2015-ENST-0056

EDITE ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

Télécom ParisTech

Spécialité “ sciences économiques ”

présentée et soutenue publiquement par

Winston MAXWELL

le 4 octobre 2016

A method to assess regulatory measures designed to limit access to harmful content on the Internet

Une méthode pour évaluer des mesures de régulation destinées à limiter l'accès à des contenus dommageables sur Internet

Directeur de thèse : **Marc BOURREAU**

Jury

M. Nicolas CURIEN, Professeur émérite, CNAM, membre du CSA	Président
M. Martin CAVE, Professeur, Imperial College, Londres	Rapporteur
M. Eric BROUSSEAU, Professeur, Université Paris Dauphine	Rapporteur
Mme. Maya BACACHE, Professeur, Télécom ParisTech	Membre du jury
M. Thierry PENARD, Professeur, Université Rennes 1	Membre du jury

T H È S E

Télécom ParisTech
école de l’Institut Mines Télécom – membre de ParisTech
46, rue Barrault – 75634 Paris Cedex 13 – Tél. + 33 (0)1 45 81 77 77 – www.telecom-paristech.fr

Un condensé de la thèse en langue française apparaît à la page 204

TABLE OF CONTENTS

		PAGE
CHAPTER 1 – MANAGING INTERNET RISKS		1
1.	Why most politicians and regulators will hate this thesis	1
2.	Bringing smart telecommunications regulation to the internet	3
3.	The challenges of regulating access to content on the Internet	4
4.	Current regulatory approaches are uncoordinated, with no guiding methodology	6
4.1	Right to be forgotten	6
4.2	Online copyright infringement	7
4.3	Illegal online gambling	8
4.4	Child pornography and terrorist propaganda	9
4.5	Hate speech	9
4.6	French audiovisual policy	10
4.7	Apparent lack of coherence	10
5.	Diminishing role of broadcasting regulation	12
6.	A methodology against which to measure regulatory proposals	12
6.1	Technical measures are inevitable	13
6.2	Technical measures create harmful side-effects	13
6.3	A reference methodology will help avoid mistakes	13
7.	Existing literature	14
8.	How the remaining chapters are divided	14
CHAPTER 2 - PRESENTING THE VARIABLES OF THE COST-BENEFIT EQUATION		19
1.	INTRODUCTION	19
2.	Content policies	21
2.1	Cybersecurity threats	21
2.2	Spam and phishing	22
2.3	Cookies and other form of tracking software	22
2.4	"Right to be forgotten" content	23
2.5	Illegal online gambling	24
2.6	Sale of cigarettes and alcohol	25
2.7	Counterfeit drugs, illegal drugs	25
2.8	Intellectual infringement	25
2.9	Defamation and the protection of privacy	26
2.10	Websites promoting racial, ethnic or religious hatred	27
2.11	Regulations designed to protect local culture and language	27

2.12 Advertising laws 28
2.13 Protection of minors against adult content 28
2.14 Child pornography 28
2.15 Content promoting terrorism 29
3. Assisting law enforcement 29
4. Valuing content policies and their enforcement 30
5. Internet intermediaries 31
5.1 Search engines 31
5.2 Hosting providers 32
5.3 Internet access providers 33
5.4 Internet domain name registrar 35
5.5 Payment service providers 36
5.6 Internet advertising networks 36
5.7 Application stores 37
5.8 Content delivery networks (CDNs) 37
5.9 Internet backbone providers 37
5.10 End-user software 38
5.11 Set-top boxes or modems 38
5.12 Device operating systems 39
6. The institutional framework 39
7. Negative externalities caused by Internet intermediary actions 40
7.1 Adverse effects on fundamental rights 41
7.2 Internet-specific harms 43
7.3 Unintended effects linked to user behavior 45
7.4 International effects 46
8. Solving the problem so as to maximizing social benefits 46
CHAPTER 3 - BALANCING FUNDAMENTAL RIGHTS 48
1. INTRODUCTION 48
2. What are fundamental rights? 48
2.1 Characteristics of fundamental rights 48
2.2 The cost of fundamental rights 50
2.3 Economic vs. non-economic rights 51
2.4 The expressive value of fundamental rights 51
3. Freedom of expression 53
3.1 General limitations to freedom of expression 53
3.2 Is the Internet like television? 53

3.3 The nature of harms to freedom of expression 54
3.4 Internet intermediary liability and free speech 56
3.5 The *Dennis* formula and its limits 57
3.6 Law and economics explanations for the high protection given to freedom of expression 60
3.7 Freedom of expression and self-regulatory measures 61
4. Privacy 62
4.1 Privacy and data protection as fundamental rights 62
4.2 Privacy rights in law and economics literature 63
4.3 Behavioral economics and privacy 66
4.4 Cost-benefit analysis applied to data protection 67
4.5 How to measure costs and benefits in privacy 72
5. Fundamental rights and proportionality 73
5.1 The three-criteria test of the European Court of Human Rights 74
5.2 Should a court give deference to lawmakers' balancing? 76
5.3 Identification of the conflicting rights and interests 77
5.4 Balancing the relevant interests 78
5.5 Absolute versus relative proportionality, cost-benefit analysis 79
5.6 Proportionality and the "least injurious means" test 81
5.7 Robert Alexy's balancing test 82
5.8 Nussbaum's ethical filter 84
5.9 Fundamental rights and the Hand formula 85
Chapter 4 - institutional alternatives for regulating access to Internet content 87
1. CATEGORIES OF INSTITUTIONAL OPTIONS 87
2. General liability or property rules enforced by the courts 87
2.1 Advantages and disadvantages of regulation by courts 88
2.2 Summary table 90
3. Administrative Regulation 91
3.1 Division of responsibilities between the lawmaker and the regulator 91
3.2 General versus detailed legislation 91
3.3 Regulatory authorities have better access to information and industry expertise 93
3.4 Risk of industry capture 93
3.5 Risk of regulatory creep 94
3.6 Territorial limitations to regulators' powers 94

3.7 Example of administrative regulation: the FTC's regulation of privacy 95
3.8 Summary table 96
4. Self Regulation 96
4.1 Self-regulation and the Internet 96
4.2 Self-regulation works well in groups with stable membership 97
4.3 Self-regulation works well where the self-regulatory organization (SRO) controls access to a scarce resource 98
4.4 The difference between unilateral self-regulation and multilateral self-regulation 98
4.5 Unilateral self-regulation by Internet platforms 98
4.6 Multilateral self-regulation and SROs 102
4.7 Conflicts of interest in SRO enforcement 102
4.8 Self-regulatory rules may not represent the public interest 102
4.9 Self-regulation and legislative threat 103
4.10 Example of multilateral self-regulation: the advertising industry 103
4.11 Summary table 106
5. Co-Regulation 107
5.1 The role of the state in co-regulation 107
5.2 Co-regulation and accountability 107
5.3 Preservation of public interest objectives 108
5.4 Enhanced legitimacy of the rules 108
5.5 Co-regulation in telecommunications regulation 109
5.6 Co-regulation in data privacy 109
5.7 Summary table 111
6. Brousseau's multilevel approach to governance 112
7. Internet requires a "racket and strings" regulatory approach 114
CHAPTER 5 – PRINCIPLES OF BETTER REGULATION APPLIED TO INTERNET 116
1. INTRODUCTION 116
2. LITERATURE ON BETTER REGULATION 116
2.1 Early scholarship: Breyer, Morrall, Hahn, and Sunstein 116
2.2 Dieter Helm examines the meaning of "good regulation" 117
3. OECD PRINCIPLES OF BETTER REGULATION 119
3.1 OECD 2012 Recommendation on Regulatory Policy 119
3.2 OECD 2011 recommendations on internet policy making 121
4. Better regulation methodology in the United States 122
4.1 Peer review by OIRA 122

4.2 Creating a baseline scenario 123
4.3 Identifying the relevant harm 123
4.4 Identifying regulatory options 124
4.5 Applying cost-benefit analysis to each alternative 125
4.6 How to quantify costs and benefits 126
4.7 Benefits and costs that are difficult to monetize 128
5. Better regulation methodology in Europe 129
5.1 European better regulation guidelines 129
5.2 European Commission guidelines assessing fundamental rights in impact assessments 129
5.3 2015 European toolbox for better regulation 131
5.4 The Renda study on cost-benefit analyses 134
5.5 Areas requiring further study 138
6. Impacts on innovation 138
6.1 Why Internet firms innovate 138
6.2 Knut Blind explains link between regulation and innovation 139
7. Adaptive or experimental regulation 141
8. Criticisms of cost-benefit analyses in regulatory decisions 142
8.1 Robert Baldwin asserts that impact assessments are ill-adapted to political realities 143
8.2 Radaelli and De Francesco compare U.S. and E.U. approaches 144
8.3 Robert Hahn and Paul Tetlock evaluate the costs of regulatory impact assessments in the U.S. 145
8.4 Ackerman and Heinzerling criticize CBAs that attempt to "price the priceless" 145
8.5 Greenstone: cost-benefit analyses require experimentation 147
9. Why conduct a cost-benefit analysis? 147
CHAPTER 6 – CREATING A METHODOLOGY FOR ASSESSING REGULATORY OPTIONS 149
1. BRINGING IT ALL TOGETHER 149
2. Elements of the methodology 151
3. The questionnaire 152
3.1 Analysis of the underlying content policy that needs to be enforced 152
3.2 The range of Internet intermediaries and actions they could take to help enforce the content policy, ranging from the least intrusive to the most intrusive 154
3.3 Remedies used in other countries 156

3.4 The institutional alternatives, including liability and property rules, self-regulation, co-regulation, and/or full-fledged administrative regulation 156
3.5 The fundamental rights affected by each proposed measure 157
3.6 Internet ecosystem 158
3.7 Behavorial economics and "nudges" 158
3.8 Adaptive and experimental regulation 158
4. A cost-benefit analysis under constraint 159
4.1 How to deal with hard-to-quantify benefits and costs? 159
4.2 Prepare a baseline scenario of no regulatory intervention, taking into account dynamic aspects such as possible evolutions of Internet technology and markets, and application of existing laws and self-regulatory policies 164
4.3 Measuring benefits compared to the baseline scenario 166
4.4 The direct costs resulting from each proposal, including direct costs for Internet intermediaries, their customers, and taxpayers 172
4.5 The indirect costs resulting from each proposal, including relative impacts on fundamental rights, on the internet ecosystem and innovation 173
4.6 How to rank proposals 177
4.7 Applying additional constraints 177
4.8 Conclusion on how to rank proposals 178
5. Public consultation 181
6. Institutional peer review 181
7. Periodic review of the measure 183
8. Conclusion 183
CHAPTER 7 – STRENGTHS AND WEAKNESSES OF THE PROPOSED METHODOLOGY AND AREAS OF FUTURE RESEARCH 185
1. STRENGTHS OF THE METHODOLOGY 185
2. Weaknesses of the methodology, and possible responses 186
3. Quantifying the unquantifiable 191

CHAPTER 1 – MANAGING INTERNET RISKS

1. WHY POLITICIANS AND REGULATORS WILL DISLIKE THIS THESIS

Politicians and regulators will dislike this thesis, because it proposes a system to dampen their enthusiasm to enact new regulation to deal with internet risks. Advocates of better regulation will like the thesis, as will advocates of net neutrality. The thesis addresses the question of how regulatory impact assessments should be conducted in the context of internet regulation, focusing in particular on cost-benefit analyses. What would a cost-benefit analysis look like for measures designed to protect citizens against harmful internet content? How can protection of fundamental rights and the internet "ecosystem" be integrated into a cost-benefit analysis?

