources to investigate could now be addressed by the unit. Essentially, the unit screens the information, e.g. whether it is Swiss related or not, and whether it is illegal or not. It is then passed to a legal clearing house, where lawyers try to establish on a case by case basis which Canton is actually concerned. The dossier is then sent to the relevant canton, which will screen the information and, most importantly, decide whether or not to initiate a prosecution. The system freed up resources that the smaller cantons would have had to divert to dealing with investigations, and provided them with clearing house which presents the cantonal authorities with the relevant files and, most crucially, allows them to claim credit for successful prosecutions.

What was perhaps most surprising about the creation of CYCOS was the tensions it generated among the cantons themselves. The biggest canton of all, Zurich, was in favour of a much bigger unit with effective investigative powers. It was hoping that the other cantons would agree. This did not materialise and Zurich therefore refused to participate in CYCOS. Furthermore, there was no way to compel it to participate.[204] The cybercrime problematique had revealed a thorny problem: many of the cantons feared that, with cybercrime on the rise, in the future most cases would end up becoming federal if cybercrime were federalised. This would spell the end of

[204] Zurich finally joined CYCOS in 2005.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the cantonal competence, and they would be left to investigate unglamorous petty crime. According to one expert it would mark 'the beginning of the end of local investigative crime fighting, and you would get an FBI instead of the current cantonal police'.[205]

Interestingly, the intercantonal association was not content to leave the federal cybercrime unit with all the publicity or credit for fighting child pornography. Thus, a year after CYCO was created, the Intercantonal police chiefs launched a high profile information campaign. The intercantonal information campaign was specifically directed against child pornography. Detailed information was made available from the cantonal websites which even included their own reporting mechanism.[206] The reporting mechanism, however, links directly to the federal level, the CYCO unit. Nevertheless, the whole procedure still leaves the impression that one is dealing with the cantonal authorities. This is not altogether too surprising since the federal unit would, in most cases, be much less familiar to most citizens than the cantonal equivalent.

The CYCOS bargain was only an interim solution however. The Genesis episode had revealed the fragmented nature of criminal investigations in Switzerland and brought the whole affair into the public limelight. Moreover, it served as a justification for re-visiting the competency question between the cantons and the confederation of the late 1990s. In this vein, another Working Group (known as the Genesis Working Group) was established in 2003, and it promptly drew attention to the cantonal limitations, especially in terms of the lack of human resources and expertise for dealing with cybercrime.[207] It was followed up by a formal consultation process that involved all the major

[205] Interview with official at the the Swiss Coordination Unit for Cybercrime Control on 23/06/04 at Berne.

[206] For more information about the initiative of the cantonal Police and Justice department representatives, see http://www.stop-pornographie-enfantine.ch/3/en/

[207] See especially the Genesis Working Groups's report of 12 novembre 2003, Modello per un perseguimento penale efficiente in casi di criminalità in rete su scala intercantonale
o internazionale, Proposte elaborate dal gruppo di lavoro istituito dalla Confederazione
e dai Cantoni per l'analisi dell'operazione 'Genesis', http://www.ejpd.admin.ch/etc/medialib/data/kriminalitaet/gesetzgebung/netzwerkriminalitaet.Par.0005.File.tmp/ber-genesis-i.pdf

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

actors.[208] For the time being, and as of 2005, no federalisation has occurred in relation to cybercrime investigation. Moreover, it is unlikely that cybercrime will be federalised. There are, however, significant pressures for granting the confederation a partial investigative role. Thus the debate is presently being framed in terms of the confederation playing a limited initial role where it is not clear which canton should take the lead. Once cantonal jurisdiction is established, it would then be passed to the relevant cantonal authorities.[209] Frustrated by the competency clashes, other groups have adopted alternative political strategies. The prominent child protection lobby, for instance, has resorted to using the institutions of direct democracy to try to achieve its policy goals. In 2004 it launched the first stage of a popular initiative -the collection of 100,000 signatures- to include a new provision against child abuse and child pornography in the Constitution.[210] The requisite signatures have been collected within the legal timeframe (18 months) and therefore a referendum is likely to be put to the people, although it still has to be approved by the Federal Council and the Parliament.

What is important to note is that the cybercrime agenda in Switzerland is being driven by the issue of child and hard pornography. It is the only issue that mobilises policymakers and is, therefore, the only route for selling cybercrime legislation. This is more difficult when the cybercrime challenge is framed in terms of hacking or internet fraud, all of which are politically much less salient. Thus, although a federal cybercrime unit has been created with responsibility for a whole series of cybercrimes, such as unlawful entry into IT systems, the spreading of computer viruses and the destruction of data, the

[208] See in particular the initiation of the consultation process and the Rapport à l'appui d'avant-projets de modification du code pénal suisse et du code pénal militaire concernant la responsabilité pénale des prestataires et les compétences de la Confédération relatives à la poursuite des infractions commises par le canal des médias électroniques (cybercriminalité), Berne, octobre 2004, available at http://www.ejpd.admin.ch/etc/medialib/data/kriminalitaet/gesetzgebung/netzwerkriminalitaet.Par.0014.File.tmp/vn-ber-f.pdf

[209] See the press release by the Dipartimento federale di giustizia e polizia, Comunicati 10.12.2004, Intensificare la lotta alla criminalità in rete, Il DFGP pone in consultazione due progetti di legge. Available at http://www.ejpd.admin.ch/ejpd/it/home/dokumentation/mi/2004/2004-12-10.html

[210] See article by Swissinfo, 1 mars, 2006, Dépôt d'une initiative contre la pédophilie, available at http://www.swissinfo.org/fre/a_la_une/detail/Depot_d_une_initiative_contre_la_pedophilie.html?siteSect=105&sid=6515492&cKey=1141638824000

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

fact is that its focus is only on hard pornography and child pornography.[211] This was a political decision and is the result of the power wielded by the cantons. The latter, as the principal paymaster (the cantons provide two-thirds of the finance for the cybercrime unit) were able to dictate what the unit should focus on.[212] Its *de facto* focus has therefore been on hard (mostly child) pornography given that this is the politically most salient issue and the one that the cantons are most concerned about.

The cybersecurity agenda has therefore been sidelined in favour of a more politically salient issue area –child pornography. This is not to say that there have been no developments in the area of cybercrime, which includes many cybersecurity issues. Although federalisation of cybercrime has failed, other mechanisms have been found. In the cybersecurity area a similar unit to CYCOS has been created at the federal level. The same competency constraints were faced and, as a result, an even weaker unit was created. The Federal Council had already acknowledged in its 1998 Information Society strategy the need for a cybersecurity plan for securing Switzerland's information infrastructure.[213] Switzerland's highest political body therefore set out to establish an interdepartmental working group to put forward proposals in order to address the issue.[214]

During the next half a decade the major outcome of the deliberations among the working groups and consultation processes was the establishment of two new federal agencies known as MELANI and SONIA.[215] The former is an analysis centre where risks and threats to the information society are studied.

[211] See the list of internet crimes on the Cybercrime Coordination Unit's website, at http://www.kobik.ch/e/index.htm

[212] Interview with official at the the Swiss Coordination Unit for Cybercrime Control on 23/06/04 at Berne.

[213] See the Strategy of the Federal Council for an Information Society in Switzerland, 18 February 1998, available at http://www.infosociety.ch/site/default.asp?dossiers=106

[214] For further information see the report by the L'Unité de stratégie informatique de la Confédération (2002) *Société de l'information vulnérable: Le défi de la sûreté de l'information.* Available at http://internet.isb.admin.ch/imperia/md/content/sicherheit/schutz-infrastruktur/information_assurance/pia_f.pdf

[215] For a detailed discussion by policymakers within the unit see Ruedi Rytz, Jürg Römer, Marc Henauer (2003) MELANI: An Analysis Centre for the Protection of Critical Infrastructure in the Information Age. Comprehensive Risk Analysis and Management Network (CRN) at the Swiss Federal Institute of Technology (ETH Zurich). Available at http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=300

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

MELANI, which is housed within the Department of Finance, is essentially an information exchange forum, where the public can also report cybersecurity problems and the private sector can exchange information with federal agencies.[216] Its major policy tool is informational, through its publications series and targeted information campaigns. It has no investigative powers. According to one source with regard to viruses and other types of computer crimes, for the time being the federal level is out of the picture since investigative competencies lie firmly with cantonal authorities.[217] It is possible to report such incidents to the federal cybercrime unit (CYCOS), but, as noted above, the cantons have ensured that its main focus is in the area of child pornography. Thus, there is no federal unit investigating computer crime – unless a demonstrable link can be made to 'organised crime' in order to activate the federal unit. On the other hand, with regard to critical information infrastructures, a Special Task Force on Information Assurance (SONIA) has been created. This operates at the highest political level and advises the Federal Council, as well as senior management representatives in the private and public sector, in the case of a crisis situation. However, unlike MELANI, it is not a permanent body and can only be convened for damage limitation in a crisis situation.[218] The cybersecurity agenda in Switzerland, especially in terms of critical infrastructure protection, is still at a relatively embryonic stage.

6. Comparative Review

In chapter 4, a crucial contextual backdrop to cybercrime policy in the three polities was identified. This was the Council of Europe Cybercrime Convention that was negotiated throughout much of the late 1990s and which came into force in 2004. Policymakers from all three polities (and in the EU case, its member states) were involved in the policy negotiations, with the US playing an especially active role. Thus, many of the policy actors were operating and interacting across these distinct policy arenas. Without ignoring or acknowledging that important interaction effects were at play, our focus has

[216] Detailed information on MELANI is available from its website: http://www.melani.admin.ch/
[217] Interview with official from MELANI 23/12/05.
[218] Dunn, M. and Wigert, I. (2004), International CIIP Handbook: An Inventory and Analysis of Protection Policies in Fourteen Countries. Swiss Federal Institute of Technology. Available at: http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

been on the explicit *within-polity* dynamics. To this end, we have been able to note that across the three federal systems, political actors at all level of public authority have been mobilised in response to the overall cybercrime challenge. In all cases, federal solutions have been proposed to address the challenge, triggering a series of vertical interactions among levels of government of varying intensities depending on the issue area. At the same time, private actors, such as civil liberties organisations or commercial organisations, have generally backed or opposed federalisation measures to the extent that such measures are congruent with their preferences. Civil liberties groups can mobilise in favour of regulation, as in the EU with anti-racist groups, or to promote the federalisation of competencies as in Switzerland in relation to child pornography, or in the US to attack federalisation attempts. From a comparative perspective, civil liberties groups have been markedly more active in the US case. Another set of important actors have been the network providers, all of whom have mobilised their political resources to try to avoid the real threat of government mandated regulation. Oftentimes, this has resulted in 'unholy alliances' between actors, such as civil liberties groups and network providers, although such coalitions can be abandoned depending on the particular issue at stake.

One notable difference in mobilisation across the cases has been in relation to some of the 'interventionist' regulatory strategies on the issue of liability of information intermediaries pursued by federal actors in both Switzerland and the US. In the US, federal measures were blocked by the courts whereas in Switzerland the Federal council preferred to adopt a wait and see approach, given developments in the neighbouring EU. In the EU, however, policymakers at the Commission adopted a 'liberal' policy strategy framed around the protecting the internal market. This was necessary to prevent the perceived dangers of unilateral member state regulation of information services. Interestingly, a similar dynamic to the EU initially occurred at the state-level in the US where the individual states attempted to legislatively enshrine their own policy measures for harmful content. In this case, it was the federal courts that intervened to prevent the proliferation of uncoordinated regulatory measures on interstate commerce clause grounds.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

6.1. Intensity of vertical interactions

Across all cases the politicisation of the cybercrime challenge, in its various dimensions, has triggered increased vertical interactions among levels of government within the three polities. This has activated a policy dynamic around the *politics of competence*. However, the intensity of the vertical interactions have varied somewhat. Generally, in the US these have been somewhat less pronounced. The debate usually centred on the *mode* of regulation rather than vertical issues of policy competencies. Thus, despite the US's dual layer of criminal legislation at both the federal and state level, all forms of cybercrimes have, in effect, been federalised. The disputes over the mode of regulation have been principally related to what have been perceived to be federal measures that are too restrictive. In the area of illegal and harmful content, federal measures have been successfully attacked by a coalition of civil liberties groups and industry groups. Here, policymaking has displayed a particular pattern whereby civil liberties groups and various other parties have tended to be excluded from the legislative drafting stage. These actors then pursue a legal strategy resulting in protracted policy battles that are played out in the court room.

It is important to note that there have also been important conflicts concerning state-level attempts at regulation. Thus far, however, federal jurisprudence has shown itself loathe to accept state regulation of the internet and, in several cases, has come close to asserting that the states simply are not constitutionally permitted to regulate the internet.[219] States are not only plagued by the first amendment constraint that blocked many of the federal measures that can at least, in theory, be overcome. They are faced with an additional hurdle, the commerce clause, which if the current federal jurisprudence holds, suggests that the states have very little scope for legislatively enshrining their own distinct measures related to internet content. In the area of computer crime and cybersecurity, some of the major tensions have been among federal agencies and the private sector, rather than levels of government. Having successfully passed federal cybercrime legislation, a

[219] See the *Dean* case on page 166.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

battle emerged among distinct federal agencies over policy responsibility. In the area of cybersecurity this has been resolved by essentially dividing powers among the DOJ and its agencies such as the FBI, and the newly created Department of Homeland Security. In this sense, the early attempts to 'securitze' cybersecurity according to a military logic failed. A distinct form of federalisation was pursued instead, which involved more cooperation with the private sector and an enhanced role for law enforcement.