Considerable science has been devoted to regulatory cost-benefit analyses, particularly in the context of environmental, health and safety regulations in the United States. The OECD and the European Commission have likewise endorsed thoughtful cost-benefit analyses as a precondition for any new regulatory measures. And yet cost-benefit analyses are rarely if ever done for laws regulating internet risks. Why focus on internet regulation? Like environmental risks, digital risks can trigger overreaction by policy makers eager to show that they are doing something about a problem created or amplified by new technology. The problems are generally real, but policy makers almost never analyse the problems and the scope of possible solutions with scientific rigor. Why should they? Politicians and regulators are generally rewarded for creating new laws and regulations, not for doing nothing. Yet a rigorous cost-benefit analysis may show that doing nothing is better than regulating. Regulatory over-reaction occurred in the United States in connection with certain health, safety and environmental risks in the 1970s and 1980s. A number of scholars highlighted the huge discrepancies in costs of many of these well-meaning regulatory measures. Some measures saved many lives at little cost; others saved few lives at astronomical cost. The purpose of the cost-benefit analysis is to highlight these differences, so that regulatory choices can be more explicit.

This thesis examines at the most common form of internet risk -- the risk of harmful content – and the most common form of internet regulation – regulations targeting internet intermediaries – and proposes a cost-benefit analysis for considering these risks and regulatory responses. The cost-benefit analysis is part of a broader impact assessment the purpose of which is to increase the quality of regulatory measures. The quality increase would occur at several levels. First, the impact assessment will decrease the likelihood of parliaments and regulators rushing into regulatory solutions that are ill-adapted to the fast-moving internet ecosystem. The impact assessment would reduce the frequency of these errors by imposing more rigorous fact-finding, a more thoughtful definition of the outcome that the measure hopes to achieve, and ways to measure success. The assessment would require a systematic consideration of costs, including indirect costs that are largely ignored in impact assessments today.

Second, the impact assessment will enhance regulatory quality by fostering competition and criticism between regulators and institutions. Systematic comparison and criticism based on a standard methodology would improve quality by permitting best practices to emerge. Today, measures are adopted in different "silos". The silos are based on country (*eg.* Italian measures versus French measures) or based on content policy (*eg.* copyright infringement policy versus right to be forgotten policy). One measure may be adopted to limit access to child pornography, another adopted for illegal gambling, and another yet for online copyright infringement with little or no coordination between the three approaches, and little debate on which approaches are most effective. The methodology would permit comparison and learning across different silos.

Third, impact assessments would increase quality by enhancing a measure's international legitimacy. If the methodology proposed in this thesis is recognized by international institutions such as the OECD and the European Commission, regulatory measures that emerge after a rigorous impact assessment would benefit from a favorable image internationally – a form of international quality label. The international quality label would signify that the country adopting the measure did its best to apply good regulation principles such as proportionality and respect for the internet ecosystem when adopting the measure. The impact assessment would presumably be available for public scrutiny, permitting international observers to verify that the methodology was applied correctly.

The proposed methodology will not yield a single good answer for any policy problem, but will permit regulators to rank alternatives based on their relative impacts on factors that are important in the context of internet policy making, including fundamental rights. The final decision on which regulatory option is best adapted to a given situation will in most cases remain political. The political decision may result in a choice that is not necessarily the optimal choice under the methodology. In that sense, the methodology is an input to the decision process rather than a decision rule of its own (Posner, 2000).

Nevertheless, my hope is that a standard methodological benchmark will lead to measures that are more consistent, more proportionate, and easier to understand for stakeholders, and that the methodology will avoid policy makers exaggerating internet-related risks and reinventing the wheel each time a new internet regulation is put forward. The methodology would also permit Europe to propose a standard that would justify regulatory intervention in certain cases, while permitting Europe to distinguish its approach from that of other less democratic countries that use internet intermediaries as tools for censorship. Interfering with internet content is a form of non-neutrality. Once regulators start down the road of internet non-neutrality, it can be hard to stop the movement. A uniform methodology would help define limits, and distinguish European measures from measures implemented in other less democratic countries. A methodology would contribute to defining what is meant by the "open internet."

The main difficulty we will encounter is attempting to integrate fundamental rights into the cost-benefit analysis. Many of the benefits flowing from a content policy (promotion of culture, protection of privacy or human dignity) are hard to quantify, let alone convert into monetary units. Many of the indirect costs of using internet intermediaries as proxies to enforce content policies will also be hard to quantify: limitations on freedom to access information, threats to privacy, harm to the internet ecosystem. But as we will see, there are ways of approaching the problem of quantifying these hard-to-quantify values.

2. BRINGING SMART TELECOMMUNICATIONS REGULATION TO THE INTERNET

Part of my career has been devoted to assisting telecom regulators in Europe justify the imposition of new regulatory measures on telecommunications operators. The task is difficult because the European directives on electronic communications impose a strict methodology that regulators must follow before they can propose new measures. Regulators must conduct a market analysis, identify one or more actors holding the dominant position, demonstrate that a market failure creates durable barriers to entry for competitors, that technological and market evolutions are not likely to cure the problem without regulatory intervention, and that competition law is not sufficient. Regulators must also show that the measure they propose is proportionate, causing the least intrusion possible while achieving the desired outcome. In some countries, regulators must present several alternatives and choose the one that is the least burdensome while still attaining the desired objective. The regulatory proposal must take into account the principles set forth in the Framework Directive[1] on electronic communications: encourage competition, investment, respect for technology neutrality. Regulators must submit the proposed solution to public consultation and then to a special task force at the European Commission, which has the power to request changes and in some cases veto the measure. Finally, the measure must be reevaluated regularly to make sure it is still fit for purpose. Regulations that are no longer needed must be withdrawn.

This methodology contrasts with the total lack of methodology for regulatory measures designed to limit access to content on the internet. Measures adopted to fight online copyright infringement, hate speech, child pornography, and privacy violations often involve internet intermediaries, including telecom operators. Yet those measures are adopted without the analytical rigor that applies to European telecommunications regulation or to health, safety and environmental regulation in the United States. The potential adverse effects of the proposed measures are not studied in detail. The impact assessments omit major considerations relating to effects on fundamental rights and adverse effects on the internet ecosystem. There is no peer review system, and no system to remove regulations that are no longer fit for purpose. If these measures were presented in a context of telecom regulation, many of them would fail the strict scrutiny imposed by the European directives.

---

[1] Directive 2002/21/EC

The study of telecommunications regulation and the literature surrounding cost-benefit analysis in the United States led me to the idea of this thesis. Would it be possible to take the analytical tools applicable to European telecommunication regulation and United States cost-benefit analyses and transpose those tools to the field of regulating access to internet content?

The question of limiting access to content is more complex than telecommunication regulation because the objectives pursued by policymakers include protection of fundamental rights, protection of children, and national security. The objectives of telecommunication regulation consist principally of achieving effective competition. The question of access to illegal content on the internet is also more complex because of the number of different internet intermediaries involved. In addition to telecom operators, search engines, app stores, social media, advertising networks, and payment providers may be called on to assist in enforcing a given content policy. However, the complexity of the problem is all the more reason to use analytical tools. The European methodology for telecommunication regulation is not perfect, but it requires regulators to ask key questions before they act: does this market failure really require a regulatory response, or is the market likely to deal with the problem on its own? Is the regulatory measure we propose the least intrusive among the available alternatives? What are the potential side effects of our proposed measure on competition, innovation and investment? These questions must be seriously analyzed in any proposed regulation of telecommunications in Europe. Cost-benefit analysis in United States regulatory policy requires that policy makers precisely define the desired outcome and develop tools to measure the outcome. In this thesis I will show that the same questions (and others) should be asked and analyzed in the context of regulations designed to limit access to harmful content on the internet.

3. THE CHALLENGES OF REGULATING ACCESS TO CONTENT ON THE INTERNET

Publishers of content and services on the internet are often located beyond the reach of national courts and police. Because the publishers are beyond reach, lawmakers and courts tend to look to internet intermediaries located within national borders as proxies to help apply content rules (Noam, 2006; Lichtman & Posner, 2004; Lescure, 2013). The internet intermediaries may be ISPs, payment providers, search engines, social media, app stores, domain name registries, browser publishers, or advertising networks (OECD, 2011).

To illustrate the difficulty facing regulators, let us use the example of hate speech: French law prohibits content that promotes racial hatred or anti-Semitism. In the United States, many forms of hate speech are protected by the First Amendment of the United States Constitution. Hate content that is published on a website based in the United States is instantly accessible by citizens of France. French victims of hate speech can bring an action before French courts and then try to obtain enforcement of the action in the United States. However, enforcement of a French judgment in the United States will be long and costly, and a United States court will not necessarily enforce a French decision that potentially interferes with United States constitutional

principles. Even if a United States court were to grant enforcement, the publisher of the content could easily move to another country and start its website again.

As this example shows, going after the source of the offending content is difficult and in some cases impossible. That leaves the option of seeking enforcement against technical intermediaries located in the country where the harm is caused. Take our example of the hate speech sites based in the United States. A number of options are available in order to make the hate speech sites less available to French citizens. Internet access providers in France could block access through various kinds of filtering. A search engine could make the site less visible on search results for French users. If the site collects payments from French users, payment providers could be called on to block payments. Browser software could be configured to make access to the site difficult. Advertising networks could be called on to block advertising. If the site uses a .fr domain name, the domain name could be seized in France.

All of these techniques can potentially be used to limit French citizens' access to an offshore hate speech site. However, all of these measures have potentially grave side effects. Technical filtering can block the targeted hate speech but can easily block other perfectly legal content. Filtering can create significant costs for internet intermediaries, can interfere with principles of net neutrality and threaten privacy. Moreover, many measures may prove ineffective, and/or encourage users to use encryption and dark networks to avoid detection, which creates other problems for law enforcement authorities.

National regulators may even be tempted to make their blocking measure apply to the entire world. In Europe, individuals have the right to request search engines to block certain harmful search results, even though the content revealed by the search is not illegal. Some European privacy regulators ask search engines to apply the blocking measure to search results worldwide, arguing that the victim is entitled to effective protection even if the search is conducted outside Europe. If applied to search results in the UNITED STATES, the blocking measure would block content protected by the First Amendment of the United States Constitution. The measure would also set a precedent for other governments who may want to silence dissent by asking a major search engine to apply global censorship. Like a potent medicine, measures taken by internet intermediaries, whether on their own or under government constraint, can have dangerous side effects.

The principles of the open internet and net neutrality prohibit interference with the free flow of content, applications and services on the internet. The open internet creates numerous economic and social benefits (OECD, 2016). Actions by internet intermediaries, whether government-imposed or voluntary, will necessarily affect the open internet. Interferences with the open internet are tolerated if they are part of "reasonable network management," that is, if the measure is intended to address a legitimate objective, and the means used to attain the objective are

proportionate (Sieradzki & Maxwell, 2008). Net neutrality so far applies only to ISPs, but its principles can in theory be extended to any kind of internet intermediary (ARCEP, 2012).

Net neutrality has at least three objectives: to prevent anti-competitive conduct by last-mile ISPs, to protect freedom of expression and to protect the borderless and end-to-end character of the internet (Curien & Maxwell, 2011). Measures that erect gateways designed to protect national content rules on the internet constitute a serious threat to the open, global character of the internet. Advocates of net neutrality also fear that if democratic countries begin to impose non-neutrality to achieve content objectives, other less democratic countries will follow suit, with measures to enforce political censorship or religious doctrine (OECD, 2011).

4. CURRENT REGULATORY APPROACHES ARE UNCOORDINATED, WITH NO GUIDING METHODOLOGY

Today many systems exist to enforce content rules on the internet, but they are developed on an ad hoc basis to deal with specific problems (Mann & Belzley, 2005).

Courts, regulators and lawmakers adopt different approaches for online copyright infringement, illegal gambling, hate speech, child pornography, right to be forgotten, and terrorism cases. There lacks a reference methodology against which to measure these initiatives.

To illustrate the point, below are examples of French measures adopted to address different content issues. These examples show the diversity of approaches used even within a single country.

4.1 Right to be forgotten

The right to be forgotten permits an individual to ask a search engine to remove certain search results that appear when someone conducts a search using the individual's name. The underlying content is not illegal. If it were, the individual could ask for removal of the content at its source, using legal claims such as defamation or invasion of privacy. In the case of the right to be forgotten, the original content (*eg*. a newspaper article) is legitimate, protected by law, and remains available on the internet. The individual simply wants the content to be less easy to find in search results because the content is old and harms the individual's current life.

The right to be forgotten flows from a court decision interpreting the broad provisions of the European Data Protection Directive 95/46/EC, and in particular the provisions that guaranty each individual a right to object to processing of his or her personal data.

For the so-called "right to be forgotten," the French data protection authority, the CNIL, has assumed the role of dispute resolution body in situations where claimants are not satisfied with the solution proposed by a search engine. In its dispute resolution capacity, the CNIL relies solely on the European Court of Justice's decision in Google France vs.

AEPD[2] (the "Costeja" decision). The CNIL applies the principles of the Costeja decision to France's Data Protection Act[3], and then issues an individual decision ordering the search engine to remove a certain search result from searches made using the individual's name. As indicated in the Costeja decision, the claimant's right to be forgotten request must be balanced against the public's right to have free access to information. If the relevant information is irrelevant, outdated and harmful to the individual, the CNIL would grant the request unless the public has a legitimate interest in having access to the information. This would be the case if the claimant were a public figure, for example. If the CNIL is satisfied that the balancing test comes out in favor of the claimant, the CNIL will order the search engine to remove the search results whenever an internet user conducts a search using the relevant individual's name. The CNIL's position is that the search engine should eliminate the search results from all searches worldwide, regardless of the country from which the search was initiated. The CNIL's decision therefore would have extraterritorial effect, limiting the information that would be seen by an internet user in the United States, for example. In rendering its orders, the CNIL currently does not take into account in its balancing test the fact that the search engine's action would likely impede access to content protected by the First Amendment of the United States Constitution. Similarly, the CNIL does not take into consideration in its balancing the precedential effect that a global order against the search engine could have for other countries who may also wish to apply their own content policies worldwide.

The current "right to be forgotten" only applies to search engines. Other internet intermediaries are not affected. The publisher of the original content, and the hosting provider, are under no obligation to remove the relevant content because the content itself is not illegal. The right to be forgotten is therefore unique in that the objective sought is not to remove or block access to the original content, but instead to make the original content more difficult to find using certain search terms and a certain kind of internet intermediary.

4.2 Online copyright infringement

France was the first country in the world to adopt a regulatory framework for fighting online copyright infringement using the so-called "graduated response" approach.

Under the HADOPI[4] graduated response regime, right holder organizations collect IP addresses of suspected infringers using peer-to-peer networks. The evidence is then transmitted to the HADOPI regulatory authority, who then asks the internet access providers to communicate the names of the subscribers corresponding to the IP

[2] CJEU Case n° C-131/12, Google Spain v. AEPD and Costeja, May 13, 2014.

[3] French Law N° 78-17 of January 6, 1978.

[4] Haute Autorité pour la diffusion des oeuvres et la protection de droits sur internet, created by Law N° 2009-669 of June 12, 2009.

addresses. According to HADOPI's activity report for 2013 – 2014, 12,265,004 identification requests were sent in total to the internet access providers. Once the HADOPI receives the names of the subscribers, HADOPI can take three steps. First, the HADOPI sends an initial e-mail to the relevant subscribers informing them of their duty to ensure that their internet access is not used for infringing purposes, and reminding the subscriber of the existence of legal online offers. According to its activity report for 2013 – 2014, the HADOPI has sent out 3,249,481 first warnings. Second, repeat infringers then receive a registered letter from the HADOPI stating that the subscriber has been identified again as the source of infringing content, and that if the conduct does not cease the HADOPI may transmit the file to the public prosecutor for sanctions, which may include suspension of internet access. According to the last figures published by the HADOPI in 2014, 333,723 registered letters of this type have been sent. For subscribers that continue to show evidence of infringing activity, the HADOPI then selects, in the third step, the files to be reviewed and may ask the relevant subscriber to participate in a hearing. The HADOPI can send the files to the public prosecutor if infringement continues.

In addition to relying on the HADOPI graduated response system, victims of copyright infringement have successfully obtained French court orders to block access to streaming sites.

Finally, the French Minister of Culture has nudged the principal French internet advertising players to agree to refuse to purchase advertising space from internet sites that manifestly promote illegal copyright infringement.[5] The list of the sites affected by this measure will be put together by an industry coordination committee based in part on a list provided by the French police authorities. The code of conduct does not provide for any sanction against advertisers that violate the code. The French Minister of Culture also hopes that a similar code will be signed shortly by banks and payment service providers. The code would prohibit payment service providers from knowingly providing service to sites that promote copyright infringement.

4.3 Illegal online gambling

France allows online gambling, but only with gambling service providers that have obtained a license. The licensing conditions are intended to protect individuals against the harms associated with addictive gambling, as well as to protect society against the development of organized crime around online gambling activities. The French regulations on online gambling are administered by a specialized regulatory authority called the ARJEL.[6] French law gives the ARJEL authority to take measures to limit

[5] A copy of the charter is available here: http://www.alpa.paris/wp-content/uploads/2001/01/20150323_MCC-signature-charte-publicite-1.pdf (consulted January 8, 2017).

[6] Autorité de regulation des jeux en ligne, created by Law n° 2010-476 of May 12, 2010.

access by French users to unlicensed gambling sites. The ARJEL has authority to draw up lists of unlicensed gambling sites to which access should be blocked. The ARJEL then submits the list to a court in an *ex parte* proceeding. The court then issues an order requiring that French ISPs block access to the relevant sites by inserting an erroneous IP address for the site in the access provider's local DNS server. The decree relating to ARJEL's blocking authority specifically provides for DNS blocking.[7]

4.4 Child pornography and terrorist propaganda

For internet content involving either child pornography or incitement to commit terrorist acts, the French police authorities are able to send blocking requests directly to ISPs without first obtaining a judge's approval.[8] The police must first attempt to obtain removal of content at its source through a request to the publisher and hosting provider, but if unsuccessful after 24 hours, the police may direct their request to local ISPs. The decree relating to blocking of child pornography or terrorist sites does not specifically refer to DNS blocking.[9] The decree says that ISPs should block access to addresses "by any appropriate means", and redirect visitors toward a website of the French police. The law refers here to blocking "addresses", not to blocking "sites" or "content", which suggests that ISPs would use DNS blocking rather than other more intrusive forms of blocking such as deep packet inspection. The French government must reimburse ISPs for the cost associated with the blocking measures.

To compensate for the fact that no judge is involved in blocking decisions, the law provides that a person named by the French data protection authority will receive copies of blocking requests and can issue recommendations to the police authorities, or ask a court to intervene.

The law relating to child pornography and terrorist site blocking also authorizes the police to address removal requests to search engines and directories.

In addition to these regulatory measures, many internet intermediaries apply self-regulatory measures to facilitate the reporting and blocking of child porn sites. This is done through an international reporting network called "INHOPE" (www.inhope.org).

4.5 Hate speech

French law prohibits content that incites racial hatred or anti-Semitism, as well as content that incites discrimination or hatred based on sex, sexual orientation or handicap. As for any illegal content, hosting providers must remove hate speech content promptly upon receiving notice, under the "notice and takedown" regime. Otherwise, victims may apply

---

7 Decree n° 2011-2122 of December 30, 2011.
8 Law n° 2014-1353 of November 13, 2014.
9 Decree n° 2015-125 of February 5, 2014.

for blocking orders before courts. The court can then order internet access providers to block access to the relevant sites.

4.6 French audiovisual policy

Both French and European law impose "must carry" obligations on telecom operators (a term that includes internet access providers) that distribute audiovisual programs.[10] The operators must distribute certain public service television channels to all subscribers, generally free of charge. The must carry obligation is limited to certain qualifying television channels that serve a general interest.

Audiovisual policy is also promoted via an obligation on providers of "on demand audiovisual media services" to invest a certain amount of their revenues in French and European production, to include in their catalog a majority of European works, and to present French and European works on the service's home page. Under the country of origin rule established by the Audiovisual Media Services Directive[11], these obligations only apply to providers of on-demand audiovisual media services established in France.

4.7 Apparent lack of coherence

The foregoing summary of measures applied in France to advance content policies on the internet is a great simplification. The purpose of the summary is to illustrate the diversity of mechanisms currently used within a single country, and the lack of any apparent methodology to explain the differences in approaches. An invisible methodology may be at work. Each measure adapted by regulators takes into account prior experience, constitutional constraints, political realities, and international benchmarks. But there's no visible roadmap. This leads to questions: Why is an independent regulatory authority used for some content (eg. illegal gambling) but not for other content (eg. hate speech)? Why is a court order required for some forms of blocking (eg. copyright infringement), but not for others (DNS blocking for child pornography, or CNIL right to be forgotten orders)? Where has self-regulation been the most successful? Why are internet access providers targeted for certain kinds of actions, and search engines targeted for others?

There are no doubt good reasons why different solutions apply to different content problems. However, policy makers approach each problem in isolation and can give the impression of reinventing the wheel each time. Without a baseline methodology against which to measure regulatory proposals, the solutions appear inconsistent and uncoordinated. Moreover, the measures cannot easily be compared to gather knowledge on what works, and what doesn't.

---

[10] Article 34-1, Law n° 86-1067 of September 30, 1986; Article 31, Directive 2002/22/EC.

[11] Directive 2010/13/EU

	Institutional authorities	**Principal Internet intermediary targetted**	**Actions**	**Self regulation?**
Copyright infringement	HADOPI	Internet access provider (IAP)	IAP provides user identification. HADOPI sends warning notices.	Advertising service providers
	Courts	Hosting providers, search engines, IAPs	Removing and/or blocking content	
Right to be forgotten	CNIL, without court order	Search engines only	Delisting certain search results	Yes – internal search engine procedures to apply "Costeja" decision
Illegal gambling	ARJEL with court order	IAPs	DNS blocking	
Child porn and terrorism	Police without court order	Hosting providers, IAPs, search engines	DNS blocking by IAPs	Yes (INHOPE)
Hate speech	Courts	Hosting providers, IAPs, search engines		Yes
Audiovisual policy	CSA	IAP, on-demand AVMS providers	Must carry. AVMS measures to promote European content	

Table 1: Summary of mechanisms used in France to advance content policies on the internet

5. DIMINISHING ROLE OF BROADCASTING REGULATION

Another factor is at work, which is the diminishing role of audiovisual regulation in advancing national content policies. Historically, the licensing of broadcasting spectrum was the best way to ensure compliance with a wide range of national content policies. In addition to prohibiting illegal content, broadcasting licenses include rules to promote media diversity, plurality of opinions, to protect national security (via foreign ownership limitations), minors, public health, culture, language and national cinema. In some cases, broadcasting rules are designed to protect other economic sectors. The range of content policies contained in broadcasting licenses goes from matters of great national importance, such as rules protecting the proper functioning of democracy, to matters involving narrow economic interests, such as the protection of advertising revenues for regional newspapers. For decades, the broadcasting license has been a convenient basket in which politicians could throw numerous content rules designed to satisfy various stakeholders.