In the EU, the intensity of vertical interactions among levels of government can be expected to be comparatively higher than in other cases, especially in those areas that touch upon sensitive issues of sovereignty related to internal security. To diminish competency clashes, EU policymakers employed an incremental approach that drew on a number of regulatory instruments, such as self-regulation, co-regulation and, finally legislative measures. One of the most controversial issues was in the area of illegal and harmful content where the danger of uncoordinated unilateral member state regulation emerged as a real threat to the internal market in the mid-1990s. The focus was initially on racist material, an area that has proven problematic to reach a consensus on given the divergences among some of the member states. Notwithstanding such difficulties, with the passing of the e-commerce directive, a policy bargain on the issue of liability for information intermediaries was achieved with direct implications for the area of racist internet content. However, the area of greatest policy activity has been the issue of online child pornography where a relative consensus among member states existed. Vertical interactions between the member states through the Council and DG JHA have culminated in a set of EU legislative measures that have harmonised EU member states' penal laws in relation to child pornography. In the area of cybersecurity, an incremental approach that has progressively become more legislative has also been pursued. Initially, EU policymakers pursued their security strategy through first pillar measures, in particular through the telecommunications and data protection regime. However, with the increased policy attention directed to 'organised crime' in the late 1990s, and terrorism after 9/11, the issue of cybersecurity took on a new meaning. Pushed by the member states, and increasingly driven by the Commission's DG JHA, a

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

series of legislative measures were implemented to approximate member states' criminal law. This culminated in a set of EU measures that have harmonised many aspects of cybercrime legislation across the member states.

In many respects, Switzerland is a rather straightforward case since penal law is a federal competence. But this only relates to substantive penal law such as defining what constitutes a crime and the corresponding criminal sanctions for violations. To this end, there have been relatively few problems in updating substantive prohibitions in the area of cybercrime, whether in relation to child pornography or computer crimes. The real policy battle has been with regard to attempts to federalise the procedural aspects related to cybercrime, and in particular the investigation of cybercrime. The procedural and investigative aspects of penal law are a competence of the sub-units. Thus when a number of policy entrepreneurs attempted to federalise this aspect of cybercrime, intensive competency clashes were generated among levels of government in Switzerland. Despite ongoing consultations on the question, the investigative aspects of cybercrime are unlikely to be federalised given that the majority of the cantons are unwilling to delegate competencies in this area to the confederation. To date, this has applied as much to the politically salient area of child pornography as it does to less salient issue of computer crimes.

6.2. Power capabilities of the centre

We can now focus on the power capabilities of the centre. Here there is significant variation between the three systems. In the US, federal agencies have been created or empowered in relation to all cybercrimes. In some cases, such as cybersecurity, this has led to a proliferation of agencies with different federal departments battling over lead responsibility. With the centralisation that resulted in the post-9/11 context, a notable consolidation has been achieved. This not only applies to cybersecurity however. The same has occurred within the FBI, which has centralised all its efforts to deal with cybercrime. Through units such as the IINI, the FBI has led the fight against child pornography by undertaking resource intensive investigative measures to track major producers and distributors of illegal content. Most recently, the

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

fight against illegal content has been expanded to include obscenity. Furthermore, a number of Presidential initiatives have since blurred the constitutional constraints between law enforcement and security. New laws have enhanced the investigatory powers of federal agencies through increased resources and large scale organisational restructuring. These have had the effect of consolidating the fragmented approach of the pre-9/11 policy context. Thus, a notable centralisation has occurred around two centres, the DHS for cybersecurity issues and the FBI's Cyber Division for all other areas of cybercrime. These federal agencies have real enforcement powers and can conduct investigations within the sub-units and assist them with their ongoing investigations. On the other hand, with regard to the private sector, federal policymakers have been more lax preferring to avoid government mandated regulation. Instead, the centre has offered industry a series of incentives through R+D programmes while empowering federal agencies with necessary enforcement powers.

When we turn our attention to the power capabilities of the centre in Switzerland and the EU, an entirely different regulatory picture emerges. In Switzerland, a competency clash among levels of government resulted in an organisational development, the Cybercrime unit. But, even here there was disagreement and the largest Canton, Zurich, initially opted out of the unit. The cybercrime unit initiative was launched by the sub-units and is largely controlled by the cantons who dictate what the unit's focus should be on. Given that the cantons' primary concern is with child and hard pornography, this has been the agency's focus. Despite the real inefficiencies with the current system, cantonal authorities have been unwilling to delegate any investigative powers to the federal level in the area of cybercrime. Furthermore, the confederation is prevented from endowing existing federal agencies with the necessary enforcement powers. The solution has been to create an agency that reduces the sub-unit's costs but leaves them with full autonomy. The same has occurred with the cybersecurity agency, its only powers are in the realm of information coordination and analysis. It cannot conduct investigations since computer crime investigations are a cantonal competence. In the area of critical infrastructure protection, however, a

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

special ad hoc group has been created to advise the Federal Council, although it is important to underline its non-permanent nature at this stage.

The Swiss case is not dissimilar to the scenario in the EU where the centre's power capabilities are similarly constrained. To this end, EU policymakers have focused on establishing a pan-European hotline using a number of instruments such as funding mechanisms and Council recommendations. Investigatory authority lies firmly with the member states however. A number of agencies have also been created such as the EU Cybercrime Forum that is housed at the Commission's Joint Reseach Centre (a full DG). However, it has no powers and limited resources and therefore amounts to nothing more than a useful website. A more promising development has been the creation of a Cybersecurity agency (ENISA). The latter is an EU independent agency that is responsible for cybersecurity issues and hopes to one day be able to carry out intrusion detection exercises and prevent network security incidents. For now, it will operate mainly as an information exchange unit carrying out analyses and assisting the member states. Furthermore, even these limited responsibilities were the subject of controversy in view of the UK's legal challenge about the agency's legal basis. In the area of critical infrastructure protection, developments are similarly at an embryonic stage and, although an EU policy is emerging in this area, it will be primarily based on extensive information coordination and intergovernmental in nature. The parallels with the Swiss agencies are especially noteworthy in terms of the nature and functional scope of the two agencies that were created.

It is possible to bring together the findings in the form of table 3 (see next page). It summarises a general pattern whereby similar vertical interactions are generated among levels of government, although in the US these have been comparatively lower. On the other hand, with regard to the power capabilities of the centre, from comparative perspective, both the Swiss and the EU form of federalism generate similar types of outcomes in which creating new agencies, or endowing existing agencies with new enforcement powers is severely constrained. In contrast, agencies have been created by the centre in the US that are not only endowed with enforcement powers but

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

can also intervene in the sub-units themselves. These options are simply not available in the EU and Swiss federal context.

Table 3: Cybercrime outcomes

	Intensity of vertical interactions	***Power capability of centre***
US	Med	High
CH	High	Low
EU	High	Low

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 8: Cross-polity comparative review

The aim of this chapter is to review the main findings of the empirical investigation from a comparative perspective. To this end, we begin by focusing on the policy context in each of the compound polities. This has impacted considerably on the outcomes that are described in section 2. From the outset we should note some of the basic theoretical assumptions that have guided the empirical investigation. Following Follesdal, we have distinguished between the centre and the sub-units (although one should also add the lower-level sub-units). The respective powers of each tier or level are determined by a constitution or, in the EU case, by a series of treaties that have the same effect. These constitutional texts reserve to the sub-units all residual powers that are not explicitly delegated to the centre. This is the same in all three cases. There is always scope, of course, for a degree of flexible interpretation but, crucially, the constitutional architecture, whether contained in a document called a constitution or a treaty, has imposed a series of constraints on potential shifts in authority to the centre. This has generated many of the constitutional conflicts that have been identified in the case studies and will be discussed below.

1. Comparative policy context

In order to frame the comparative review of findings, this section begins by highlighting similarities and differences in the cross-polity policy context. In particular, two policy areas have been at the core of the analysis: the regulation of commerce on the one hand, and 'internal security' measures, on the other. With regard to the former, from a comparative constitutional perspective one of the core powers delegated from the sub-units to the centre is the regulation of commerce. This has taken the form of allowing the centre to monitor how the sub-units apply their own rules in this area.[1] It is a delegated power that has been explicit right from the outset. That is to say,

[1] Coglianese, C. and Nicolaidis, K. (2001), Securing Subsidiarity: The Institutional Design of Federalism in the United States and Europe in Nicolaidis, K. and Howse, R. (eds.). *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*, Oxford: Oxford University Press.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

the foundational constitutional texts included specific provisions for the regulation of commerce, both among the sub-units themselves and their relations with foreign parties. Since cross-border markets do not arise spontaneously when territorial interests are strong, non-majoritiarian institutions such as regulators and/or courts have played a crucial role in the market creation process. Thus, the regulation of commerce, or the 'internal market' as it is referred to in the EU, can offer considerable scope for federalisation. To this end, and as the case studies have shown, there is a tendency to frame policy issues in terms of a 'commerce' or 'internal market' argument. This usually offers a legal basis and a policy route for federal actors to acquire authority over a given issue area. As demonstrated in the empirical chapters, this has been especially prominent in the EU and the US cases.

The other common feature of decentralised federal polities is that law enforcement powers and the operation of the criminal justice system have usually been reserved to the sub-units. This is not unrelated to the fact that law enforcement is a sensitive aspect of sovereignty and, therefore, during foundational constitutional moments these (residual) powers have usually been reserved to the sub-units. Neither the US constitution nor the Swiss Federal constitution of 1848, contained provisions which granted the federal level competencies in the field of criminal law. These have evolved over time and this has applied as much to the US and Switzerland during their formative development, as it does presently to the EU. Of course, over time, a creeping centralisation of powers using legal and political channels, such as constitutional amendments, court decisions or informal 'bypassing strategies' have been used to overcome some of the perceived inefficiencies generated from very decentralised set ups in the US and Switzerland[2].

We can start by focusing on the US where, through a deliberate constitutional design the criminal justice system operates on various levels, the federal, state and local. Historically, there has been a deeply engrained belief that

[2] On 'bypassing strategies' see Obinger, H, Leibfried, S. and Castles, F.G. (2005), Bypasses to a social Europe? Lessons from federal experience, *Journal of European Public Policy*, 12:3, pp.545-571.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

general law enforcement powers reside with the states and are administered locally.[3] Until recently, this has been upheld by a delineation of competencies which has placed fundamental restrictions on the expansion of federal law enforcement powers. However, this careful decentralisation of criminal law authority is being undermined by a wave of federalisation. According to the American Bar Association,[4] nearly half of all the federal criminal legislation enacted since 1865 have been passed since 1970. The reasons for this wave of federalisation are manifold but one significant factor is the perceived need, on the part of the federal authorities, to be seen to be addressing high profile criminal incidents and other social ills by passing federal legislation[5]. This has been an important contextual backdrop to many of the issues areas examined in the case studies. There is of course a rational self-interest to passing federal criminal legislation even though, in practice, only five per cent of prosecutions are federal.[6] As we have seen in the cases studies, it confers new powers on federal entities (prosecutors, administrative agencies, courts etc.) and to executive departments, such as the Department of Justice, which assume broad supervisory responsibilities over the new federalised crime, as well as extending the power of federal investigatory agencies such as the Federal Bureau of Investigation (FBI).[7] Despite the potential for variations given the dual level criminal justice system, the empirical investigation has shown that in those issue areas involving criminal legislation, the latter has been effectively federalised.

The operation of the criminal justice system in Switzerland has neatly illustrated the constraints of Switzerland's model of federalism. The Swiss constitution of 1848 left the responsibility for criminal legislation to the

[3] Stuntz, W.J. (2001), Terrorism, Federalism, and Police Misconduct, *Harvard Journal of Law and Public Policy* 25, pp 665-681.

[4] American Bar Association (1998), The Federalization of Criminal Law, Task Force on the Federalization of Criminal Law.

[5] Recent examples of controversial laws include the Brady Bill (a gun control bill), the Violence Against Women Act and the Gun Free School Zone Act, all of which bear testimony to federal lawmakers wanting to take credit for policy or passing new legislation that, in some cases, duplicates existing state law, see American Bar Association 1998; and Pickerel, M.J. and Clayton, C.W. (2004), The Rehnquist Court and the Political Dynamics of Federalism, *Perspectives on Politics* 2:2, pp 233-248.

[6] See Stuntz (2001).

[7] American Bar Association (1998).

DOI: 10.2870/1208

cantons. It was to take a further century, however, before a Swiss Penal Code came into effect. During this time various efforts to craft a federal penal code were attempted, most notably in 1898 when the revised Constitution of 1874 was amended to make criminal legislation a federal competence.[8] Only after half a century of preparatory work, including comparative studies on existing cantonal criminal legislation, various expert committees and a referendum vote passed by a narrow majority, did the Swiss Penal Code come into force in 1942. Although the substantive law aspects of what actually constitutes a crime were federalised, the same cannot be said for procedural law. This determines the procedures for investigating crimes and collecting evidence and was the competence of the 26 cantons.[9] This has generated significant variations among the cantons, a situation not entirely unrelated to the fact that the cantons drew inspiration from French, German/Austrian and Italian codes of criminal procedure.[10] However, with the second total revision of the Swiss Constitution in 1999, the federal level has been vested with new powers to harmonise procedural criminal law –to date this has not been accomplished, although draft proposals are being drawn up.[11] This rather unique constitutional set up, in which the centre (subject to the considerable constraints of the Swiss policy process) defines substantive criminal law while the sub-units enjoy more or less complete autonomy for the investigation and prosecution of crimes helps to explain another Swiss peculiarity –the absence until relatively recently of a national/federal police force endowed with investigative powers and, until 2004, the lack of a federal criminal court. Over the past decade the increasing internationalisation of crime has put a considerable strain on this extremely decentralised set up. In response the investigation of certain areas of criminal activity -namely organised crime- have been federalised. Nevertheless, although a federal police office has been created, its remit is strictly limited to investigating 'organised crime'. It is

[8] Trechsel, S. and Killias, M. (2004 a), 'Sources of Criminal Law' in Dessemontet, F. and Ansay, T. (eds.) *Introduction To Swiss Law*. Aspen Publishers.

[9] See Article 64-bis of the Swiss Constitution.

[10] See Trechsel, S. and Killias, M. (2004 b), 'Laws of Criminal Procedure' in Dessemontet, F. and Ansay, T. (eds.) *Introduction To Swiss Law*. Aspen Publishers.

[11] See Kalin, W. (2004), 'The Judicial System' in Klotti, Knoepfel, Kriesi, Linder, and Papadopoulos (2004) and Trechsel and Killias (2004a).

DOI: 10.2870/1208

against this specific contextual backdrop that the cybercrime issue became politicised.

Similar factors in terms of the constraints faced by the centre can be identified in the EU policy context. In the EU, the development of many internet-related policies have been framed in terms of a need to prevent distortions to the 'internal market'. In this respect, the 'internal market' justification has provided the intellectual (and legal) basis for many of the harmonisation measures examined in this investigation. Following the successful internal market legislative programme of the 1990s, a new push in the separate, but increasingly connected domain of justice and home affairs was launched by EU policymakers. To understand the EU's growing involvement in the area of internet criminality one has to take account of the major treaty modifications, all of which have had far reaching implications for the this policy area. During the 1990s, within the space of little over a decade the policy field of justice and home affairs, which did not even figure within the scope of the treaties and was characterised by limited intergovernmental cooperation, has advanced to the top of the political agenda.[12] One of the major turning points came with the Treaty of Amsterdam in 1997, which introduced new legal instruments, 'Decisions' and 'Framework Decisions'. This coincided with the explosion of the internet and, as we have seen for the EU case, the new legal instruments were put to effective use in all the policy areas examined. As a result, new mechanisms for approximating criminal laws and facilitating cooperation among member state justice systems were created and have been applied to all the issue areas studied. Furthermore, following the entry into force of the Amsterdam Treaty the small task force for justice and home affairs was expanded into a full Directorate General (DG) and has since become the driving force behind initiatives in the area of organised crime and cybercrime.[13] It is within the context of this new mobilising project in the area of 'internal security' that most of the policy measures under investigation have

[12] It was not until the Maastricht Treaty of 1991 that police and judicial cooperation was brought into the treaty structure. See in particular Monar, J. (2001), Justice and Home Affairs, *Journal of Common Market Studies* 39 Annual Review pp121-137; and Walker, N. (2003), 'The Pattern of Transnational Policing' in Neburn, T. (ed.) *A Handbook of Policing*, London: Willan Publishing.

[13] Interview with European Commission official at the Joint Research Centre 23/05/04.

DOI: 10.2870/1208

been framed. As we have seen, to a much greater extent than market regulation, the harmonisation of criminal laws and closer cooperation among law enforcement agencies touches on core aspects of EU member states' sovereignty.

2. Comparative review of empirical findings

In all cases and across all issue areas federal policymakers have mobilised to offer regulatory solutions to politically salient internet related issues. Part of the motivation may be attributed to a genuine desire to reduce the inefficiencies generated from capability and resource asymmetries among the sub-units. Another reason or justification for federalising solutions is to prevent possible distortions as a result of the sub-units adopting divergent responses to problems with spillover effects. One the consequences of increased federal activity is that the centre can expand the scope of its authority into new areas. If successful policies are pursued, the centre may even boost its support among the general public. The sub-units have been similarly trying to maximise popular support, and to this end have tried to retain as much control of the decision process as possible. Under conditions where the sub-units can prevent the migrations of authority to the centre, the former have tried to ensure that implementation and enforcement remains fully under their control. This has been shown to be particularly the case in Switzerland and the EU. On the other hand, private actors, such as interest associations and business organisations, have had varying policy preferences depending on the specifics of the issue area. As a general rule, they have clearly supported the level of government which best represents their particular interests.

Our focus can now be directed to the first of the two dimensions of the research inquiry. With regard to the strategic vertical interactions, attempts by the centre to offer federal solutions to internet criminality and internet governance problems in all three polities can clearly be identified. This has activated greater vertical interactions among the different levels of government. But these interactions have also varied in their intensities

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

depending on the issue area. This has been the case in relation to the copyright domain where the intensity of vertical interactions has been notably lower in the US, followed by Switzerland. By contrast, in the EU the intensity of vertical interaction around this issue area remained extraordinarily high. This is not unrelated to the fact that the EU is still in the process of trying to federalise its copyright regime, not a straightforward task given the diverging national traditions in this area. Nonetheless, vertical interactions also remained stubbornly high in the US until relatively recently, and in Switzerland the cantons blocked the creation of a federal agency for almost half a century. Thus, from a historical comparative perspective the EU is still at an early stage of federalising copyright. The EU direction is, however, rather clear. It is one that involves further federalisation of substantive legal norms and enforcement procedures at the EU level.

Swiss insights have been especially relevant for the EU in the area of cybercrime where considerable vertical interactions were generated among levels of government. Yet, in many respects, Switzerland should have been the most straightforward case concerning legal competencies given that penal laws are a federal competence. Thus, there is no need to harmonise prohibitions in this area, since they are regulated by federal legislation. A similar outcome, but using different legislative mechanisms has been achieved in the US. Despite the multi-layer criminal justice system in the US where substantive prohibitions can differ from state to state, the cybercrime domain has been effectively federalised. From comparative perspective, the EU is engaged in a similar process of harmonising penal legislation in the area of cybercrime which, in turn, generates vertical policy dynamics over legislative outputs. Legal competencies regarding data protection rules have also been effectively federalised in the EU and in Switzerland. However, the nature and the extent of federalisation has been politicised and this has tended to activate significant vertical policy dynamics among levels of government. With regard to certain aspects of data privacy a self-regulatory model has emerged in the US, rather than a comprehensive federal framework. But, in those areas that have been subject to federalisation, e.g. spam, surveillance and interception measures in cyberspace, there have been

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

very intense vertical policy interactions. In sum, as expected the intensity of vertical interactions among levels of government has generally been rather high, with the exception of copyright in the US.

Although there are certain similarities among the three units of analysis with regard to the vertical dimension, this is less so with regard to the specificity of the policy outputs. In all three polities, constitutional constraints imposed important limitations on the centralising mechanisms available to the centre. However, as we have seen, those constraints can be overcome more easily in certain policy contexts and given certain pre-conditions. This has been particularly the case in relation to the policy enforcement dimension. Here notable differences among the cases can be identified. With regard to data privacy, in both the EU and Switzerland multi-tiered regimes have been created in which the sub-units, or even lower units such as the Lander in Germany or city data protection commissioners in Switzerland, enjoy important enforcement powers. Delegating further authority to central/federal data protection authorities has therefore been a highly politicised issue, especially in Switzerland. A competing intercantonal agency to represent the sub-units was created in the Swiss case, and this can be compared to a similar intergovernmental agency that exists in the EU. Both federal level data protection offices have limited powers and tend to rely on the use of informational campaigns as an important policy tool. By contrast, in the US, the absence of a specific data protection authority means that conflicts are largely enforced by the courts and/or by federal agencies such as the FCC or the FTC.

With regard to copyright, litigation strategies have been pursued by private parties in all three units. For those private interests concerned, litigation in the copyright domain has been characterised by similar constraints in the EU and Switzerland. In both these cases, data protection rules and the need to deal with varying sub-unit investigative authorities, have posed greater difficulties for the decentralised enforcement strategies of private actors. Furthermore, no central body and/or investigative agency exist at the federal level to coordinate strategies in this domain. In the US, on the other hand, the

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

decentralised enforcement strategy has been pursued with a litigious zeal that is both more difficult to conduct and less appropriate for the EU and Swiss policy contexts. With regard to mechanisms for centralised enforcement, no such policy instruments exist in the EU or Switzerland. In the US, on the other hand, private actors not only rely on their own measures to police violations but have also been supported by federal actors. To this end, significant resources have been directed to creating federal agencies specialised in the investigation of copyright infringement, and these have achieved some notable successes over the last few years[14]. This dynamic can also be detected in the area of cybercrime (in relation to both computer crimes and investigation of distributors of illegal content). In both areas, the FBI's investigative powers, in terms of its capacity to monitor and analyse internet traffic, and its ability to use undercover investigative methods in the fight against child pornography, have been notably enhanced.

These policy options are simply *not* available in the EU or even in the Swiss context, where implementation and enforcement is carried out exclusively by the sub-units and where any attempts to centralise policing would be firmly resisted. In the Swiss case, the federal police force's remit is narrowly restricted to organised crime and cantonal competence over the investigation and prosecution of crimes dominates. Moreover, a strict delineation of competencies concerning cybercrime has imposed serious constraints on the federal level's ability to frame cybercrime as a national security issue. Therefore, the investigation and prosecution of cybercrime remains an exclusive cantonal competence. Under such conditions, the cantons have been careful to only delegate coordination functions to a central organisation (e.g. CYCOS).

This is not dissimilar to the EU, where there have been successful attempts at harmonising cybercrime related penal laws in combination with the development of new cooperation and monitoring mechanisms at the centre.

[14] The two main units are the Justice Department's, the Criminal Division's Computer Crime and Intellectual Property Section and the Computer Hacking and Intellectual Property. For statistics on the number of investigations see the 'Report of the Department of Justice's Task Force on Intellectual Property' US Department of Justice, Office of the Attorney General, October 2004.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

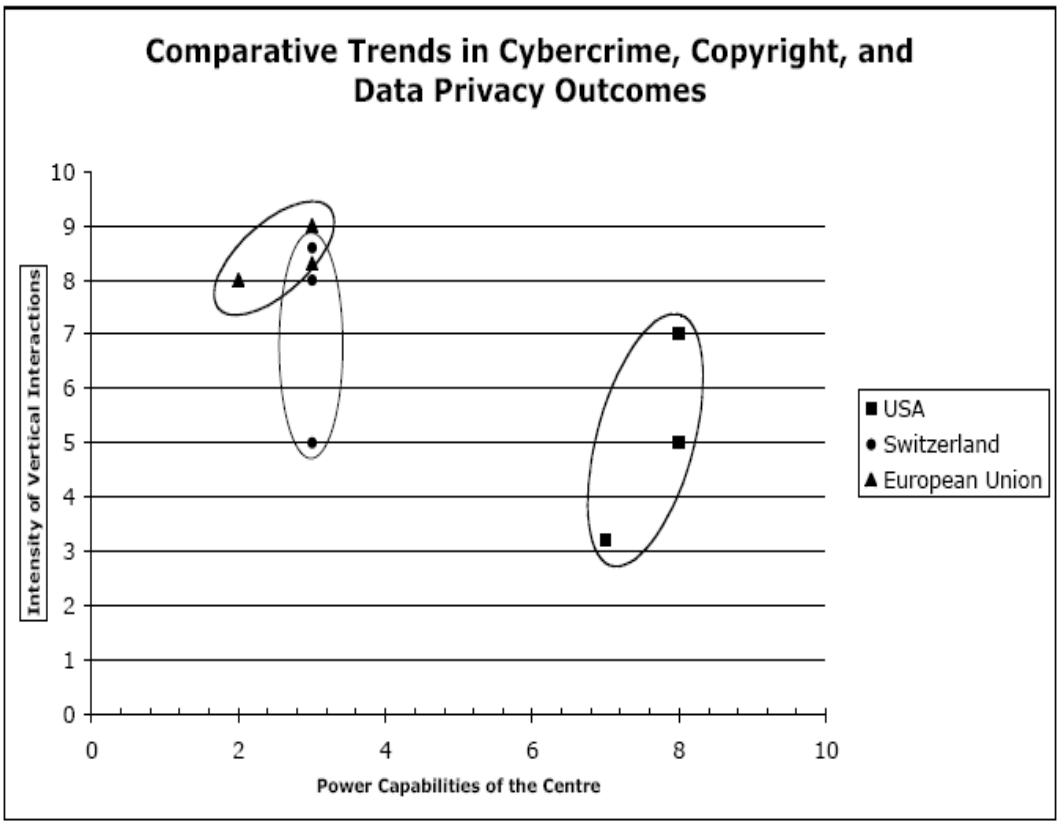
The creation of the new Network and Information Security Agency is an example. Yet the member states have been careful not to endow it with any regulatory or investigative powers, and its main function is to collect and analyse data with the aim of assisting the member states. The same holds for the network of EU funded European hotlines. Just as in the Swiss case, the investigation and prosecution is dominated by the sub-units. In general, where the power capabilities of the centre have been weak, and the latter has been dependent on the resources or the consent of the sub-units (as in Switzerland and the EU), the sub-units have preferred to only delegate coordination functions to the central level. Furthermore, where no federal level enforcement agency exists, such as in the area of copyright enforcement, there has been no process of agency creation. Where the power capabilities of the centre have been more significant (as in the US), the centre has been able to draw on its own resources and has not been constrained by the sub-units in pursuing its enforcement agenda. In this context, it has been easier to create new federal agencies with autonomous investigatory powers or to empower existing ones. The synoptic figure (see next page) summarises some of the major trends.

The scatter plot provides us with a visual representation of the two dimensions of this study (see Appendix for an explanation of the coding criteria).This is intended to serve as a simple heuristic device for displaying the two dimensions discussed above. The case studies have revealed that conflictual vertical interactions have been generated from a cross-polity comparative perspective, much as one would expect in federal polities. However, the case studies have allowed us to discriminate somewhat further and identify potential variance in the intensity of vertical policy dynamics. For instance, the policy domain of copyright has generated less intensive vertical interactions in the US. On the other hand, the horizontal axis conveys the differences in the power capabilities of the centre. These differ quite markedly. Overall, the Swiss and EU cases tend to cluster around the same area. One of the aims of the concluding chapter will be to examine this space that is populated by the Swiss and EU cases in more detail. Is it possible to identify a new category of ‘compound polity’ in this space with specific institutional and

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

regulatory features? Sketching out the contours of this new form of 'compound polity' is an exercise that will be left for the concluding chapter.