The license to use spectrum is a convenient tool. Spectrum is part of the public domain. It belongs to the government, so the government can legitimately impose conditions in connection with its use. Just as the government can impose building rules for beachfront property designed to protect cultural and environmental aesthetics, it can impose usage rules on spectrum designed to promote French culture. In France at least, broadcasting spectrum is licensed free of charge, whereas mobile broadband spectrum is licensed in exchange for a hefty license fee. The government imposes content rules on broadcasters in lieu of a license fee.

Over-the-air broadcasting still commands a large share of audience and viewing time in France. But its influence is diminishing, and will one day disappear. Some day in the future, most viewers will consume content online, using connected TVs, smartphones or tablets. Over-the-air channels received via a rooftop antenna will become the exception. Most broadcasters will make their content available via broadband (fiber, DSL, 4G/5G). When content providers no longer need broadcasting spectrum, governments will no longer have an easy "hook" through which to impose content policies. Governments will have to look elsewhere, and will turn to telecom operators and other internet intermediaries to fill the regulatory void. In 2006 Eli Noam predicted that telecommunication regulation will "become" broadcasting regulation, and that telecom operators will be asked to enforce national content policies because they are the only entities that regulators can reach within their jurisdictions (Noam, 2006). In fact, Noam's prophecy can be applied not just to telecom operators, but to any internet intermediary that falls within a regulator's jurisdictional reach. The decline of broadcasting regulation as a tool to regulate access to content explains why regulators look increasingly to internet intermediaries for solutions.

6. A METHODOLOGY AGAINST WHICH TO MEASURE REGULATORY PROPOSALS

As the examples above show, lawmakers adopt measures to address a particular problem. Sunstein (1996) refers to this as the "pollutant of the month" syndrome. The measures create

controversy and are often challenged in court. The measures are often accused of disproportionately harming fundamental rights, being costly and ineffective, and/or threatening the internet ecosystem (Haber, 2010). There lacks today a theoretical benchmark against which to test the relevant measures – whether imposed by government or voluntary -- to ensure that they are as efficient as possible, and harm fundamental rights as little as possible.

6.1 Technical measures are inevitable

We will start from the premise that national measures to involve internet intermediaries in the enforcement of content policies are inevitable (Noam, 2006). The question is not whether they will emerge, but how they should be built (Mann & Belzley, 2005).

6.2 Technical measures create harmful side-effects

As noted above, measures implemented by internet intermediaries to block or limit access to illegal content can create negative externalities, including adverse effects for fundamental rights, net neutrality, and the internet ecosystem. Like a potent medicine, measures affecting internet intermediaries must be prescribed with care in order to avoid dangerous side effects. A blocking measure targeting illegal content can also block legal content. Some technical measures create privacy risks for users, and/or significant costs for internet intermediaries. Some measures may simply be ineffective. A government-imposed measure may also set a precedent for other countries, thereby creating an international arms race in regulation that could threaten or destroy the open character of the internet.

6.3 A reference methodology will help avoid mistakes

If we accept as a given that certain technical measures are necessary, we need to consider what form should those measures take, and who should be in charge of administering them so as to minimize their harmful side effects.

I propose in this thesis a reference methodology that could be used to evaluate regulatory proposals that affect internet intermediaries. The methodology would involve a questionnaire designed to help policy makers define the problem to be addressed, the alternatives available to address the problem and the direct and indirect costs generated by each alternative. The questionnaire would be followed by a cost benefit analysis (CBA), and the application of certain constraints. The questionnaire and cost-benefit analysis would then be subject to public consultation and to an institutional peer-review process. Finally, the regulatory measure would be subject to periodic *ex post* reviews to ensure that the measure is delivering its expected benefits and is not creating unexpected side-effects.

7. EXISTING LITERATURE

The proposal builds on five categories of existing literature:

i. Law and economics literature dealing with the most efficient level of law enforcement (Shavell, 1993) and most efficient level of ISP involvement to fight copyright infringement and other forms of illegal content (Lichtman & Landes, 2003; Lichtman & Posner, 2006; Mann & Belzley, 2005);

ii. Law and economics literature on net neutrality (Wu, 2003; Yoo, 2005; Curien & Maxwell, 2011);

iii. Law and economics literature on better regulation, the new public management and cost benefit analyses, with particular emphasis on environmental, health and safety regulation (Breyer, 1982; Sunstein, 1996; Hahn, 2004; Hahn & Litan, 2005; Posner, 2002; Ogus, 1998; Hancher, Larouche & Lavrijssen, 2003; Renda *et al*., 2013);

iv. Literature on institutional alternatives for internet governance, including self-regulatory and co-regulatory structures (Marsden, 2011; Brousseau, 2007; Weiser, 2009; OECD, 2011);

v. Literature on the principle of proportionality, and the balancing of fundamental rights (Hickman, 2008; Tranberg, 2011; Sauter, 2013; Monaghan, 1970; Lemley & Volokh, 1998; Callanan et al., 2009).

8. HOW THE REMAINING CHAPTERS ARE DIVIDED

The remainder of this thesis is organized as follows:

Chapter 2 will make an inventory of the factors that must be weighed when developing regulatory proposals. Chapter 2 will list the national content policies for which regulators may be tempted to enact regulation. Enforcement of those content policies is the expected benefit of regulation. Chapter 2 will establish a list of technical intermediaries and technical measures that can potentially be used to implement content policies. These are the technical tools that regulators might consider using. Chapter 2 will mention institutional alternatives and list the negative side effects that government-imposed technical measures might cause. These are the potential costs of regulation.

Chapter 3 will focus on the balancing of fundamental rights. The European Court of Justice, the European Court of Human Rights and the United States Supreme Court afford to internet users a high level of freedom of expression. Internet content is entitled to the highest level of protection, similar to protection afforded to print media. The imposition of broadcast-style regulation on internet content would likely be illegal, violating the European Convention on Human Rights.

Other fundamental rights in the balance include:

- the right to protection of property, which can justify measures designed to fight online copyright infringement;

- the right to security, which can justify measures designed to fight child pornography and terrorism;

- the right to privacy, which can be infringed by invasive technical measures, but can also justify measures taken to enforce national privacy laws (*eg.* the right to be forgotten);

- the right to freely conduct a business, which can be interfered with when burdensome technical measures are imposed on internet intermediaries, or regulators proscribe certain business models.

Each technical measure can enhance or impair fundamental rights. Courts have developed a balancing test to weigh these rights against each other, and determine a measure's acceptability under constitutional principles. Chapter 3 will explain the proportionality test used by European courts, and how the test has been applied to technical measures designed to limit access to illegal content. Chapter 3 will also examine how law and economics scholars approach the fundamental rights of privacy and freedom of expression, which are the two rights most directly affected by technical measures imposed on internet intermediaries.

Chapter 4 will examine the institutional aspects of technical measures, including the four main categories of institutional frameworks that can be used for regulating access to internet content:

1) General liability or property rules enforced by the courts, which I call "court regulation";

2) Detailed regulatory rules developed and enforced by an administrative or regulatory body, which I call "administrative regulation";

3) Self-regulatory regimes, which can involve unilateral regulation by each firm through individual terms of use ("unilateral self-regulation"), and regulation through collective codes of conduct ("multilateral self-regulation");

4) Co-regulatory regimes, in which self-regulatory measures and government-imposed measures work together ("co-regulatory systems").

These four institutional frameworks often coexist with, and complement, each other. Indeed the first framework, general liability or property rules enforced by the courts, almost always exists, either by itself or as a backstop for other regulatory measures. In the shadow of liability rules and court enforcement, private actors use unilateral self-regulation, *ie*. regulation through terms of use, to govern their relationship with users. The main additional options are administrative

regulation, multilateral self-regulation and co-regulation. Chapter 4 will identify the advantages and disadvantages of these various institutional options, and how they can be used to deal with internet content issues. The objective is to put institutional options into the mix when evaluating regulatory alternatives. Brousseau's (2007) work on multi-level governance will be discussed.

Chapter 5 will focus on better regulation methodology, regulatory impact assessments and cost benefit analyses. Both the UNITED STATES and Europe have developed methodology for testing regulatory measures using a cost-benefit analysis. The rigor with which the cost-benefit analyses are applied varies. Chapter 5 will examine the cost-benefit methodology and "good regulation" criteria proposed by the OECD, the United States government and the European Commission.

A study by Renda *et al.* (2013) examines how cost benefit analyses should be conducted in the context of EU "better regulation" guidelines. Government Circular A4 describes the nuts and bolts of regulatory cost benefit analyses in the United States. Chapter 5 will also present the views of authors who argue that regulatory impact assessments are incompatible with the realities of the political process.

Chapter 6 will attempt to bring together the themes of the preceding chapters by presenting a system for evaluating regulatory proposals affecting internet intermediaries. The system is inspired by the European Framework for regulating electronic communications and by the European Commission's methodology for conducting regulatory impact assessments. The system consists of five parts:

- A questionnaire requiring policy makers to identify what the regulator hopes to achieve, how success will be measured, the regulatory options available, and the main costs and benefits associated with each option;

- A cost-benefit analysis requiring the preparation of a baseline scenario of no regulatory action and a comparison of the costs and benefits of various regulatory alternatives to the baseline scenario. The cost-benefit analysis will include a step where additional constraints can be imposed, which may lead to the elimination of certain regulatory proposals;

- The third part of the system consists of a public consultation, inviting stakeholder comments to the proposed regulatory impact assessment. The regulator would then revise the impact assessment to reflect stakeholder comments.

- The fourth part of the system consists of a peer review process pursuant to which the regulatory impact assessment is reviewed by an independent body. Robust peer review is a critical element of any "better regulation" strategy. Peer review of this kind exists already for cost-benefit analysis performed in the United States and regulatory impact

assessments performed in the EU. In the field of electronic communications, a specific review system exists pursuant to which the European Commission reviews national regulatory proposals, and can in some cases veto them, prior to their adoption by national regulators. The system proposed in this thesis would require that proposed national measures affecting internet intermediaries undergo a similar review process.

- Finally, the system would require periodic *ex post* reviews to ensure that the measure continues to deliver the expected benefits in spite of technological and market developments. Regulations that are no longer fit for purpose would be amended or removed altogether.

Chapter 7 will point out weaknesses of the proposed system and areas for future research.

In conclusion, the thesis will propose tools that will help determine what action (if any) is appropriate to deal with a given problem of harmful content, including what institutional framework, and what internet intermediary. The methodology will help trace lines, as illustrated on the following figures:

Figure 1: A combination of institutional framework and technical measure to deal with hate speech

Figure 2: a combination of institutional framework and technical measure to deal with copyright infringement

The methodology will necessarily be imperfect given the many variables involved and the difficulty measuring them in an objective manner. The methodology will also create extra costs of its own. Regulatory impact assessments, public consultations and institutional peer review take time and resources that could be invested elsewhere. These extra costs would have to be compared to the benefits derived from better rulemaking. Better rulemaking means laws and regulations that are effective, create fewer costs and adverse side effects, are more predictable, consistent, and future-proof.

Applying cost-benefit analyses to internet regulation will help make trade-offs more visible, avoid costly errors, and will lead to the emergence of international best practices. Without the methodology, the accumulation of uncoordinated national measures will lead to the balkanisation of the internet.

CHAPTER 2 - PRESENTING THE VARIABLES OF THE COST-BENEFIT EQUATION

1. INTRODUCTION

As noted in Chapter 1, this thesis presents a methodology for evaluating regulatory measures relating to content policies. The methodology involves several variables, which I present briefly in this chapter. Subsequent chapters will take a deeper dive into certain variables and balancing tests.

The methodology starts with a given **content policy**, for example a policy to reduce or eliminate images of child pornography online, or a policy to apply the "right to be forgotten."

For any given content policy, there should exist an ideal combination of **internet intermediary action** (eg. website blocking based on DNS server) and **institutional framework** (eg. self-regulation) that maximize the net benefits of the measure. The net benefits are equal to:

a) the benefits for society flowing from application of the measure;

b) less the direct and indirect costs resulting from the measure.