Figure 1



Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute
DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Part III Conclusions

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute
DOI: 10.2870/1208

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Chapter 9: The EU from comparative federalism perspective

This concluding chapter aims to situate the findings described in the empirical chapters, and the cross-polity comparative analysis, within a broader theoretical framework. First, it provides an overview of the insights yielded by adopting an explicit comparative federalism perspective to the EU and its policy dynamics. Second, it revisits the theoretical issues outlined in the preliminary chapters, especially chapters 2 and 3. In particular, the findings will be discussed in relation to the theoretical framework that has underpinned the approach pursued in dissertation. Third, and by way of conclusion, the final section offers some (tentative) conclusions and outlines the contours of a prospective research agenda based on a 'compound polity' understanding of the EU.

1. Comparative federalism as a lens for analysing EU policy

Chapter 8 has already provided an overview of the major findings of the in-depth cases studies from a cross-polity perspective which need not be revisited here. Instead, our attention in this section is chiefly directed towards understanding the EU and its policy dynamics from comparative perspective. The dissertation began by identifying a limited universe of so-called 'compound polities'. This, in turn, raised certain issues related to research design and the question of inclusion/exclusion of cases.[1] Rather than following the more popular EU/US comparative format, all known cases were included.[2] This was referred to as an *n*= 2 + EU type research design and was discussed at length in chapter 3. On the basis of further specification of similarities and differences, two important dimensions were identified for guiding the empirical investigation: the nature of strategic vertical interactions among levels of government, and horizontal

[1] See Ragin, C.; Berk-Schlosser, D.; and de Meur, G. (1996). 'Political methodology: Qualitative methods' in Goodin, R. and Klingemann, H. (eds.). A new handbook of political science. Oxford: Oxford University Press.

[2] See for instance Fabbrini, Sergio (2004). Transatlantic constitutionalism: Comparing the United States and the European Union. European Journal of Political Research 43:4, pp. 547-569.

DOI: 10.2870/1208

variations in the power capabilities of the centre, especially in terms of modes of policy implementation and enforcement.

The next stage was to apply this conceptualisation to a new policy field: the governance and regulation of the internet. This policy field however, should not be seen as constituting a single policy domain. This has been amply demonstrated in the detailed case studies. In fact, the focus has been on three very distinct (but overlapping) policies: data privacy, copyright, and internet criminality. Thus, by maximising variance in the policy fields studied we have been able to focus on issue areas involving a number of distinct policy logics or modes. This is, of course, most relevant to the EU case, although we have also been able to show that distinct policy modes also apply to the other cases, especially Switzerland. What has linked the distinct policy fields, however, is the internet or technology induced challenge. The internet's spectacular growth rates have made it a central and permanent feature of the economy and social life and this reality explains, in large part, the accompanying politicisation of the new medium (for an extended discussion see chapter 4). Because of this, the three issue areas investigated have been politically salient. Most importantly, they have all required authoritative political resolution by the state rather than market solutions. Thus, a series of negative externalities, many of which were framed in terms of the Rikerian[3] type of 'external threat' discussed in chapters 2 and 3, provided important incentives for mobilising political actors to seek centralising policies.

The main dimensions of the investigation could, of course, have been extended. As mentioned in chapter 4, the strategic interactions among the various levels of government identified need to incorporate crucial developments taking place at the international level that, in most instances, actually preceded domestic

[3] Riker's external threat hypothesis and its more recent modifications are discussed at length in chapters 2 and 3. See in particular Riker, William H. (1964a), *Federalism: Origins, Operation, Significance*. Boston: Little, Brown. For recent modifications see Filippov, M. (2005) Riker and Federalism, *Constitutional Political Economy*, 16, pp93-111; and McKay, D. (2004). William Riker on federalism: sometimes wrong but more right than anyone else? *Regional and Federal Studies*, 14: 2, pp.167-186.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

rulemaking.[4] This is certainly the case with regard to the cybercrime related activities that were being framed within the Council of Europe (where the US was also a signatory). And the same applies to the area of copyright through the internationally negotiated WIPO Internet Treaties of 1996. In this sense, important interaction effects between the three political systems have been produced. Policy actors not only had to take their domestic constituents' interests into account, but also had to keep a sharp eye on internal developments in other jurisdictions that could impact on their ability to regulate effectively within their own borders. This has been evident in all three cases with the EU's data protection regime, in particular, offering a notable example of extra-territorial effects. The greater the international spillover effects of the issue area, the more likely bargaining will also take place in an international institutional setting, via bilateral and/or multilateral negotiations. As we have seen, such negotiations can even precede domestic rulemaking. Such concerns have been beyond the scope of this dissertation and the substantive empirical focus has, instead, been on the activities of the centre and its interaction with the sub-units in the three compound polities.

Notwithstanding the above limitations, the claim advanced in this dissertation is that certain trends are clearly discernable and that, furthermore, EU policy dynamics can be profitably understood from a comparative perspective drawing on federal experiences. In many respects, the third pillar area of justice and home affairs has offered us a valuable laboratory for comparative research strategies.[5] In terms of lesson drawing, the emerging EU model comes closest to

[4] See Nicolaidis, K and Howse, R (eds.) (2001). *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

[5] It is perhaps worth noting in this context some of the proposed measures in the EU's most recent attempt at institutional reform, the recently rejected Constitutional treaty. The Constitutional treaty included a number of reforms to the decision-making process of the third pillar. In line with the theoretical propositions advanced throughout this dissertation, the EU would not have been granted new enforcement and/or investigative powers in the third pillar domain. These would have remained fully under the control of the sub-units. Instead, only substantive legal rules related to the third pillar, i.e. such as legislation on matters of criminal prohibitions and sanctions, would have profited from being handled in a less intergovernmental fashion. This would have certainly increased the possibilities for the further harmonisation of penal legislation in the EU.

the Swiss model. To this end, Swiss insights concerning the weak nature of federal investigative agencies and a propensity towards legal harmonisation at the centre with the sub-units controlling the implementation and enforcement process, could be especially relevant to the future trajectory of current EU policies in the newly emerging domain of police and judicial cooperation. In fact, some legal scholars have already directed their attention to the contours of the emerging EU penal code.[6] The argument advanced in this dissertation, however, does not in any way imply that an EU Penal Code will emerge *a la Suisse.* Instead, the focus has been on using theories of comparative federalism as a basis for advancing theoretical claims or hypotheses regarding the effects of different federal institutions in shaping political competition and influencing policy outcomes. To the extent that this has been achieved, it is argued that important insights can be yielded for the EU case by adopting a comparative perspective focused on similarities with present (as well as earlier) experiences in compound polities such as the US and Switzerland.

Of course, the sheer scale and complexity of the EU exercise, as well as the heterogeneity among the sub-units, make it the most daring experiment to date.[7] Yet this does not mean that the policy dynamics in areas such as internal security, where the centre faces considerable policy constraints, cannot be profitably compared to those experienced in other federal systems. It took over a century after the ratification of the US Constitution for a federal level law enforcement agency to emerge, a highly controversial decision at the time.[8] Even then, the US model of federalism has ensured a great variation among the sub-units, despite the growing federalisation of criminal laws.[9] In Switzerland, it also

[6] On an EU penal code see Storbeck, J. and Toussaint M. (2003), Outline of a Balanced and Effective Internal Security Strategy for the European Union, *European Journal of Crime, Criminal Law and Criminal Justice*, 12:1, pp 1-13.

[7] Walker (2003).

[8] Theoharis, A.G. (2000), 'A brief history of the FBI's role and powers' in Theoharis, A. G., Poveda, T G., Rosenfeld, S., and Powers, R.G. (eds.), *The FBI: A Comprehensive Reference Guide* Phoenix, Arizona; Oryx Press.

[9] Brenner, S.W. (2001), State Cybercrime Legislation in the United States of America: A survey, *Richmond Journal of Law and Technology* 2.

took a century after the foundational constitutional moment for a truly federal penal code to emerge and, although a federal police force has recently been created, its remit is strictly limited to 'organised crime' issues. Seen in this light, developments in the EU over the past two decades could be considered, from historical comparative perspective at least, as truly revolutionary.[10] For the foreseeable future, the EU will have to straddle a middle road between the dual nature of the criminal system in the US, and the pressures to harmonise substantive prohibitions that were experienced in Switzerland. One conclusion remains clear however. Although the EU may possess peculiar features, such as its highly intergovernmental third pillar structure, this should not preclude analysts from making theoretically grounded comparisons with other federal polities. On the contrary, as has been demonstrated throughout this dissertation, a comparative federalism perspective can illuminate even the most seemingly unique policy fields.[11]

2. The wider theoretical context

This section focuses on the broader theoretical context that has underpinned this dissertation's empirical focus. Using insights derived in large part from the rationalist inspired paradigm of comparative federalism, a conceptual model was developed for undertaking a structured and focused comparison of how lawmakers in the three federal polities have responded to a number of internet related policy challenges. In this regard, Rikerian insights have alerted us to the institutionally derived incentives for political actors, especially at the central level, to seek centralising solutions to policy issues with cross-border effects.[12] Where possible, and relevant, central level political elites tried to frame issue areas in terms of the need to address an 'external threat' that, in many cases, posed

[10] This is the argument made by Monar, Jorg (2001). Justice and Home Affairs. Journal of Common Market Studies 39 Annual Review pp121-137.See also Walker (2003). See also Walker, N. (2003) The Pattern of Transnational Policing. In *A Handbook of Policing*. Ed. Neburn, Tim ed. London: Willan Publishing.

[11] McKay, D. (2001), *Designing Europe: Comparative Lessons from the Federal Experience*. Oxford: Oxford University Press.

[12] McKay (2004).

DOI: 10.2870/1208

dangers to societal well being or the viability of the political and/or economic order. This was most evident in the case of data privacy and cybercrime issues across the three polities. But even in the case of copyright enforcement, the policy discourse has been framed in terms of threats to a polity's economic security from organised crime. This has been most evident in the EU case -not altogether too surprising given that the latter is still in the process of trying to federalise the copyright domain. More broadly, and as shown in the case studies, the external threat justification has been used by EU level policy elites across all issue areas investigated. But this dynamic has not been exclusive to the EU and it has been equally detected in all three polities. Riker's insights, and their modification by the latest wave of theorising in comparative federalism,[13] have therefore been especially relevant. Thus, the case studies have focused on the intense conflicts between central level and sub-unit political actors over the appropriate locus of political authority. In fact, throughout the empirical investigation Stepan's 'demos constraining' thesis about coming together type federal polities, which tend to be characterised by a fear of excessive centralisation, has been verified.[14] Indeed, such fears have been a notable feature of the political dynamic in the three compound polities. To the extent that centralisation of policy fields has occurred therefore, it has been the result of strong external pressures on sub-unit political elites. Even then, the sub-units have resisted centralisation efforts and delegated only coordination functions to the central level while retaining legal competencies. This was most evident in Switzerland and the EU where the strategic interactions concerning the allocation of policy competencies have been especially conflictual.

Drawing on the rationalist inspired federal theories, and their focus on the strategic interactions among distinct levels of government, two guiding hypotheses were formulated to structure the empirical investigation. With regard to the first hypothesis, the increasing politicisation of the internet, and the

[13] Fillipov (2005), McKay (2004)

[14] See chapter 3 for a more detailed discussion of the Stepan thesis. See Stepan A (1999). Federalism and democracy: Beyond the US style. *Journal of Democracy* 10, pp. 19-34.

DOI: 10.2870/1208

regulatory dilemmas that surround its governance, has provoked attempted allocational shifts in authority towards the centre level. Furthermore, central level political elites have tried to frame the policy challenge in terms of an external threat. This has generated typical centre-periphery conflicts over policy outputs. The process has been detected in all three units of analysis and, although the intensity of those interactions has varied, it has generally been of a highly conflictual nature. In sum, the *politics of allocating policy competencies* has been characterised by similar strategic interactions in the three polities.

With regard to the second guiding hypothesis, variations in the power capabilities of the centre have notably influenced the specificity of policy outputs. Thus, in Switzerland and the EU, the weak power capabilities of the centre help to explain why coordination and monitoring mechanisms have been developed to address thorny regulatory issues. As the empirical investigation has shown, the consensus decision-making styles and the decentralised modes of policy implementation and enforcement of the EU and Switzerland have tended to produce certain distinctive effects. Whereas the stronger power capabilities of the centre in the US made it easier for federal actors to create new enforcement agencies or considerably empower existing ones. Thus, although the *politics of allocating policy competencies* where characterised by similar dynamics, those related to the *politics of enforcement* clustered around two types. On the one hand, the more centralised US variant and, on the other, the more decentralised implementation and enforcement model of the Swiss and EU variant. The explanation for the variance in policy regimes is therefore rooted in the different structuring effects of federal political institutions in the two types of compound polities (see the theoretical discussion of chapter 3).

The framework adopted in this dissertation has therefore parted from a rather different theoretical standpoint to the covenantal theories discussed in chapter 2, which tend to focus on cooperative arrangements. The relations between levels of governmental have been shown to be anything but cooperative in the case

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

studies. Instead, the strategic interactions have been characterised by intense political conflict over the appropriate allocation of political resources. In line with the theoretical propositions of rationalist approaches, bargaining over the choice of alternative constitutional and institutional arrangements constituted one of the most fundamental conflicts. Thus, the focus of rationalist inspired federal theories is to identify how specific institutions shape political competition and create incentives for political actors to favour or reject federalising solutions. This has been the central empirical focus of the dissertation.

In a similar vein, the findings are relevant, and to a certain extent somewhat at odds, with some of the contemporary literature on EU policy modes. This is especially so with regard to Wallace's extension of the Lowi typology and her identification of two additional policy modes in the newer areas of active EU involvement.[15] The empirical investigation has certainly revealed that these so-called new policy modes have been used. In particular, the 'policy coordination' format of benchmarking and policy comparisons, as well as the 'intense transgovernmentalism' policy mode, which involves greater third pillar cooperation, are all mechanisms that were shown to have been put to effective use by EU policymakers. But this dissertation has demonstrated that a comparative federalism lens can also show us similar policy modes in other polities. Mechanisms of 'policy coordination', for instance, were also found in the Swiss case and the same applies to the EU's version of 'intense transgovernmentalism'.[16] While none of this necessarily detracts from the value of the Wallace typology, there is a danger in deploying ever new conceptualisations of distinct policy modes or identifying novel policy logics, especially when a comparative perspective could yield similar and more generalisable findings. The biggest danger is that, if uniqueness is overly

[15] See Wallace, H. (2005). 'An institutional anatomy and five policy modes' in Wallace, H, Wallace, W and Pollack, M. (Eds.), *Policy-Making in the European Union*. Oxford: Oxford University Press.

[16] The OMC type policy coordination that Wallace refers to has been practiced for decades in Switzerland, while a more appropriate term for 'intense transgovernmentalism' in the Swiss policy context would be 'intense trans-Cantonalism'.

DOI: 10.2870/1208

emphasised, an appreciation of the wider political science literature within which EU studies fits will tend to get de-emphasised.[17]

3. Conclusions: Towards a Consensus Compound Polity?

In this last section some tentative conclusions on the institutional contours of compound polities will be offered. Since this dissertation is mainly a study of the political dynamics surrounding three different issues areas great care must be taken in generalising from one policy field to others. Nonetheless, it is argued that the detailed case studies have revealed certain traits about the policy dynamics that are potentially common to other policy areas. Of course, it would have also been possible to look at other policy areas, such as those of a distributive nature, e.g. monetary policy, or those of a redistributive nature, such as welfare regimes, as well as the more regulatory type that has been the focus of this dissertation. Such a task has been beyond the scope of this dissertation, although it is possible to point to important insights revealed in these areas by some scholars of comparative federalism.[18] To this end, the focus has been on analysing an under-explored domain (mostly related to third pillar issues) from an explicit comparative perspective. Moreover, in selecting a policy field and, in particular the three distinct issue areas, the aim has been to maximise variance in terms of possible policy logics (for instance, first and third pillar domains in the EU case). This discussion brings us neatly to a critique of the Lowi policy modes approach. It centres on the argument that a policy typologies framework is too restrictive because issue areas within a specific policy field interact with one another, can operate with different policy logics, and thus cannot be neatly

[17] See in particular the critique by Moravcsik, A. on p. 170-1 of (1999), 'The Choice for Europe': Current Commentary and Future Research: A Response to James Caporaso, Fritz Scharpf, and Helen Wallace, *Journal of European Public Policy* (March), pp. 168-179, who argues that the 'detailed and open-ended policy analysis of the kind practised by Wallace…' would '….benefit greatly from more disciplined and focused social scientific debates among theoretically and methodologically replicable claims.'

[18] This is discussed more fully in chapter 2. On monetary and fiscal relations see McKay, D. (2005). Economic logic or political logic? Economic theory, federal theory, and the EMU. *Journal of European Public Policy* 12:3 (June), pp. 509-527. On social and welfare policies see Obinger, H. Leibfried, S. and Castles, F.G. (2005). Bypasses to a social Europe? Lessons from federal experience. *Journal of European Public Policy*, 12:3, pp.545-571.

compartmentalised into one of the three policy modes.[19] The typologies approach applied to the EU, therefore, suffer from similar weaknesses that plagued the original Lowi schema. In particular, the different policy types are not empirically separable in practice, but often overlap.[20] This has also been brought out in the empirical investigation where notable cross-pillar interaction effects were identified. Furthermore, different policy logics have applied to different stages of the policy-making cycle.[21] With these qualifications in place it is possible to proffer some tentative conclusions on a so-called 'compound polity' understanding of federal political institutions with a view to suggesting further possible research avenues for the EU case.

Two distinctions were made that were based, firstly, on similarities (and difference) with regard to certain *structural* factors mainly related to macro-institutional configurations and, secondly, in relation to the political and policy *process*. The *structural* and *process* distinction may have enabled us to capture crucial features of a 'compound polity' that have tended to be neglected in the recent literature.[22] Based on some of this dissertation's insights, a number of core features of the Swiss and EU compound polity variant can be distinguished.[23] These include some of the following features:

[19] See in particular the critique offered by Greenberg, George D., Jeffrey A. Miller, Lawrence B. Mohr, and Bruce C. Vladek (1977) Developing Public Policy Theory: Perspectives from Empirical Research. *American Political Science Review* 71:4. pp1532-1543.

[20] This point has recently resurfaced in Follesdal and Hix's recent critique of Majone's argument that the EU should specialise on regulatory politics. They question the centrality of Majone's policy mode distinctions 'when the empirical reality of decisions is a continuum between policies that are predominantly efficient and policies that are predominantly redistributive, with many mixes'. See Føllesdal, A. and Hix, S. (2006). Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik. *Journal of Common Market*, 31:2, pp. 153–70.

[21] This was in fact one of the main insights provided by Gary Marks in his account of multi-level governance in the Structural Funds. See Marks, G. (1996) 'Exploring and Explaining Variation in EU Cohesion Policy' in Hooghe, L. (ed.) *Cohesion Policy and European Integration: Building Multilevel Governance*, Oxford: Oxford University Press

[22] Much of this literature, discussed at length in chapter 3, is concerned with looking at how similarities in structural variables, such as the macro-institutional setting or constitutional architecture, produce analogous outcomes.

[23] This exercise should be seen as a purely heuristic device. For a graphical representation of these institutional features see Figure 1 chapter 8.

DOI: 10.2870/1208

1) Origins: A 'coming together' type federalism of *diverse* component units *not* imposed from above. Furthermore, the Swiss/EU models also tend to be characterised by a high degree of cultural, linguistic and ethnic heterogeneity, but with differences concentrated in specific territorial units rather than dispersed across the entire polity.[24]

2) Macro-Institutional features: The defining feature appears to be a multiple separation of power: vertically among more than *two* different territorial levels (e.g. a multi-tiered system) and horizontally divided central organs with a collegial type executive. Moreover, the tendency is towards 'semi-parliamentary' systems rather than presidential ones as in the US.

3) *Consensus Policy styles*: that are characterised by a non-majoritarian style of decision-making and a political culture that seeks to achieve far-reaching consensus through lengthy pre-consultation phases, and process of extensive negotiation and deliberation among all stakeholders. In addition, the process of interest intermediation gravitates towards a consociational rather than an overtly pluralist model.

4) An extremely decentralised *mode of policy implementation and enforcement* dominated by the sub-units which, in turn, significantly weakens the power capabilities of the centre. This is due to the latter's almost exclusive dependence on the sub-units for policy execution. This type of compound polity therefore tends to be characterised by the weak power capabilities of the centre.

This piecemeal attempt to sketch some basic institutional contours of what could be referred to as a 'consensus compound-polity' could be a starting point for further comparative research strategies especially in what, at first sight, appear to be seemingly unique policy fields. This type of approach stands in stark contrast

[24] See in particular Lijphart, A (1984) and (1999), *Patterns of democracy*. New Haven, CT: Yale University Press.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

to the *sui generis* approaches that have come to dominate much of EU studies and tend to encourage novel conceptualisations that are not rooted in the broader political science discipline. To the extent that the EU has features comparable to more mature political systems, we should be cautious of relying too much on *solipsistic* theories of the EU.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

References

Abromeit, Heidrun (2002). Contours of a European Federation, *Regional and Federal Studies*, 12:1 pp.1-20.

Akdeniz, Yaman (1999). The Regulation of Internet Content in Europe: Governmental Control vs. Self-Responsibility, *Swiss Political Science Review*, 5(2), pp.123-131.

_____ (2000). Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance ded Paris (The County Court of Paris), Interim Court Order, 20 November, *Electronic Business Law Reports*; 1(3), pp.110-120.

Allen, D. (2005). 'Cohesion and Structural Funds: Competing Pressures for Reform?'. In Wallace, H. Wallace, W. and Pollack, M. (eds.) *Policy-Making in the European Union, Fifth Edition.* Oxford: Oxford University Press.

Althouse, A. (2004). The Vigor of Anti-Commandeering Doctrine in Times of Terror, 69 *Brooklyn Law Review* 1231.

American Bar Association (1998). The Federalization of Criminal Law, Task Force on the Federalization of Criminal Law.

Anderson, J. (1996). The Shifting Stage of Politics: New Medieval and Postmodern Territorialities? *Environment and Planning: Society and Space* 14: 133-153.

Anderson, P. (1997). 'Under the Sign of Interim' in Gowan, P. and Anderson, P. (eds). *The Question of Europe*. London, Verso.

Auer, Andreas (2005a). Adoption, ratification and entry into force. *European Constitutional Law Review* 1: pp.131-135.

_____ (2005b). The constitutional scheme of federalism. *Journal of European Public Policy* 12:3 (June), 419-431.

Auer, A., Malinverni, G., and Hottelier, M. (2006). *Droit Constitutionnel Suisse, Volume II Les Droit Fundamentaux*, Stampfli Editions, Berne.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Bachtiger, A. and Steiner, J. (2004). 'Switzerland: territorial cleavage management as paragon and paradox' in Amoretti, Ugo M. and Bermeo, Nancy (eds.). *Federalism and Territorial Cleavages*. Baltimore: Johns Hopkins University Press.

Bar, Francios and Murase Emily. (1997). The potential for transatlantic cooperation in telecommunications service trade in Asia. *Berkeley Roundtable on the International Economy* (1997).

Baran, Jan and Wiley, Richard (1999). 'Politicking In Cyberspace' in Election Law Publications available at: http://www.wrf.com/publications/publication.asp?id=143479162000

Barbook, R and Cameron A. (1997). The Californian Ideology. *Science as Culture* 26. Part 1, pp. 44-72.

Barendt, E. (2005). *Freedom of Speech*, 2nd edition. Oxford: Oxfod University Press.

Barnouw, Erik (1966). *A History of Broadcasting in the United States: A Tower in Babel: Vol 1 A Tower in Babel*. New York: Oxford University Press.

Bartolini, S. (2005). *Restructuring Europe*. Oxford, Oxford University Press.

Baxter W. P. (2003). Has Spam been Canned? Consumers, Marketers, and the Making of the CAN-SPAM Act of 2003, *NYU Journal of Legislation and Public Policy*, 8:1 pp 163 at 166.

Baylis, T.A. (1989). *Governing By Committee*. New York: State University of New York Press.

Bednar, Jenna (2004). Authority migration in federations: A framework for analysis. *PS: Political Science and Politics* 37, 403-408.

Beer, Samuel (1993). *To Make a Nation: The Rediscovery of American Federalism.* Cambridge, MA: Belknap Press of Harvard University Press.

Bell, Tom W. (2001). Internet Privacy and Self-Regulation: Lessons from the Porn Wars. Cato Institute Briefing Papers.

Bendrath, Ralf (2001). Cyberwar debate: Perception and politics in US critical infrastructure protection. *Information and Security*. 77, pp. 80–103

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Benkler, Yochai (2000). Internet Regulation: A Case Study in the Problem of Unilateralism. *European Journal of International Law* 11(1):171-185.

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

Bennett, Colin and Raab, Charles (2003) *The Governance of Privacy: Policy Instruments in Global Perspective*. London: Ashgate.

Bermann, George A Nicolaidis, Kalypso (2001). Basic Principles for the Allocation of Competence in the United States and the European Union in K Nicolaidis, and R Howse, ed *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

Bernauer, Thomas and Caduff, Ladina (2004). In whose interest? Pressure group politics, economic competition, and environmental regulation. *Journal of Public Policy* 24, 99-126.

Berners-Lee, T. (1996). The World Wide Web: Past, Present and Future, available at: http://www.w3.org/People/Berners-Lee/1996/ppf.html

von Beyme, K. (2005). Asymmetric Federalism between globalization and regionalization. *Journal of European Public Policy* 12:3, pp. 432-447.

Birnhack, M. and Elkin-Koren, N. (2003). The Invisible Handshake: The reemergence of the State in the digital environment. *Virginia Journal of Law and Technology* 8:6.

Blondel, J. (1998). Il Modello svizzero: un futuro per l'Europa?. *Rivista Italiana di Scienza Politica* n. 2, pp. 203-227.

Börzel, Tanja (2003). Shaping and Taking EU Policies: Member State Responses to Europeanization. Queens Papers on Europeanization, No. 2, Queens University, Belfast.

Börzel, Tanja and Hosli, Madeleine (2003). Brussels between Bern and Berlin: Comparative federalism meets the European Union, *Governance* 16:2, pp. 179-202.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Börzel, T. and Risse T. (2000). When Europe Hits Home: Europeanization and Domestic Change. EUI Working Paper No. 2000/56, European University Institute, Florence.

Boyle, J (2000). The First Amendment and Cyberspace: The Clinton Years *Law and Contemporary Problems* 63, pp 337.

Bratton, William Wilson and McCahery, Joseph A. (2000). Fiscal Federalism, Jurisdictional Competition and Tax Coordination: Translating Theory to Policy in the European Union (January 17). George Washington University Law School, Public Law and Legal Theory Working Paper No. 006

Braun, D. (ed) (2000). *Federalism and Public Policy*, Aldershot: Ashgate.

Brenner, Susan W. (2001). State Cybercrime Legislation in the United States of America: A survey. *Richmond Journal of Law and Technology* 2.

_____ (2004). US Cybercrime Law: Defining Offences, *Information Systems Frontiers* 6:2 pp115-132.

Brickey, Kathleen (1996). The commerce Clause and Federalized Crime: A tale of two thieves, 543 *Annals of American Academy Political and Social Science* 27.

Buchanan, James (1995). Federalism as an ideal political order and an objective for constitutional reform. *Publius* 25:2 (Spring), pp. 19-27.

Buchanan, James M. and Faith, Roger L. (1987). "Secessions and the Limits of Taxation: Toward a Theory of Internal Exit. *American Economic Review* 78: 1023-31.

Bulmer, S. (1983). Domestic politics and EC policy-making. *Journal of Common Market Studies* 21:4, pp. 261-280.