The direct and indirect costs include:

i. the direct costs of implementation of the measure by the internet intermediaries;

ii. the direct costs of the institutional framework, including enforcement costs;

iii. the costs associated with interference with fundamental rights, including freedom of expression, privacy, procedural fairness, the right to property and the right to conduct a business;

iv. the costs associated with interference with the open internet including harm to innovation;

v. the costs associated with other unintended effects, including changes in user behavior.

This chapter will provide a brief overview of these benefits and costs. Many benefits and costs will be difficult to measure, making a standard cost-benefit analysis difficult. Chapter 6 proposes explores ways of quantifying certain benefits and costs, or using qualitative labels where quantification is not possible.

The diagram below shows on the y axis the level of net benefits and on the x axis the level of enforcement of the relevant content policy using different regulatory options. Q^1 represents the ideal level of enforcement, ie. a measure that maximizes net social benefits. The measure Q^2 provides a more complete level of enforcement of the relevant content policy, but does not maximize net social benefits when all costs (including effects on fundamental rights and the internet ecosystem) are taken into account.

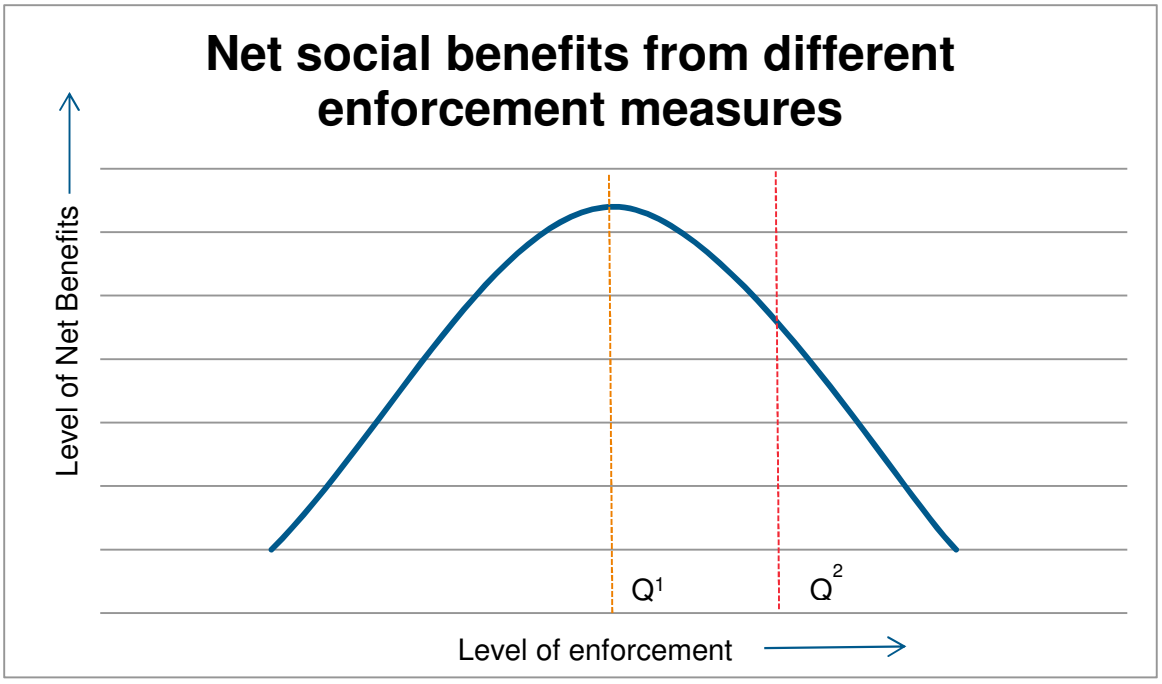


Figure 3: The ideal level of enforcement of a content policy is the one that yields the highest net social benefits (x axis = level of enforcement, y axis = total benefits less total costs)

This chapter will provide a brief overview of five main variables in the "net social benefits" equation, *ie.*:

- the content policy that requires an enforcement measure. Those content policies are intended to address market failures;
- the kinds of internet intermediaries that can potentially take action to enforce the content policy;
- the institutional options that are available;
- the potential harms to fundamental rights;
- the potential harms to the internet ecosystem.

2. CONTENT POLICIES

There are a range of content policies that internet intermediaries could potentially help enforce. For some content policies, the involvement of internet intermediaries may be highly effective without significant side effects. For other policies, the involvement of internet intermediaries may be ineffective, or worse: The harmful side effects may outweigh the benefit derived from the measure.

Below is a list of fifteen categories of content policies that may prompt proposals for internet intermediary action. The content policies described below reflect government responses to market failures. In some cases, the content policies are designed to protect property rights, which are necessary to ensure an efficient allocation of scare resources. In other cases, the content policy is designed to compensate for negative externalities, as in the case of policies designed to limit spam and the use of cookies. The content policy may be designed to ensure that a market for certain criminal activities, e.g. the sexual exploitation of children or the sale of illegal drugs, does not exist at all, because of the intolerably high negative externalities that those transactions create.

The existence of a given content policy, such as a law prohibiting copyright infringement or child pornography, constitutes a first level response by government to a market failure. The second level of analysis, and the one most relevant for our discussion, is whether existing government mechanisms for enforcement, combined with existing market-based enforcement mechanisms, provide an optimal level of enforcement. If the answer is no, then some form of regulatory intervention may be necessary to bring enforcement mechanisms closer to a socially optimal level. This regulatory intervention may implicate internet intermediaries.

As will become evident in Chapter 6, the existence of a given content policy will usually be taken as a given in any regulatory impact assessment. The key question will not be whether the content policy should exist, but whether the level of enforcement is optimal. In some cases, internet intermediaries may have a role in building a socially optimal enforcement strategy. The actions of internet intermediaries may flow from self-regulatory measures or from government constraint. In other cases, the socially optimal enforcement strategy may rely exclusively on traditional enforcement tools used by the police and/or litigation before civil courts.

Below is a non-exhaustive list of content policies for which internet intermediaries may have a role to play.

2.1 Cybersecurity threats

Internet intermediaries have long contributed to the fight against malicious software code and other forms of cyber-attacks. Cyber security threats may consist of malware, spyware, denial of service attacks, or other techniques designed to disrupt computer systems and/or steal confidential information from systems. internet intermediary action

here has long been considered effective and essential to protect the internet and its users. Most internet intermediaries already take action to protect their services and customers against cyber-attacks. Cyber-attacks create costs for internet intermediaries, and the risk of these costs is to a large extent internalized by internet intermediaries. The market therefore provides a reasonably high level of cyber security enforcement, without the need for government regulation.

Like national defense, certain aspects of cyber security have the characteristics of public goods, and may be under produced without regulatory intervention. For example, to build an effective national cyber-defense strategy, it may be necessary for corporations to disclose to government authorities information about cyber-attacks. Yet such information-sharing will generally not occur without a regulatory obligation because the information-sharing will create costs for corporations, and they will have a tendency to free-ride in the absence of regulatory constraint.

2.2 Spam and phishing

Spam and phishing do not aim directly to disrupt computer systems, but instead seek to take advantage of vulnerable internet users. Some forms of spam may be legitimate advertisements. But they are sent to millions of e-mail addresses simultaneously at almost no cost for the sender. The massive sending of e-mails creates negative externalities: annoyance for internet users and potential risk for the network. Phishing is a form of internet fraud in which the sender of the spam pretends to be a bank or other legitimate vendor, and thereby tries to obtain through fraud confidential information from the internet user.

2.3 Cookies and other form of tracking software

Unlike spyware, cookies generally serve legitimate business purposes. They are used to track internet users' browsing habits in order to make browsing easier, to permit the web publisher to gather statistics, and to permit web publishers and advertising networks to place targeted advertising. Certain uses of cookies pose privacy threats, particularly when cookies share browsing habits with advertising networks to facilitate behavioral advertising. The market failures here are information asymmetries: consumers do not know what cookies are doing and therefore cannot make rational decisions. Data privacy laws may therefore require that users be informed of the presence of cookies and that for certain uses of cookies (eg. advertising) users give their prior consent. Targeted advertising permits web publishers to provide free services and information to users, contributing to the diversity of content available on the internet. Therefore content policies that limit the use of advertising cookies must be balanced against the benefits that cookies bring to web publishers, and ultimately to users.

2.4 "Right to be forgotten" content

Certain content may be perfectly legal, but its availability on the internet may cause damage to individuals. For example, an old newspaper article describing the financial difficulties of an individual may continue to appear prominently in search results, even though the article is outdated and not relevant to the individual's current life and financial situation. Individuals may also be harmed by articles or photos describing unflattering events that occurred in the person's youth. To address this kind of harm, the European Court of Justice held that individuals have the right to ask search engines to eliminate from search results content of this kind, as long as the elimination does not unduly interfere with freedom of expression.[12] The United States also has laws that recognize a "right to be forgotten" in limited situations. California's so-called "Eraser Law"[13] allows minors to require the deletion of photos or other information that they previously posted on social media; the Federal Credit Reporting Act (FCRA)[14] prohibits organizations that provide credit scoring from taking into account negative events that occurred more than seven years previously. The application of the European version of the "right to be forgotten" poses complex problems for governments and internet intermediaries because each delisting requires a fact-specific balancing of fundamental rights. The territorial reach of the right to be forgotten is also highly contentious.

From a law and economics perspective, the harm caused to a person as a result of his or her unflattering (but true) information being readily available to anyone searching the internet using the person's name could be considered as a negative externality, ie. the cost caused to the person is not taken into account in the transaction between the supplier of the search service and the user of the search services. Posner (1978) argues that the availability of true but unflattering information leads to efficient transactions, both in professional and private contexts. The availability of information reduces inefficient search costs, and fewer transactional errors due to information asymmetries.

The user of a search engine purchases a search service precisely in order to find information about the object of the search. When the search term is a person, the information sought may include unflattering information. The searcher therefore derives a private benefit from finding such information, and that benefit may offset in whole or in part the cost suffered by the person whose embarrassing information was revealed. The "right to be forgotten" therefore does not resemble classic situations of negative externalities, because the thing that is being purchased and which has value for the purchaser is precisely the thing that creates the harm to the third party. This is similar to the situation of a person offering to pay a dollar to a factory to emit a certain amount of pollution because the purchaser derives benefit from the pollution emitted (even though

12 CJEU Case n° C-131/12, Google Spain v. AEPD and Costeja, May 13, 2014.
13 CAL. BUS. & PROF. CODE § 22581 (West 2015).
14 15 U.S.C. § 1681.

the pollution bothers a neighbor). If there were a market in the pollution, the neighbor would pay the factory, or the prospective purchaser of pollution, in order to prevent the transaction from taking place. If the victim's offer exceeds the purchaser's, the transaction would not take place. Conversely, if the purchaser of the pollution proposes more than the victim, the transaction would take place, and this would be efficient.

In the case of unflattering information, the same reasoning would apply. If the value of the information to the searcher is higher than the value of concealment to the victim, the information should be revealed. However as Posner (1978) points out, the market in true information is different from other markets. The concealment of true information about goods or persons would yield inefficient transactions (eg. hiring decisions) based on incorrect information (information asymmetries). The concealment would generate inefficient search costs such as hiring a private detective instead of using a search engine, and lead to potential adverse selection effects, in that a searcher may assume that all persons are hiding unflattering information, even those who aren't.

Unfiltered search results also provide significant positive externalities to web publishers. Web publishers are not party to the transaction between the provider of the search service and the user, or party to the transaction between the provider of the search service and advertisers. They are third parties, and derive significant benefit from search transactions because their content is visible to those looking for it. This avoids having to spend large sums on advertising. Search neutrality, like net neutrality, creates significant positive externalities that also must be considered when imposing "right to be forgotten" policies on search engines.

The "right to be forgotten" is relatively new, and has not yet been studied by economists. Under what conditions the right to be forgotten yields a welfare-maximizing outcome is beyond the scope of this thesis. What is important here is how regulators should evaluate different technical and institutional alternatives for achieving the desired "right to be forgotten" outcome.

2.5 Illegal online gambling

Gambling is highly regulated in most countries. The purpose of regulation is both to protect individuals against gambling addiction and to protect the public against the development of organized crime and money laundering in connection with gambling operations. In some jurisdictions, gambling of all forms is illegal. In other jurisdictions, gambling operations are legal but require a license. In both cases, jurisdictions will seek to enforce their policies by preventing citizens from gambling on illegal gambling websites, most of which will be situated outside of the relevant country. Internet intermediaries are often asked to help limit access to these offshore web sites.

Laws designed to fight illegal online gambling include France's so-called "ARJEL" law, which created an independent regulatory authority in charge of licensing legitimate online gambling platforms, as well as making a list of illegal platforms to which access should be blocked.[15] The ARJEL regulatory authority must apply to a court for an order requiring all internet access providers in France to block access to the illegal gambling sites.

Like cigarette smoking, online gambling is a demerit good that generally creates more harm than good to the gambler. Yet because of myopia and addiction effects, the individual will not be able to weigh the harm and benefits in a rational manner, leading to decisions that are not in the gambler's own interest. Gambling also creates negative externalities, by leading to personal bankruptcies, and markets for illegal loans, which hurt third parties. Finally, online gambling can create problems of information asymmetries, because it is very hard for gamblers to distinguish honest online gambling sites from ones that are dishonest or linked to organized crime.

2.6 Sale of cigarettes and alcohol

The sale of cigarettes and alcohol is regulated both to protect public health, particularly that of minors, and to raise tax revenues for the state. Cigarettes and alcohol are demerit goods, creating harm to those who consume the products but also harm to third parties, thereby creating negative externalities. Jurisdictions applying these policies will seek to prevent consumers from purchasing cigarettes and alcohol via the internet from vendors who are not subject to the regulations of the relevant jurisdiction.

2.7 Counterfeit drugs, illegal drugs

Drugs are also highly regulated. Some drugs are illegal in all circumstances (*eg*. heroin), other drugs require a prescription. A growing problem is the sale via internet of counterfeit drugs, *ie*. drugs that are made to appear identical to legitimate drugs but are in fact illegal copies. The copies are at best ineffective, at worst highly dangerous. A buyer may not know the difference between a legitimate drug and a fake. Internet intermediaries may be asked to help shut down these dangerous web sites.

2.8 Intellectual infringement

The internet has made it easy to violate copyright and trademark laws. Individuals can create digital copies of protected works (music, films, books, photos, sheet music) with relative ease and make the works freely available on the internet. Copyright violations on the internet can originate from organized criminal operations, or from the actions of ordinary citizens who wish to share or consume content without monetary gain. Sale of counterfeit goods is also facilitated by the internet, leading to harm to purchasers who think they are buying a product with a particular level of quality, and to legitimate sellers

[15] Law n° 2010-476 of May 12, 2010.

who invest in product development and advertising and who are taken advantage of by free-riding counterfeiters. Copyright and trademark infringement laws protect a property right, thereby nudging people to acquire protected works and products through the legitimate market as opposed to through black market mechanisms. Internet intermediaries will often implement policies to limit online infringement, either pursuant to their own internal policies, or as a result of government regulation.

There are numerous examples of laws and self-regulatory initiatives designed to fight online copyright infringement. One of the best known examples internationally is the French HADOPI law, described in Chapter 1.

Other examples include the UK's Digital Economy Act, which calls for an industry agreement involving ISPs and other stakeholders, failing which additional regulatory measures would be imposed on internet intermediaries. The United States relies heavily on the Digital Millennium Copyright Act to impose notice and take-down obligations on internet intermediaries for copyright infringement. The UNITED STATES also has a system for seizing the domain names of websites that infringe intellectual property. Finally, the UNITED STATES has implemented a self-regulatory framework, called the Center for Copyright Information, that resembles in many respects the French HADOPI regime.

Many question whether the property right created by copyright laws is overly restrictive in the digital era. Proponents of copyright reform argue that certain digital uses of protected works should be permitted under an extended "fair use" exception to copyright. The debate on the scope of copyright is beyond the scope of this thesis, but sometimes interferes with the debate on the role of internet intermediaries. The way digital intermediaries enforce copyright can affect how copyright exceptions are applied in practice, thus affecting the scope and existence of the right itself.

2.9 Defamation and the protection of privacy

Certain content published on the internet will is illegal because it is defamatory or wrongfully invades an individual's privacy. Photos taken of a person in a private setting may be illegal, as may be the publication of information relating to an individual's private life (*eg*. her confidential health information). Under law and economics, the existence of a privacy right is considered efficient so that people do not invest needlessly in high walls and security measures, and so that people communicate more freely. Publishing false and harmful information about an individual is defamatory. False information about people, like false information about goods, leads to inefficient transactions.

The publishers of the defamatory or privacy-invading content may be impossible to locate, making enforcement on the internet difficult. Internet intermediaries may be called on to

help. Content that violates defamation or privacy law will be removed at the source wherever possible, because the individual victim's rights will outweigh the publisher's freedom of expression and the public's right to access the information. In other words, the objective will be to remove the content entirely from the internet, or block its access if removal is not possible. This contrasts with the "right to be forgotten," where the underlying content is not defamatory or a serious enough violation of privacy rights to merit removal. Instead, the content should only be made more difficult to find when using certain search terms.

2.10 Websites promoting racial, ethnic or religious hatred

A number of countries prohibit websites that promote racial, ethnic or religious hatred. The First Amendment of the United States Constitution prohibits the state from adopting laws that regulate speech based on the ideas conveyed, which limits the United States government's ability to prohibit so-called "hate speech". In Chapter 3 I explain that "chilling effects" are largely behind this broad interpretation of freedom of speech principles. In European countries, constitutional freedom of expression principles give more flexibility to the state to regulate content that promotes racial hatred or anti-Semitism. Internet intermediaries frequently assist in eliminating hate speech on the internet, either through voluntary acceptable use policies, or through government-imposed measures such as blocking. Chapter 3 examines the law and economics justification for prohibiting (or not) hate speech.

2.11 Regulations designed to protect local culture and language

Certain countries have regulations to promote local film production, local culture and language. These rules are generally part of the country's broadcasting regulations. However, as the difference between traditional broadcasting and internet content becomes blurred, a number of countries are considering how regulations designed to protect and promote culture on television can be applied to the internet. Some proposals would involve internet intermediaries as vectors for cultural policy. For example, the so-called "Lescure Report" in France[16] proposed that ISPs allocate more bandwidth to online video platforms that voluntarily agree to promote French culture and audiovisual production. The objective of these cultural policies is generally to redistribute wealth toward producers of local content, so that they remain viable in the face of lower-priced popular content from the United States. The mechanism is similar to regulations designed to protect local agriculture. The rationale for these regulations is generally that a rich cultural ecosystem is a public good that will be under-produced by the market without public intervention.

[16] P. Lescure, "Contribution aux politiques culturelles à l'ère numérique", May 2013.

2.12 Advertising laws

Consumer protection laws govern all forms of advertising. Broadcasting laws generally contain additional rules for television advertising. Advertising laws may seek to address information asymmetries and/or seek to discourage consumption of demerit goods. Countries may seek to apply these advertising policies to content on the internet, even content that originates from outside the country. As is the case for other content policies, it is not inconceivable that internet intermediaries might be asked to help police these measures, by blocking certain forms of advertising that violate local laws.

2.13 Protection of minors against adult content

Some content is legal for adults, but prohibited for minors. A major objective of broadcasting laws is to protect minors from sexually explicit and violent content. Providers of adult content are generally required to make sure that only adults may access the content. For some content, it may be sufficient that the program be scheduled late at night and/or have a warning label advising that the content may be inappropriate for young viewers. Lawmakers will try to find ways to make sure that these measures are applied on the internet, potentially calling on internet intermediaries to implement age verification mechanisms. Parental control software already addresses this issue in part.

So-called "adult" content is linked to a broad category of content considered "inappropriate," including nudity, violence or degrading content. Many social media platforms prohibit this sort of inappropriate content under their acceptable use policies. I will examine these acceptable use policies in Chapter 4, under the heading "unilateral self regulation."

Regulation of adult content must take into account the harm caused to the viewer of the content, but also potential harm to third parties (externalities). These harms must be weighed against freedom of expression. The harms to the viewer and to third parties are potentially much greater when the viewer is a child, because of the effects on the child's personality and future development.

2.14 Child pornography

Images depicting the sexual exploitation of children are illegal in virtually all countries. Police attempt to identify and arrest persons who possess and share such images. Governments may also take measures to ensure that websites proposing such images are not accessible to the public. These government policies are supplemented by self-regulatory programs implemented by internet intermediaries in cooperation with law enforcement authorities.

Examples of initiatives designed to limit online child pornography include France's so-called LOPPSI 2 law[17] which authorizes the Ministry of Interior to create a list of URLs corresponding to websites with images of child pornography. The Ministry of Interior may then require internet access providers to block access to the relevant URLs. On the self-regulatory front, internet intermediaries participate in the INHOPE network, which permits a centralized reporting of child pornography sites. Internet intermediaries then voluntarily take steps to impede access to the relevant sites. For example, British Telecom implements a so-called "Clean Feed" system to impede access to child porn sites.[18] This is done on a purely voluntary basis.

2.15 Content promoting terrorism

In an effort to limit access to websites that recruit young and vulnerable people to join the so-called Islamic State and other terrorist organisations, France recently enacted a law permitting the police to require ISP blocking of websites that promote terrorism.[19] The blocking can be ordered by the government without a court order. As I will explain in Chapter 3, blocking websites without a court order raises concerns about fundamental rights. One of the important safeguards of fundamental rights is to make sure that a judge is involved when a fundamental right is curtailed.

3. ASSISTING LAW ENFORCEMENT

In addition to asking internet intermediaries to help enforce pre-defined content policies, governments also rely on internet intermediaries to help locate criminals and gather evidence for criminal investigations of all kinds. This is generally done by asking certain intermediaries to provide metadata that can help track a suspected criminal's online activities. In the context of criminal investigations, the metadata is provided only after the police have obtained an authorization from a prosecutor or judge. In the context of intelligence gathering activities, government agencies are subject to fewer constraints, and may in some cases collect large amounts of metadata directly from internet intermediaries. The internet intermediaries' role in assisting law enforcement or intelligence agencies is not linked to a particular content policy, and therefore falls outside the scope of this thesis.

Nevertheless, the role of internet intermediaries in assisting law enforcement involves many of the same trade-offs as those examined here. For example, how far may governments go in asking internet intermediaries to gather data and make the data available to the government? What surveillance techniques are proportionate? An EU-funded study called "SURVEILLE" attempts to build a methodology for examining these questions, a methodology that shares some characteristics with the system presented in this thesis. I examine the SURVEILLE project in more detail in Chapter 7.

---

17 Law n° 2011-267 of March 14, 2011.

18 https://en.wikipedia.org/wiki/Cleanfeed_(content_blocking_system) (consulted January 22, 2017)

19 Law n° 2014-1353 of November 13, 2014.

4. VALUING CONTENT POLICIES AND THEIR ENFORCEMENT

For the purposes of building our methodology, we should assume that all content policies have legitimacy in the relevant country where they were adopted, *ie*. they have all been adopted by a democratically-elected legislature after debate, and are subject to appropriate constitutional guarantees. I therefore exclude from discussion content policies with doubtful legitimacy, such as content policies adopted by totalitarian governments to suppress political dissent.