Bulmer, S. and Burch, M. (2000). 'The "Europeanization" of Central Government: the UK and Germany in Historical Institutionalist Perspective' in Aspinwall, M. and Schneider, J. (eds.) *The Rules of Integration*, Manchester: Manchester University Press.

Bulmer, S. and Lequesne, C. (2002). New Perspectives on EU-Member State Relationships. *Questions de Recherche,* Centre d'études et de recherches internationales Sciences Po, Paris.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Burgess, Michael (1986) (ed.) *Federalism and Federation in Western Europe*, Croom Helm, USA Cambridge: Belknap Press.

_____ (1989). *Federalism and European Union*. London: Routledge.

Burley, A.M. and Mattli, W. (1993). Europe before the court: A political theory of legal integration. *International Organization*, 47, pp.41-76.

Burrell R. and Coleman A. (2005). *Copyright Exceptions: The Digital Impact*, Cambridge University Press.

Cannon, Robert (1995). The legislative history of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway. *Federal Communications Law Journal*. 1996; 49(51).

Cappelletti, Mauro, Monica Seccombe and Joseph Weiler. (1986). *Integration through Law: Europe and the American Federal Experience*. New York: W. de Gruyter.

Caporaso, J. (1996). The European Union and Forms of State: Westphalian, Regulatory or Post-Modern? *Journal of Common Market Studies*, 34:1, pp. 29-52.

Caporaso, J. and Keeler, J (1995). 'The European Union and Regional Integration Theory' in Mazey, S. and Rhodes, C. (eds.) *The State of the European Union: Building a European Polity?* Boulder: Lynne Rienner, pp. 29-62.

Castells, Manuel (1996). *The Rise of the Network Society*. Oxford: Blackwell.

Cate, Fred and Litan, Robert (2002) Constitutional issues in information privacy. *Michigan Telecommunications and Technology Law Review* 9 (1) 35-63.

Chalmers, D. (2004). The Dynamics of Judicial Authority and the Constitutional Treaty, in Weiler and Eisgruber, eds., Altneuland: The EU Constitution in a Contextual Perspective, *Jean Monnet Working Paper* 5/04. Also available at: http://www.jeanmonnetprogram.org/papers/04/040501-14.html

Charlesworth, Andrew (2000). "Clash of the Data Titans? US and EU Data Privacy Regulation ." *European Public Law* 6 (2000), pp.253-74.

Chryssochou, D. (1994). Democracy and Symbiosis in the European Union. *West European Politics*, 17:4, pp.1-14.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Clarke, J. (2004). The United States, Europe, and Homeland Security: Seeing soft security concerns through a counterterrorist lens. *European Security*, 13, pp.117-138.

Coglianese, Cary and Nicolaidis, Kalypso (2001). Securing Subsidiarity: The Institutional Design of Federalism in the United States and Europe in Nicolaidis, K. and Howse, R. (eds.). *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union.* Oxford: Oxford University Press.

Cohen, Stephen; Delong, Bradford; and Zysman, John (2000). Tools for Thought: What is new about the 'E-conomy'. *Berkeley Roundtable on the International Economy* (Working Papers 138)

Corstens, G.J.M. (2003). Criminal Law in the First Pillar? *European Journal of Crime, Criminal Law and Criminal Justice*, 11/1 pp 131-144.

Costa, O. and Magnette, P.. (2003). The European Union as a Consociation? A Methodological. Assessment. *West European Politics*, 26(3), pp.1-18.

Cowles, Maria Green (2001). *Who are the Rule-Makers of E-Commerce: The Case of the Global Business Dialogue on E-Commerce*. Washington DC: American Institute for Contemporary German Studies.

Crombez, Christophe (1996). Legislative procedures in the European Community. *British Journal of Political Science* 26, pp. 199-228.

Dahl, R. (1971). *Polyarchy: Participation and Opposition*. New Haven, CT: Yale University Press.

_____ (2001). *How Democratic is the American Constitution?* New Haven: Yale University Press.

Dahl, Robert and Tuft, E.R. (1973). *Size and Democracy*. Stanford, CA: Stanford University Press.

Dann, P. (2003). The European Parliament and Executive Federalism: Approaching a parliament in a semi-parliamentary democracy. *European Law Journal* 9:5 (December), p. 549-574.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Della Porta, D. and Mosca, L. (2005). Global-net for Global Movements? A Network of Networks for a Movement of Movements. *Journal of Public Policy*. 25 :1. pp165-190.

den Boer, Monica and Monar Jorg (2002). Keynote Article: 11 September and the Challenge of Global Terrorism to the EU as a Security Actor. *Journal of Common Market Studies*. 40 (Annual Review):11-28.

den Boer, Monica and Wallace, William (2000). Justice and Home Affairs in H. Wallace and W Wallace, *Policy-making in the European Union*. Oxford: Oxford University Press.

Diez T. and Wiener, A. (2004). *European Integration Theory*. Oxford: Oxford University Press.

Donahue John D, Pollack Mark A.(2001). Centralization and Its Discontents: The Rhythms of Federalism in the United States and the European Union in K Nicolaidis, and R Howse, ed *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

Dosi, Giovanni *et al (*eds.) (1988). *Technical Change and Economic Theory*. London: Pinter.

Douglas, J Susan (1987). *Inventing American Broadcasting 1899-1922*. Maryland: John Hopkins University Press.

Dunn, Myriam and Wigert, Isabelle (2004). *International CIIP Handbook: An Inventory and Analysis of Protection Policies in Fourteen Countries*. Swiss Federal Institute of Technology.

Dye, Thomas R. (1990). *American Federalism: Competition among governments*. Lexington, Mass: Lexington Books.

Eaglesham, Jean (2001). Yahoo! Bans Hate Propaganda. *Financial Times*, January 3: 12.

Easton, David (1957). An Approach to the Analysis of Political Systems. *World Politics*.; 9(3):383-400.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Eckstein, Harry (1975). 'Case Study and Theory in Political Science' in Greenstein, Fred and Nelson Polsby (eds.), *Handbook of Political Science vol. 7: Strategies of Inquiry.* Reading MA.: Addison -Wesley, pp. 79-137.

Eichengreen, Barry J. and von Hagen, Juergen, (1996). Fiscal Policy and Monetary Union: Is There a Tradeoff between Federalism and Budgetary Restrictions? (March). NBER Working Paper No. W5517. http://ssrn.com/abstract=4105.

Elazar, Daniel J. (1987). *Exploring Federalism*, Tuscaloosa: University of Alabama Press.

_____ (1991) *Federal systems of the world: A Handbook of federations, confederations and autonomy arrangement*, Longman Group UK Limited, London.

_____ (2001). 'The United States and the European Union: Models for Their Epochs' in Nicolaidis, K. and Howse, R. (eds.). *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

European Integration', *Public Administration* (Autumn 1988), pp.239–78.

Fabbrini, Sergio (2004). Transatlantic constitutionalism: Comparing the United States and the European Union. *European Journal of Political Research* 43:4, pp. 547-569.

Fabbrini, Sergio and Sicurelli, Daniela (2004). The Federalization of the EU, the US and Compound Republic Theory: The Convertion's Debate. *Regional and Federal Studies*, 14:2 pp.232-254.

Featherstone, K. and Radaelli, C. (2003). 'A Conversant Research Agenda'. In Featherstone, K. and Radaelli, C. (eds.) *The Politics of Europeanization* Oxford: Oxford University Press.

Filippov, Mikhail, Ordeshook, Peter C., and Shvetsova, Olga (2004). *Designing Federalism : A Theory of Self-Sustainable Federal Institutions*, : Cambridge: Cambridge University Press.

Filippov, M. (2005) Riker and Federalism, *Constitutional Political Economy*, 16, pp93-111

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Fitzgerald, Michael (2003). *Homeland Cybersecurity Efforts Doubted*, SecurityFocus, 2003-03-11.

Føllesdal, Andreas, (2003). "Federalism", The Stanford Encyclopedia of Philosophy (Winter 2003 Edition), Edward N. Zalta (ed.), URL http://plato.stanford.edu/archives/win2003/entries/federalism/

_____ (2005). Towards a stable *finalité* with federal features? The balancing acts of the Constitutional Treaty for Europe. *Journal of European Public Policy* 12:3 (June), pp. 572-589.

Føllesdal, A. and Hix, S. (2006). Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik. *Journal of Common Market*, 31:2, pp. 153–70.

Forsyth, M. (1981). *Unions of States: The Theory and Practice of Confederation*. Leicester: Leicester University Press.

Forsyth, Murray (1996). 'The Political Theory of Federalism: The Relevance of Classical Approaches' in Joachim Jens Hesse and Vincent Wright (eds), *Federalizing Europe: The Costs, Benefits and Preconditions of Federal Political Systems*. Oxford: Oxford University Press.

Franda, Marcus (2001). *Governing the Internet: The emergence of an international regime*. London: Lynne Rienner.

Garrett, Geoffrey and Tsebelis, George (1996). An institutional critique of intergovernmentalism. *International Organization* 50:2 (Spring), pp. 269-299.

Gellman, R. (1996). *Politics, Policy, and Technology: Perspectives on Proposals for Federal Health Confidentiality Legislation in the United States*, available at: http://www.privacyexchange.org/iss/confpro/bcfedhealth.html

George, Alexander L. and Bennett, Andrew (2005). *Case studies and theory development in the social sciences.* Cambridge, MA: MIT Press.

George, Stephen A. (2004). 'Multi-level Governance and the European Union', in: Ian Bache and Matthew Flinders (eds.) *Multi-Level Governance*. Oxford: Oxford University Press, pp. pp107-26.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Giacomello, Giampiero and Mendez, Fernando (2001). Cuius Regio, Euis Religio, Ominum Spatium?' State Sovereignty in the Age of the Internet. *Information and Security.* 7 pp15–27.

Gimore, Bill (2003). "Tin Towers and the Third Pillar: Some Security Agenda Developments." *EUI Working Papers* Law No 2003/7 (2003).

Ginsburg, J. (2002). How Copyright Got a Bad Name for Itself. *Columbia Journal of Law and Arts* 26: 61.

Goldsmith, Jack. (2000a). "Unilateral Regulation of the Internet: A Modest Defence." *European Journal of Internation Law* 11 (2000):135-48.

Goldsmith, Jack (2000b). Yahoo! Brought to Earth. *Financial Times*. November 27.

Goldsmith, J. and Sykes, A. (2001), The Internet and the Dormant Commerce Clause, *Yale Law Journal* 110 pp 786.

Goldstein, P. (1989). Copyright. Little Brown and Company 1989, 1st ed, Vol II.

Gorges, Michael (2001). "New Institutionalist Explanations for Institutional Change: A Note of Caution." *Politics* 21 (2001):137-45.

Cowles, M. G. (2001), *Who are the Rule-Makers of E-commerce: The case of the Global Business Dialogue on E-Commerce*. Washington DC: American Institute for Contemporary German Studies

Green, Joshua (2002). *The Myth of cyberterrorism*. The Washington Monthly Online.

Greenberg, George D., Miller, Jeffrey A., Mohr, Lawrence B., and Vladek, Bruce C. (1977). Developing Public Policy Theory: Perspectives from Empirical Research. *American Political Science Review* 71:4. pp 1532-1543.

Griffiths, Richard (2001). Internet for Historians, History of the Internet Course Outline. Available at: http://www.let.leidenuniv.nl/history/ivh/frame_theorie.html

Gross, G. M. (1996). Spinoza, and the Federal Polity. *Publius*. 26:1 pp117-135.

Guzzini, Stefano (1993). Structural Power: The Limits of Neorealist Power Analysis International Organization, 47: 3, pp. 443-478.

Haas, Peter M. (1992). Introduction: Epistemic Communities and International Policy Coordination. *International Organization*, 46:1 pp1-36.

Hafner, K. and Lyon, M. (1996). *Where wizards stay up late: The origins of the internet*. New York, NY: Simon & Schuster.

Halberstam, Daniel (2001). Comparative Federalism and the Issue of Commandeering in Nicolaidis, K. and Howse, R. (eds.). *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

Halbert, Deborah J. (1999). *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*. Quorum Books Westport, Connecticut.

Hall, Peter and Taylor, Rosemary C. R. (1996). Political Science and the three new institutionalisms. *Political Studies* XLIV (1996):936-57.

Hargreaves, Deborah (2001). EU and the space cowboys. *Financial Times* February 4.

Hauben, M. and Hauben, R. (1997). *Netcitizens: On the History and Impact of Usenet and the Internet.* California: Los Alamitos.

Heisenberg, Dorothee (2005). Negotiating Privacy: The European Union, the United States and Personal Data Protection. Boulder, CO: Lynne Rienner Publishers.

Herman, S. (2004). "Introduction", in Trager Symposium: Our New Federalism? National Authority and Local Autonomy in the War on Terror, 69 *Brooklyn Law Review* 1201, at 1214-1418 (2004).

_____ (2005). Collapsing Spheres: Joint Terrorism Task Forces, Federalism and the War on Terror, 41 *Williamette Law Review*, 941-949.

_____ (2006) The USA PATRIOT Act and the Submajoritarian Fourth Amendment, 41 Harvard Civil Rights – *Civil Liberties Law Review* 67, pp 71.

Hetcher, S. (2000). "The FTC as Internet Privacy Norm Entrepreneur", 53 *Vand. L. Rev* 2041.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Hix, Simon (1994). The study of the European Community: the challenge to comparative politics. *West European Politics* (1994).

_____ (1996). CP, IR and the EU! A rejoinder to Hurrell and Menon. *West European Politics,* Vol.19, No.4, pp802-4.

_____ (1998). The Study of the EU II: The 'new governance' agenda and its rival. *Journal of European Public Policy* 5:1, pp. 38-65.