All of the content policies examined in Section 2 above are presumed legitimate, but they do not all have equal importance to society. The fight against terrorism, child pornography and counterfeit drugs will likely be more important to society than content policies designed to curb online copyright infringement. This does not make rules designed to curb online copyright infringement any less legitimate than rules designed to fight child pornography. It simply means that where enforcement resources are limited, there may be a compelling argument for devoting more resources to the fight against child pornography than to the enforcement of online copyright infringement. This would be the case, for example, if for a given 1,000€ of enforcement resources, society could save one child from sexual assault, compared to preventing 1000 illegal movie downloads. (This assumes that society values the saving of a child more than preventing 1000 downloads, which is a reasonable assumption.)

Content policies generally carry different values in terms of society's "willingness to pay" for enforcement. The price society is willing to pay to prevent terrorism may be higher than the price society is willing to pay to enforce rules designed to protect local cinema production, for example. The price attached to a given content policy will help determine the amount of tax revenues devoted to the policy's enforcement, and the number of trade-offs and collateral harms that society is willing to accept in order to enforce the policy. For example, society may tolerate more intrusions of privacy in the context of fighting terrorism than in the context of fighting copyright infringement. Some actions by internet intermediaries may be justified for enforcing a high-stakes content policy, whereas the same action would not be justified for enforcing a content policy that has a lower value to society.

Trying to create a hierarchy of content policies using a willingness to pay measurement is fraught with difficulty, and can lead in some cases to absurd results. First, there exists no market for content policies, so willingness to pay can only be guessed at. Second, just because fighting child pornography commands a higher willingness to pay than fighting copyright infringement does not mean that resources should always be devoted to child pornography at the expense of copyright infringement. Societies will generally devote resources to both, but in different amounts.

Another complicating factor is the absence of consensus on the social importance of certain content policies. Critics of copyright laws argue that certain aspects of copyright law reflect the highly-effective lobbying of certain industry groups as opposed to a balanced representation of citizens' views. Thus content policies, like any other aspect of lawmaking, can be subject to

various degrees of regulatory capture (Stigler, 1971). The problems associated with valuing content policies and fundamental rights will be addressed in more detail in Chapter 6, which deals with cost-benefit analyses.

Each content policy may have an ideal enforcement strategy associated with it. Shavell (1993) examines the factors that determine the theoretically optimal form and level of law enforcement. Shavell's determinants show when enforcement efforts should occur, *ie*. before the act, via prevention and deterrence measures, or after the fact, via punishment (fines and imprisonment). Other determinants influence the form that sanctions should take, *ie*. monetary sanctions or imprisonment, and whether private or public enforcement (or a combination of the two) is optimal.

Enforcement strategies are closely linked to the type of content policy that is being applied. As we will see in Chapter 6, one of the most difficult tasks for policymakers will be to define their enforcement objective with precision. What level of preventive measures do we expect internet intermediaries to apply. In most cases, 100% enforcement of a content policy will not be optimal because of the high level of associated costs. As noted in Section 1 of this chapter, optimal enforcement will occur at a point where social benefits net of costs are maximized. This will generally occur at a point where the sum of (i) the costs of enforcement plus (ii) the costs of the relevant harm that the content policy seeks to address, is minimized.

5. INTERNET INTERMEDIARIES

Now that we have identified the main categories of content policies, let us look at the internet intermediaries that might be called upon to promote the content policies, and the actions they might take. Whether internet intermediaries should take such action, and in what institutional framework (self-regulation, government compulsion), will be examined later.

Below is a list of internet intermediaries that could be called on to enforce a content policy, and a short description of the measures they might take. The list does not purport to be exhaustive.

5.1 Search engines

Search engines can take several actions to limit access to undesirable content. The first is to make sure that sites presenting undesirable content do not purchase advertising on the search engine, and therefore do not appear in the list of sponsored search results. For example, a search for information about Viagra would not show a sponsored link for a known vendor of counterfeit drugs. The second potential measure consists of ensuring that the relevant site does not turn up at all in the search results, or does not appear in the search results for certain national versions of the search engine. This is what happens when a search engine delists a site completely in response to certain name-based searches under a so-called "right to be forgotten" request. The third option for search engines is to adjust search results so that the undesirable content appears low in the rankings. This solution might be appropriate where delisting the site entirely might

create a disproportionate restriction of freedom of expression. An example of this sort of action is where the search engine gives higher priority to music or video download sites that have received a trust seal, or lower priority to sites that numerous internet users have complained about. This solution has been discussed in the context of the text of *Mein Kampf*, which fell into the public domain in 2016. Search engines would give higher ranking to the version of *Mein Kampf* that is commented by respected historians, and lower ranking to sites that use Mein Kampf for revisionist propaganda (Alexandre, Coen & Dreyfus, 2016).

The measures applied by a search engine might also be limited to certain geographic areas. Search engines often have localized versions of their sites that internet users see by default based on their IP address. For example, an internet user in France will generally hold an IP address belonging to a French ISP. When that internet user goes to a search engine, the search engine will recognize the IP address as belonging to a French ISP and present to the internet user the French localized version of the search engine. Geographic adjustments of search results based on the IP address of the user are relatively easy for users to avoid. If they take affirmative steps, users can obtain access to another version of the search engine. However, only a small percentage of users actually do this.

More drastic geographic restrictions can be implemented, but those generally involve more intrusive and disproportionate measures that violate international law. For example a regulator might want to impose on the search engine a change to its worldwide search results, a measure that would have the effect of extending the enforcement of the country's content policy to worldwide users of the search engine. For example, content that violates a content policy in Turkey would also be delisted for users in the United States or France. Another option would be to ensure that all internet traffic transits through a single gateway, making circumvention of the localized version of the search engine impossible. This technique is used in certain totalitarian countries. We see from this example that the range of actions is quite broad, going from relatively light touch measures to measures that have a strong adverse effect on freedom of expression worldwide. These adverse effects must be included in the cost-benefit analysis that I present in Chapter 6.

5.2 Hosting providers

Hosting providers contract with providers of content to make their content available on the internet. Hosting providers constitute the entry point for content onto the internet and are the closest link to the person publishing the content. The notice and takedown rules that exist under United States and European law were drafted with hosting providers in mind. Once a hosting provider takes down content, the content is in theory eliminated at its

source. In most cases, the hosting provider has a contractual relationship with the original publisher of the content and can therefore inform the publisher about the takedown request and seek the publisher's comments. The hosting provider is the internet intermediary located closest to the source of the illegal content, and has in theory a direct contractual link with the content's publisher.

This simplified image of hosting providers and of takedown mechanisms is complicated by several factors. First, content that is eliminated at its source by the hosting provider may still exist on other caching servers belonging to other internet intermediaries. In theory, operators of caching servers are supposed to verify continuously that the source content is still present on the original hosting server and should eliminate content that has been removed from the original host. In practice, however, many caching servers will retain copies of the original content long after the source copy has been eliminated. The second complicating factor is that the notice and takedown rules that regulate how and when hosting providers eliminate undesirable content are not universally applied. Publishers of undesirable content will often use the services of a hosting provider located in a country that does not have notice and takedown rules, or in a country that has such rules, but doesn't enforce them.

Many social media platforms are considered hosting providers and therefore apply notice and takedown rules with respect to the content posted by users. The notice and takedown rules imposed by law will often be supplemented by contractual terms of use imposed by the platforms on their users. Under its terms of use, the hosting provider may proactively screen for certain kinds of undesirable content or remove undesirable content (eg. nudity) upon receipt of a complaint. The terms of use may expand the notion of undesirable content to include content that is not necessarily illegal but that violates the acceptable use policy of the service, *e.g.* nude or degrading photos. This self-regulatory aspect of hosting providers will be examined in Chapter 4.

5.3 Internet access providers

The internet access provider ("IAP") is the telecommunication provider that connects end-users, and provides them with access to the internet.

The internet access provider is generally the subscriber's cable operator, mobile operator, or copper or fiber telecom operator. In sparsely populated areas, a satellite operator may be the IAP. When an internet user connects to the internet through his or her employer or school, the internet access provider may be the employer or school. For example, university students may connect to the internet using the university network; government employees may connect to the internet using the government network. The university or government network will be deemed the IAP in those cases.

Internet access providers routinely analyze and filter internet traffic in order to protect the network and their users from harmful viruses and other cyber security threats. Some corporate, government and university networks also block access to certain undesirable content, such as pornography sites or peer-to-peer services. However, beyond this, internet access providers generally do not take measures to voluntarily block content unless they are required to do so by a court or government order. What internet access providers may or may not filter, and on what basis, are highly contentious issues. They go to the heart of the net neutrality debate.

The net neutrality debate has two aspects. The first aspect is whether an internet access provider may block or slow traffic for its own commercial or competitive purposes. The second is whether an internet access provider may block or slow traffic for public policy reasons. Most of the net neutrality debate has focused on the first aspect, *ie*. whether an internet access provider can charge a premium to certain content providers in order to give them higher quality service, while leaving other content providers with a slower service. As regards the second aspect of the net neutrality debate, most commentators believe that IAP blocking for public policy reasons should be conducted with extreme care and only after a court decision. The reason for this caution is that any action by an internet access provider would create a number of undesirable spillover effects that would harm individual users' freedom of access to information, as well as the proper functioning of the internet. Because of these negative externalities, blocking measures should therefore be decided by a court.

internet access providers are technically *able* to limit subscribers' access to certain content. However, the technical tools used to accomplish blocking are imperfect. One mechanism consists of interfering with the internet address lookup function on the DNS server. The internet access provider alters the data on its own DNS server so that the DNS server provides wrong address information for certain domain names, making it impossible for the user to reach the desired site. Critics view this form of DNS blocking as a dangerous form of tinkering with the internet's universal addressing system. It is a technique used by hackers for "man in the middle" attacks.

Internet access providers may also block access to certain IP addresses. The problem here is that a given IP address may be shared by many content providers. Consequently, using an IP address as a means to block access to content creates a risk of blocking access to large amounts of other perfectly legal content.

Internet access providers are also able to apply deep packet inspection (DPI) to identify with precision certain undesirable content and then either block the content or slow it down. This form of filtering creates a significant risk for individuals' right to privacy. Deep packet inspection tools of this kind may be used by internet access providers to identify

cybersecurity threats. DPI may also be used in totalitarian countries to spy on individuals' internet use and identify political opponents. Deep packet inspection also creates technical challenges: DPI may slow down the network and/or be costly to deploy.

Internet access providers may also apply more "light touch" measures, such as sending warning notices to certain internet users who repeatedly download copyrighted content without permission. The internet access provider may also provide the identity of the subscriber to administrative authorities, who may send warning notices to the subscriber, or even apply sanctions. This is how "graduated response" mechanisms work, which are designed to discourage users from violating copyright law.

Internet access providers also respond to law enforcement and court requests to provide information on the identity of the subscriber, and on the internet sites accessed by the user. In this way, they contribute to law enforcement efforts to punish the authors of undesirable content, but do not intervene directly in blocking content.

5.4 Internet domain name registrar

The management of the internet's addressing system is delegated to a limited number of organizations in the world. For example, the United States corporation VeriSign manages the addressing system for all domain names that end in .com, .gov, .net or .org. The French organization AFNIC manages the addressing system for domain names that end in .fr. These organizations maintain the central database that permits a given domain name to be associated with a particular IP address. The central database is like a central phone book that is then replicated at a local level around the world so that each internet access provider and each internet backbone provider has the same phone thesis in its own DNS servers.