_____ (2002). Why the EU should have a single president, and how she should be elected, LSE Working paper available at: http://personal.lse.ac.uk/HIX/Working_Papers/Why%20the%20EU%20Should%20Have%20a%20Single%20President.pdf

_____ (2005). *The Political System of the European Union*. Basingstoke, Hampshire: Palgrave MacMillan.

Hix, S. and Goetz, K. H. (2001). 'Introduction: European Integration and National Political Systems' in Hix, S. and Goetz, K.H. (eds.) *Europeanised Politics? European Integration and National Political Systems* London: Frank Cass.

Hobbes, Thomas (1968). *Leviathan*, edited by C.B. MacPherson. New York: Penguin Classics.

Hoffmann, S (1966). Obstinate or Obsolete?: The Fate of the Nation-State and the Case of Western Europe. *Daedalus* 95, pp. 892-908.

Hooghe, Liesbet. (ed.) (1996). Cohesion Policy and European Integration: Building Multilevel Governance. Oxford: Oxford University Press.

Hooghe, L. and Marks, G. (2001). Multilevel Governance and European Integration. Lanham/Oxford: Rowman & Littlefield.

Hoornbeek, J. (2004), Policy-making institutions and water policy outputs in the European Union and the United States: A comparative analysis, *Journal of European Public Policy* 11:3 (June), pp. 461-496.

Hug, S. (2002). *Voices of Europe. Citizens, Referendums and European Integration*. Lanham, Md: Rowman & Littlefield.

Hurrel A. and Menon A. (1996). Politics like any other? Comparative politics, International relations and the study of the EU. *West European Politics*, 19:2, pp386-402.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Hutter, Michael (2001). Efficiency, viability and the new rules of the Internet. *European Journal of Law and Economics* 11 (2001):5-22.

Hutter, Michael (2000). The Commercialization of the Internet. In *Understanding the Impact of Global Networks on Local, Social, Political and Cultural Values*. Ed. Engel, C and Keller K. Baden-Baden: Nomos.

Jachtenfuchs, M. (1997). Democracy and Governance in the European Union, in Follesdal, A. and Koslowskil, P. (eds.) (1997), *Democracy and the European Union*. Berlin: Springer, pp. 37-64.

Jachtenfuchs, P. (2001). The Governance Approach to European Integration. *Journal of Common Market Studies*, 39:2, pp245-264.

Joerges, C. and Neyer, J. (1997). From intergovernmental bargaining to deliberative political process: The constitutionalization of comitology. *European Law Journal*, 3, pp.273-299.

Jordan, A. (2001). The European Union: an evolving system of multi-level governance ... or government? *Policy & Politics*, 2, p.201.

Jordan, Tim. (2001). Language and Libertarianism: The politics of cyberculture and the culture of cyberpolitics. *Sociological Review*. 49 (1), pp1-17

Kahn , Robert and Cerf Vint (1999) What Is The Internet (And What Makes It Work) Available at: http://www.Internetpolicy.org/briefing/12_99.html

Kalin, Walter (2004). The Judicial System in U Klotti, P Knoepfel,.H Kriesi, W Linder, Y Papadopoulos (eds) *Handbook of Swiss Politics*. Zurich: Neue Zürcher Zeitung Publishing.

Katayal, Neal (2001). Criminal Law in Cyberspace, *University of Pennsylvania Law Review* Vol 149 pp1004-1112.

Katyal, S. (2004). Privacy vs. Piracy. *International Journal of Communications Law and Policy*. Special issue on Cybercrime, Issue 9, pp1-126.

Kelemen, Daniel (2002). Regulatory federalism: EU environmental regulation in comparative perspective. *Journal of Public Policy*; 20:3, pp.133-167.

_____ (2003). The Structure and Dynamics of EU Federalism, *Comparative Political Studies*, 36: 1/2 pp184-208.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

_____ (2004). *The Rules of Federalism*. Cambridge, MA: Harvard University Press.

Keman, M. (2000). 'Federalism and policy performance' in Wachendorfer-Schmidt, U. (ed.) *Federalism and Political Performance*. London: Routledge, pp. 196-227.

Kerr, Orin S. (2003). Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't. *Northwestern University Law Review*, Vol. 97. pp.607-664

Kies, R. and Kriesi, H. (2005). 'Internet voting and opinion formation: the potential impact of a pre-voting sphere' in Trechsel, A.H and Mendez, F. (eds.) *The European Union and E-Voting. Addressing the European Parliament's Internet Voting Challenge*. London: Routledge.

Kiessling, T. and Blondeel, Y. (1998). The EU regulatory framework in telecommunications: A critical analysis. *Telecommunications Policy* 22 (7) pp. 571-592.

Kincaid, John.(1993). From cooperation to coercion in American federalism: housing, fragmentation and preemption 1780–1992. *Journal of. Law Politics* 9pp 333–430

King, G, R Keohane, and S Verba. 1994. *Designing social inquiry: Scientific inference in qualitative research* . Princeton: Princeton University Press

Kissling-Näf, I. and Wälti, S. (2004). 'The implementation of public policies' in Klöti, U., Knoepfel, P., Kriesi, H., Linder, W., and Papadopoulos, Y. (eds). *Handbook of Swiss Politics*, Zurich: NZZ, pp. 563–600.

Kloti, U. (2001). Consensual government in a heterogeneous polity. *West European Politics* 24:2 pp.19-25.

Krasner Stephen (1982). Regimes and the Limits of Realism: Regimes as Autonomous Variables, *International Organization*, 36: 2, pp. 497-510.

_____. (1999). *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press.

Kriesi, H and Trechsel, A (forthcoming) Swiss politics. Continuity and Change in a Consensus-Democracy. Cambridge: Cambridge University Press.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Landau, Susan (2005). Security, Wiretapping, and the Internet. *IEEE Security and Privacy* 3, no. 6: 26-33.

Lane, Jan-Erik and Ersson, Svante (2000). *The new institutional politics: Performance and outcomes*. London: Routledge.

Lessig, Lawrence (1999). *Code and other laws of cyberspace* . New York: Basic Books.

Lessig, L. and Resnik P. (1999) Zoning speech on the Internet: A legal and technical model. *Michigan Law Review* 98:pp.395-431.

Lijphart, Arend (1984). *Democracies: Patterns of majoritarian and consensus government in twenty-one countries*. New Haven, CT: Yale University Press.

_____. (1999). *Patterns of democracy*. New Haven, CT: Yale University Press.

Linder, W. and Vatter, A. (2001), Institutions and outcomes of Swiss federalism: The role of cantons in Swiss politics, *West European Politics* 24:2 95-121.

Lindner, Brigette (2005). Demolishing copyright: The implementation of the WIPO Treaties in Switzerland. *European Intellectual Property Review*, 27(12), pp 481-488.

Litman, Jessica (2001). *Digital Copyright*. Prometheus Books.

Littoz-Monnet, Annabelle (2006). Copyright in the EU: droit d'auteur or right to copy? *Journal of European Public Policy* 13:3 pp.438-455.

Long, Willaim and Pang Quek, Marc (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbour compromise. *Journal of European Public Policy* 9:3, pp 325-344.

Lowi, Theodore J. (1964). American business, public policy, case-studies, and political theory. *World Politics* 16:4, pp. 677-715.

Mach, A., Hausermann, S., and Papadopoulos, Y (2003). Economic regulatory reforms in Switzerland: adjustment without European integration, or how rigidities become flexible. *Journal of European Public Policy* 10:2 pp.301–318.

Mair, Peter (1996). 'Comparative Politics: An Overview' in Goodin, Robert E. and Klingemann, Hans-Dieter (eds.) *A New Handbook of Political Science*. Oxford: Oxford University Press.

Majone, Giandomenico. (1994). The Rise of the Regulatory State in Europe. *West European Politics*, 17, pp.131-156.

_____ (2006). The common sense of European integration. *Journal of European Public Policy*. 13:5 pp607-626.

Mansell, Robert and Silverstone, Roger (eds.) (1996). *Communication by design. The Politics of Information and Communications Technologies* . Oxford: OUP.

Mansell, Robin and Steinmueller Edward. (2000). *Mobilizing the Information Society*. Oxford: Oxford University Press.

March, James G. and Olsen, Johann P. (1984). The new institutionalism: Organizational factors in political life. *American Political Science Review* 78, pp. 734-49.

Maria Green (2001). *Who are the Rule-Makers of E-commerce: The case of the Global Business Dialogue on E-Commerce*. Washington DC: American Institute for Contemporary German Studies.

Marks, G. (1993). 'Structural Policy and Multilevel Governance in the EC'. In Cafruny, A.W. and Rosenthal, G.G. (eds.) *The State of the European Community.* Boulder: Lynne Rienner.

_____ (1996). 'Exploring and Explaining Variation in EU Cohesion Policy' in Hooghe, L. (ed.) *Cohesion Policy and European Integration: Building Multilevel Governance.* Oxford: Oxford University Press.

Marks, G. Hooghe, L. and Blank, K. (1996). European Integration from the 1980s: State-Centric V. Multilevel Governance. *Journal of Common Market Studies*, 34:3, pp343-378.

Marks G; Nielsen, Francois; Ray, Leonard; and Salk, Jane (1996). 'Competencies, cracks and conflicts: Regional mobilisation in the European Union' *Comparative Political Studies*, Vol.29, No.2, pp. 164-192.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Mayer, Franz (2000). Europe and the Internet: The Old World and the New Medium. *European Journal of International Law*; 11(1):149-169.

Mayntz, Renate and Scharpf, Fritz W. (1975). *Policy-making in the German federal bureaucracy*. Amsterdam: Elsevier.

Mazumdar, Anandashankar (2003). EU Council Agrees to Move forward with proposals to harmonize computer crime laws. *Computer Technology Law Report* . Mar 21; 4(6).

McKay, David (1997) On the Origins of Political Unions: The European Case, *Journal of Theoretical Politics*, Vol. 9, No. 3, 279-296

_____ (1999). *Federalism and European Union: A Political Economy Perspective*. New York: Oxford University Press.

_____ (2000). Policy legitimacy and institutional design: Comparative lessons for the European Union. *Journal of Common Market* Studies 38:1, pp. 25-44.

_____ (2001). *Designing Europe: Comparative Lessons from the Federal Experience*.Oxford: Oxford University Press.

_____ (2004). William Riker on federalism: sometimes wrong but more right than anyone else? *Regional and Federal Studies*, 14: 2, pp.167-186.

_____ (2005). Economic logic or political logic? Economic theory, federal theory, and the EMU. *Journal of European Public Policy* 12:3 (June), pp. 509-527.

Mendez, F. and Trecshel, A.H. (2005). 'The European Union and e-voting: upgrading Euro-elections?' in Trechsel, A. and Mendez, F. (eds.) *The European Union and E-Voting. Addressing the European Parliament's Internet Voting Challenge*. London: Routledge.

Milner, H. (2002). The Global Spread of the Internet: The Role of International Diffusion and Domestic Political Institutions in Technology Adoption. Paper presented at conference on "Interdependence, Diffusion and Sovereignty," held at Yale University, May 10-11, 2002.

Monar, Jorg (2001). Justice and Home Affairs. *Journal of Common Market Studies* 39 Annual Review pp121-137.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Moravcsik, Andrew (1999). 'The Choice for Europe': Current Commentary and Future Research: A Response to James Caporaso, Fritz Scharpf, and Helen Wallace. *Journal of European Public Policy* (March), pp. 168-179.

Mota, S. (2002). 'The U.S. Supreme Court Addresses the Child Pornography Prevention Act and Child Online Protection Act in *Ashcroft v. Free Speech Coalition* and *Ashcroft v. American Civil Liberties Union*' (2002) 55 *Federal Communications Law Journal* 85, at 88.

Mueller, Milton (2000). Technology and Institutional Innovation: Internet Domain Names. *International Journal of Communications Law and Policy* (2000).

_____ (2002). *Ruling the Root. Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Negroponte, Nicholas (1995). *Being Digital*. New York: Knopf.

Nelson, Lisa (2004) Privacy and Technology: Reconsidering a crucial public policy debate in the post-September 11 era. Public Administration Review 64 (3) 259-269

Neustadt, R. (1991). *Presidential Power and the Modern Presidents*. New York: Free Press.

Nicolaidis, Kalypso and Howse, Robert (eds.) (2001). *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

Norberg, A. and O'Neil, J. (1996). *Transforming Computer Technology: Information processing for the Pentagon, 1962-1986*. John Hopkins University Press: Baltimore.

North, Douglass (1990). *Institutions, institutional change and economic performance*. Cambridge: Cambridge University Press.

Obinger, H. Leibfried, S. and Castles, F.G. (2005). Bypasses to a social Europe? Lessons from federal experience. *Journal of European Public Policy*, 12:3, pp.545-571.

Occhipinti, J D. (2003) *The Politics of EU Police Cooperation: Toward a European FBI?*, Boulder: Lynne Rienner.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Olsen, J.P. (2003). 'Europeanization' in: Cini, M. (ed) *European Union Politics*, Oxford: Oxford University Press.

O'Neil, M. (1996). *The politics of European integration: A reader*. London: Routledge.

O'Neil, M and Dempsey, J (1999). Critical Infrastructures Protection: Threats to Privacy and Other Civil Liberties and Concerns with Governments Mandates on Industry. *Depaul Busienss Law Journal*. 1999; 12:97.

Papadopoulos, Y. (2005). Implementing (and radicalizing) art. I-47.4 of the Constitution: is the addition of some (semi-)direct democracy to the nascent consociational European federation just Swiss folklore? *Journal of European Public Policy* 12(3): 448–467.

Pentland, C. (1973). *International Theory and European Integration*. New York: Free Press.

Peterson, J. (1995). Decision-making in the European Union: Towards a Framework for Analysis. *Journal of European Public Policy* 2:1, pp. 69-93.

Peterson, J. and O'Toole, P. (2001), 'Federal Governance in the United States and the European Union: A policy network perspective', in Nicolaidis, K. and Howse, R. (eds.) (2001). *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

Pickerill , Mitchell J. and Clayton, Cornell W. (2004) The Rehnquist Court and the Political Dynamics of Federalism, *Perspectives on Politics* 2: 2 pp 233-248.

Pierson, P. (1996). The Path to European Integration: A Historical Institutional Analysis. *Comparative Political Studies*, 29:2, p125.

Pierson, Paul and Skocpol, Theda (2002). 'Historical institutionalism in contemporary political science' in Katznelson, Ira and Milner, Helen V. (eds.). *Political Science: State of the Discipline*. American Political Science Association.

Pinder, John (1986). European Community and nation-state: a case for neo-federalism? *International Affairs*, Vol. 42:1, pp. 41-54.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

_____ (1993). 'The New European Federalism: The Idea and the Achievements' in M. Burgess and A.G. Gagnon (eds), *Comparative Federalism and Federation*. New York and London: Harvester Wheatsheaf.

Pollack, M. (1994). Creeping Competence: the Expanding Agenda of the European Community. *Journal of Public Policy*, 14(2), pp. 95-145.

Radaelli, C. (2000). Whither Europeanization? Concept Stretching and Substantive Change. European Integration Online Papers Vol. 4 No. 8.

_____ (2004). Europeanisation: Solution or problem? European Integration online Papers (EIoP) Vol. 8 , N° 16: http://eiop.or.at/eiop/texte/2004-016a.htm

Ragin, C.; Berk-Schlosser, D.; and de Meur, G. (1996). 'Political methodology: Qualitative methods' in Goodin, R. and Klingemann, H. (eds.). *A new handbook of political science*. Oxford: Oxford University Press.

Riker, William H. (1964a), *Federalism: Origins, Operation, Significance*. Boston: Little, Brown.

_____ (1964b). Some ambiguities in the notion of power. *American Political Science Review* 58:2, pp. 341-349.

_____ (1975). 'Federalism', in Fred I. Greenstein and Nelson Polsby (eds), *The Handbook of Political Science, Volume V*: Government Institutions and Processes. Reading, MA: Addison Wesley.

_____ (1993). Federalism in R Goodin and P Petit, eds, *A Companion to Contemporary Political Philosophy*. Oxford: Blackwell.

_____ (1996), 'European Federation: Lessons of Past Experience', in Joachim Jens Hesse and Vincent Wright (eds), *Federalizing Europe: The Costs, Benefits and Preconditions of Federal Political Systems*. Oxford: Oxford University Press.

Rhodes, M (1997) The Welfare State: Internal Challenges, External Constraints', in M. Rhodes, P.Heywood and V. Wright (eds.) *Developments in West European Politics*, Macmillan Press

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Risse, T. Cowles, M. and Caporaso, J. (2001). 'Europeanization and Domestic Change: Introduction' In Risse, T. Cowles, M. and Caporaso, J. (eds.) *Transforming Europe. Europeanization and Domestic Change* Ithaca: Cornell University Press.

Rohmer, Sandrine and Bloise, Joelle (2003). Le mp3 face au droit d'auteur du point de vue des utilistiers. *Pratique Juridiques Actuelle*, pp 51-57

Rosamond, B. (2000). *Theories of European Integration.* Basingstoke: Macmillan.

Rose, R. (2000). The end of consensus in Austria and Switzerland. *Journal of Democracy* 2: 2 pp.26-40.

Rosenau, James and Durfee Mary. 1995. *Thinking theory Thoroughly*. Boulder: Westerview Press .

Rosenzweig, Roy (1998). Wizards, Bureaucrats, Warriers and Hackers: Writing the history of the Internet. *American Historical Review* 103.

Rothstein, Bo (1996). Political institutions: An overview. In *A new handbook of political science*. Ed. Goodin, R and Klingemann H. Oxford: Oxford University Press.

Samuelson, P. (1997a). The Copyright Grab. *Wired*, Archive 4.01 - Jan 1996. Also available at URL: http://www.wired.com/wired/archive/4.06/romer_pr.html

_____ (1997b). The U.S. Digitial Agenda at WIPO, *Virginia Journal of International Law*, 37 at pp 369-431.

_____ (1999). Intellectual Property rights and the digital economy: Why the anti-circumvention regulations need to be revised. *Berkeley Technology and Law Journal* 14 (1999).

_____ (2002). Toward a 'New Deal' for copyright in the information age. *Michigan Law Review* 100, 1488-1505.

Sandholtz, Wayne (1999). Globalization and the evolution of rules. In *Globalization and Governance*. Ed. Prakash, Aseem and Hart Jeffrey eds. London: Routledge.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Shaffer, G. (2000). Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards, *Yale Journal of International Law*, Vol. 25, pp. 1-88.

Shapiro, M. (1997). The problems of independent agencies in the United States and the European Union. *Journal of European Public Policy*. 4:2 pp 276-291.

Sbragia, Alberta M. (1993) "The European Community: A Balancing Act" in: *Publius. The Journal of Federalism*, N. 23, Summer, pp. 23-38

Sbragia, Alberta M. (ed.) (1992). *Europolitics, Institutions and Policymaking in the New European Community*, The Booking Institutions, Washington D.C.

Scharpf, F.W. (1988). The joint-decision trap: Lessons from German federalism and European integration. *Public Administration* 66, pp. 239-278.

_____ (2001) European Governance: Common Concern vs the Challenge of Diversity. Jean Monet Working Papers. 2001(No. 6/01 Symposium: The Commission White Paper on Governance).

Schmidt, V (2001). 'Federalism and State Governance in the European Union and the United States: An Institutional Perspective' in K Nicolaidis, and R Howse, ed *The Federal Vision: Legitimacy and levels of governance in the United States and the European Union*. Oxford: Oxford University Press.

_____ (2006). Procedural democracy in the EU: the Europeanization of national and sectoral policy-making processes. *Journal of European Public Policy*, 13: 5, pp. 670-691.

Schmitter, Philippe and Kim, Sunhyuk (2005). The Experience of European Integration and the Potential for Northeast Asian Integration. *Asian Perspective* 29(2): 5-39.

Schwarzenegger, Christian (2002). Computer Crimes in Cyberspace, A comparative analysis of criminal law in Germany, Switzerland and Northern Europe, Jusletter available at www.weblaw.ch/jusletter/jsp?ArticleNr=1957

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Sciarini, P., Fischer, A., and Nicolet, S. (2004). How Europe hits home: evidence from the Swiss case. *Journal of European Public Policy*, Volume 11:3 pp. 353-378.

Serdült, Uwe (forthcoming). Drogenpolitik von unten: Drogenpolitische Massnahmen und Politiknetzwerke in Bern, Chur, St. Gallen und Zürich.

Sidjanski, D. (2000). *The federal future of Europe: From the European Community to the European Union*. Michigan: University of Michigan Press.

Sieber, Ulrich (1998). Legal Aspects of Computer-related Crime in the Information Society . COMCRIME Study.prepared for the European Commission. Available at: www.europa.eu.int/ISPO/legal/en/comcrime/sieber

Siebert, H. and Koop, M.J. (1993). Institutional competition versus centralization: Quo vadis Europe? *Oxford Review of Economic Policy* 9:15-30.

Sorkin, D. (2003). Spam Legislation in the United States, 22 *John Marshall Journal of Computer & Information. Law., 22*.

Speer, D (2000). Redefining Borders: The challenges of cybercrime, *Crime, Law & Social Change* 34: pp.259-273.

Spitz, D. and Hunter, S.D. (2005). Contested Codes: The social construction of Napster. *The Information Society*, 21: pp.169-180.

Stein, Eric (1981). Lawyers, Judges, and the Making of a Transnational Constitution. *American Journal of International Law* 75, p. 1-27.

Stepan Alfred (1999). Federalism and democracy: Beyond the US style. *Journal of Democracy* 10, pp. 19-34.

Storbeck, Jurgen and Toussaint, Mascia (2003). Outline of a Balanced and Effective Internal Security Strategy for the European Union, *European Journal of Crime, Criminal Law and Criminal Justice*, 12/1 pp 1-13.

Strate, Jacobson and Gibson (eds.) (2001). Communication and Cyberspace: Social Interaction in an Electronic Environment. 2nd ed. Hampton Press.

Stuntz, William J. (2001). Terrorism, Federalism, and Police Misconduct. *Harvard Journal of Law and Public Policy* Vol 25 pp 665-681.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Sutter, Gavin (2000). Nothing new under the sun: Old fears and new media. *International Journal of Law and Information Technology* 8(3).pp338-337

Taylor, Paul (1983). *The Limits of European Integration*. London and Canberra: Croom Helm.

Thatcher, M. (2001). The Commission and national governments as partners: EC regulatory expansion in telecommunications 1979–2000. *Journal of European Public Policy*, 8:4, pp. 558-584.

Theoharis, Athan G. (2000). A brief history of the FBI's role and powers in A G. Theoharis T G. Poveda, S Rosenfeld, R G Powers (eds) *The FBI: A Comprehensive Reference Guide* Phoenix, Arizona; Oryx Press.

Thierer, Adam D., Crews Jr., Clyde Wayne, and Pearson, Thomas (2002). Birth of a digital new deal. *CATO Policy Analysis* No 457.

Tiebout, C. (1956). A Pure Theory of Local Expenditure. *The Journal of Political Economy* 64, pp. 416-424.

Trechsel, A. H. (2005). How to federalize the European Union...And why bother. *Journal of European Public Policy* 12:3 (June), 401-418.

Trechsel, Alexander H (2004) Popular Votes in U Klotti, P Knoepfel,.H Kriesi, W Linder, Y Papadopoulos (eds) *Handbook of Swiss Politics*.Zurich: Neue Zurcher Zeitung Publishing

Trechsel, Stefan and Killias, Martin (2004 *a*) 'Sources of Criminal Law' in Dessemontet, F & Ansay, T (ed) *Introduction To Swiss Law*. Aspen Publishers.

Trechsel, Stefan and Killias, Martin (2004 *b*) 'Laws of Criminal Procedure' in F Dessemontet, & T Ansay, (ed) *Introduction To Swiss Law*. Aspen Publishers.

Tsebelis George (1994). The power of the European Parliament as a conditional agenda setter. *American Political Science Review* 88:1, pp. 128-142.

Tsebelis and Garret (2001). The Institutional Foundations Of Intergovernmentalism And Supranationalism in the European Union, *International Organization*, Vol:2, pp363.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Udekem-Gevers, Marie and Poullet Yves. (No date) "Concerns from a European user empowerment perspective in internet content regulation: An analysis of some recent statements." *ECLIP II*

Vogel, David. 2001. "Ships Passing in the Night: The changing politics of risk regulation in Europe and the United States." *EUI Working Papers, Robert Schuman Centre*.

Walker, Neil. 2003. The Pattern of Transnational Policing. In *A Handbook of Policing*. Ed. Neburn, Tim ed. London: Willan Publishing.

Wallace, H. Wallace, W. Webb, C., eds. (1977), Policy-making in the European Community, London: Wiley

Wallace, H. Wallace, W. and Pollack, M., eds. (2005) Policy-Making in the European Union, Fifth Edition. Oxford: Oxford University Press

Wallace, H. (2000). Europeanisation and Globalisation: Complimentary or Contradictory Trends? *New Political Economy*, 5:3,. 369-82.

Wallace, H. (2005). 'An institutional anatomy and five policy modes' in Wallace, H, Wallace, W and Pollack, M. (Eds.), *Policy-Making in the European Union*. Oxford: Oxford University Press.

Wallace, W. (1982). Europe as a confederation: The community and the nation-state. *Journal of Common Market Studies* 21, pp. 57-68.

Watts, Ronald L. (1988). *Executive Federalism: A Comparative Analysis*. Kingston, Ontario: Institute of Intergovernmental Relations, Queen's University Watts 1999.

Watts, R. (1998). Federalism, Federal Political Systems, and Federations, *Annual Review of Political Science*, Vol. 1, pp.117-137.

Webster, Frank. 1995. *Theories of the Information Society*. London: Routledge.

Weiler, J.H.H. (1982). Community member states and European integration: Is the law relevant. *Journal of Common Market Studies* 22:1/2, pp. 39-56.

Weingast, Barry R. (1995). The economic role of political institutions: Market-preserving federalism and economic growth. *Journal of Law, Economics, and Organization* 11, 1-31.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Werle, Raymond and Volker Schneider. 1999. "The Internet Society and its Struggle for Recognition and Influence." *MPIfG (Max Plank Institute for the studies of societies)* Working Paper 99/12 (1999).

Werle, Raymund. (2001). Internet @ Europe: Overcoming institutional fragmentation and policy failure. *European Integration online Papers* 5.

Wheare, K.C. (1967). *Federal Government (4th edition)*. London: Oxford University Press.

Zimmer, Eric A. and Hunter Christopher D. (2001). Risk and the Internet: Perception and Reality. In *Communication and Cyberspace: Social Interaction in an Electronic Environment*. Ed. Strate, Jacobson and Gibson Eds. Hampton Press.

Zimmerman, J.F. (2001). National-state relations: Cooperative federalism in the twentieth century. *Publius: The Journal of Federalism*, 31(2), pp.15-30.

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Appendix

The coding for Figure 1 in chapter 8 was based on the values in Tables 1, 2, and 3 included below. The following scores were attributed to the values (Low= 3; Medium= 6; High= 9) for measuring the two dimensions: 1) intensity of vertical interactions and 2) power capabilities of the centre.

Table 1: Data privacy outcomes

	Intensity of vertical interactions	***Power capability of centre***
US	High	High
CH	High	Low
EU	High	Low

Table 2: Copyright outcomes

	Intensity of vertical interactions	***Power capability of centre***
US	Low	High
CH	Medium	Low
EU	High	Low

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208

Table 3: Cybercrime outcomes

	Intensity of vertical interactions	***Power capability of centre***
US	Med	High
CH	High	Low
EU	High	Low

Mendez, Fernando (2007), The Governance and Regulation of the Internet in the European Union, the United States and Switzerland: A comparative federalism approach
European University Institute DOI: 10.2870/1208