By altering the central database entry for a given domain name, an internet addressing authority can send false address information to local DNS servers around the world. This can have the effect of blocking access to a given website at a global level. This is what occurred when the United States Department of Justice seized the domain name Megaupload.com. The United States government took possession of the domain name as if it were a physical object located in the United States, and required that VeriSign change the IP address associated with that domain name. This changed the address data in the central database and the false address information was then replicated in the DNS servers around the world. The effect was that anyone attempting to connect to the Megaupload.com site was rerouted to a web page created by the United States Department of Justice.

Publishers of illegal content can quickly set up new sites, with new addresses, and avoid the effect of these kinds of blocking measures. The DNS blocking must be constantly updated to be effective.

5.5 Payment service providers

Some of the most serious forms of illegal content on the internet (*eg.* Illegal drugs) involve payment by end users. Because payment cannot be made in cash on the internet, sellers of illegal content must rely on payment service providers. Payment service providers are regulated, and rely on the international banking system. Where providers of payment services refuse to provide service to sellers of illegal content and services, this can contribute to drying up their source of funds.

Certain new payment services are not regulated and do not depend on the international banking system. Peer-to-peer payment services, such as Bitcoin, are decentralized and can be used even in cases where legitimate payment service providers refuse to do business with the relevant merchant.

Using payment service providers as a proxy to limit access to illegal content and services only functions for paying content. Free content is not affected. Moreover, new payment technologies allow users and merchants to effect payments without relying on the services of traditional payment networks. This can reduce the effectiveness of using payment service providers as enforcers of content policies. Nevertheless, payment service providers often voluntarily agree to discontinue service to sites that are manifestly illegal. This is referred to as the "follow the money" approach to fighting illegal content. The actions of payment providers generally result from non-binding charters or MOUs (Memoranda of Understanding). Non-binding charters and MOUs are part of what I call "multilateral self-regulation" in Chapter 4.

5.6 Internet advertising networks

Some websites offer illegal content for free, relying on advertising revenues from third-party advertisers to fund the site. To earn money from advertising, a website generally must use the services of one or more internet advertising networks. Those networks act as intermediaries between the website and third-party advertisers. Most mainstream brands do not want to be associated with undesirable content and will instruct ad networks to avoid them. Conversely, some advertisers may actively seek out this kind of content and be happy to place advertising on illegal websites. For example, an advertiser for online gambling may want to advertise its services on other gambling sites, including illegal ones.

Internet advertising networks are able to stop doing business with certain websites, which has the effect of reducing the websites' ability to monetize advertising space. The

effectiveness of this measure may be limited by the fact that alternative advertising networks can easily emerge to serve the market. Unlike payment service providers, which in theory are regulated, internet advertising service providers are unregulated, and barriers to entry are low. As part of "follow the money" initiatives, major advertising intermediaries undertake to cease providing service to sites that propose manifestly illegal content. As is the case with payment providers, these initiatives are generally part of non-binding charters or MOUs.

5.7 Application stores

Application (or "app") stores are centralized platforms that permit publishers of applications to present their applications for download to end-users. The application stores publish guidelines that application publishers must comply with in order to make their application available on the platform. Not surprisingly, the application stores prohibit applications that provide illegal content or services. Although each application is not individually reviewed by the operator of the app store, once the application store receives complaints it will evaluate the relevant application and eliminate it from the platform if it does not comply with the app store's guidelines. In this respect the application store resembles a hosting provider, acting pursuit to a "notice and takedown" procedure.

5.8 Content delivery networks (CDNs)

Content delivery networks provide services to providers of bandwidth-intensive content such as video in order to improve the quality perceived by end-users. Typically a content delivery network will transport content to caching servers that are located near the internet access network of the end-user. When the end-user requests a given video, the request is rerouted to a server located near the end users' internet access provider, thereby reducing the distance and number of network hops required.

Before it was shut down by the United States Department of Justice, Megaupload.com used the services of a large content delivery network to enhance the quality of service to end-users. So far, content delivery networks have not been visibly involved in limiting access to undesirable content.

5.9 Internet backbone providers

Internet backbone providers carry traffic between the upstream internet access provider serving the hosting provider that hosts the content and the downstream internet access provider serving the end-user. These internet backbone providers are interconnected with each other through transit and peering agreements. The interconnection points between backbone providers handle huge amounts of data, making individual filtering difficult. Nevertheless, some totalitarian countries implement monitoring and filtering measures at large internet traffic exchange points. Intelligence agencies in democratic countries may

monitor data via infrastructure installed at the level of internet backbone providers. However, filtering is generally not implemented at large internet exchange points, at least in democratic countries.

Filtering at a centralized international gateway can make it difficult for end-users in the country to work around filtering at the DNS level. However, such filtering reduces the performance of the internet for users in the country, and transforms the local internet into a national network, interconnected with the internet at a centrally controlled choke-point.

5.10 End-user software

Software or apps on the end-user's terminal can help block harmful computer viruses. Parental control software can block access to adult websites. Ad blocking software can limit advertising. Privacy software can limit cookies and other tracking devices.

Putting access control features on end-user software has the advantage of not interfering with the normal operation of the internet. It also puts the end-user in control, and thereby reduces the risk of interfering with the user's fundamental rights. Relying on software in the user's terminal requires regular software updates, and thus may be less effective than more centralized filtering measures. Moreover, because the end-user is in control, the end-user can easily de-activate the system and obtain access to illegal, but desired, content. This may frustrate one of the objectives of policymakers, who want to make access to certain content difficult for users.

While in theory under the control of the end-user, end-user apps or software are also controlled, at least in part, by the software publisher. The software publisher may make choices by default. These default choices result in the blocking of certain content. Although users can in theory override the publisher's default settings, the default settings will in most cases remain untouched. The criteria used to set the default list of blocked content can be based on objective public interest criteria, or may in some cases be influenced by commercial or competitive considerations. For example, the ad-blocking software AdBlock Plus seeks payment from certain large content providers in order to be placed on AdBlock Plus's "Acceptable Ads" white list.[20] This sort of commercial negotiation with upstream content publishers is what defenders of net neutrality seek to prevent.

5.11 Set-top boxes or modems

Set-top boxes and modems are generally under the control of the internet access provider. The set-top boxes or modems may contain software installed by the internet access provider to regulate access to certain content. In some cases, the end-user will be provided an interface to modify default settings defined by the internet access

[20] https://adblockplus.org/about#monetization (consulted January 22, 2017)

provider. In other cases, the end-user will only be able to change the settings by changing his or her account with the internet access provider. The account parameters are then changed within the internet access provider's network and the update is pushed to the subscriber's set-up box or modem via a software update. The software in the set-top box and the modem are part of the internet access provider's network.

5.12 Device operating systems

The application programming interface (API) of device operating systems can contribute to the protection of end-users against harmful content. The operating systems will have measures to protect against cyber attacks that may result in the theft of end-user data or unauthorized surveillance. APIs are also used to force app developers to implement privacy-friendly policies. For example, the API will not allow the application to have access to the user's list of contacts without obtaining explicit user consent. The same rule may apply when an application seeks to access geolocation information within the device. Consequently, publishers of operating systems can build in mechanisms that help enforce content policies.

To date, most initiatives to limit access to harmful content have focused on notice and takedown at the hosting provider level. "Follow the money" self-regulatory initiatives are frequent, as are court-ordered blocking by IAPs at the DNS server. Search engines are also becoming popular targets, as was demonstrated by the recent "right to be forgotten" cases.

The purpose of this list is to highlight the wide range of technical intermediaries and actions that regulators may consider when approaching a problem relating to access to harmful content. The methodology I propose in Chapter 6 requires the drafters of the impact assessment to list all the potential internet intermediaries that might contribute to enforcing the content policy, so that no alternatives are overlooked.

6. THE INSTITUTIONAL FRAMEWORK

By institutional framework, I mean the legal rules and institutions that provide the context in which an internet intermediary may act to enforce a content policy. For example, in a purely self-regulatory framework, the underlying legal rules will be contract law and liability rules applicable to internet intermediaries. The institutions will be courts evaluating internet intermediary behaviour after the fact. It is on this institutional framework that an internet intermediary will build its self-regulatory program, *via* its contractual terms of use and an evaluation of potential liability in different scenarios.

In a government-administered regulatory framework, the underlying legal rules will be the regulations adopted by the legislature and the regulatory authority; the institutions will be the regulatory authority and the courts.

The point here is that internet intermediary actions never occur in a vacuum. They will always arise in the context of an institutional framework of some kind. Even self-regulatory measures are part of an institutional environment consisting of liability and property laws enforced by courts. The choice of the institutional framework will affect the costs and benefits accompanying the relevant measure. A well-crafted institutional framework will permit the enforcement mechanism to achieve its intended result more effectively while minimizing adverse effects on fundamental rights. By contrast, a poorly-crafted framework may cause the measure to miss its intended mark, and/or aggravate harm to other rights.

The institutional framework is closely related to the question of the ideal law enforcement strategy, a question I alluded to briefly in Section 4 of this Chapter. For example, general liability rules will generally be more efficient when the victim is able to identify the person responsible for the harm and enforce a damages award against him or her (Shavell, 1984). By contrast, where the perpetrator of the harm is difficult to identify or is likely to not have assets sufficient to pay for the harm, then regulation will in most cases be more efficient than liability rules. As expressed by Shavell (1984),

> *"the measure of social welfare is assumed to equal the benefits parties derive from engaging in their activities, less the sum of the costs of precautions, the harms done, and the administrative expenses associated with the means of social control. The formal problem is to employ the means of control to maximize the measure of welfare."* (Shavell, 1984, p. 359).

In this thesis, the "institutional framework" corresponds to Shavell's "means of social control", *ie*. the combination of legal rules and institutions that form the backdrop for internet intermediary action.

Various institutional choices will be examined in Chapter 4. The methodology proposed in Chapter 6 requires that various institutional frameworks be considered, and that the costs of each alternative be taken into account in the cost-benefit analysis.

7. NEGATIVE EXTERNALITIES CAUSED BY INTERNET INTERMEDIARY ACTIONS

The effectiveness of any measure taken by an internet intermediary can be measured in the first instance by comparing the cost of implementing the measure with the measure's success in enforcing the relevant content policy. (Measuring "success" in enforcing a content policy is a complex question in its own right, which I will examine in Chapter 6.) If an internet intermediary can cheaply implement a measure that has a 99% success rate in enforcing the relevant content policy (*eg*. prohibiting access to online child pornography), the measure would appear at first glance worthwhile. In reality, the calculation is more complex because most measures undertaken by internet intermediaries can create negative externalities, *ie*. costs to society that are not internalized by the internet intermediary and its customer. The costs of these negative

externalities may be much higher than the direct costs of the measure to the internet intermediary, and may also outweigh the anticipated benefits flowing from enforcement of the relevant content policy. When these negative externalities are considered, the relevant measure may prove to do more harm than good.

Many of the costs associated with the negative externalities examined below are difficult to measure in monetary terms. The monetary value associated with harm to freedom of expression or privacy, for example, can be estimated only through use of artificial and contestable assumptions. As I will show in Chapters 3 and 6, various methods can be used to measure hard-to-quantify benefits and costs. For example, a scoring mechanism was proposed by Alexy (2012), and is currently used in a European Commission – funded research project called SURVEILLE, which is intended, among other things, to measure the impact that certain police surveillance and investigation techniques have on fundamental rights.

The approaches I propose in Chapter 6 will permit policymakers to compare different approaches and their relative impact on fundamental rights, innovation and net neutrality. The methodology is designed to identify the approach that appears, based on the scoring systems, to maximize social benefits net of the costs.

Listed below are the main negative externalities that might arise from the action of an internet intermediary.

7.1 Adverse effects on fundamental rights

The first series of negative externalities relates to the impact on fundamental rights. The effects on fundamental rights, and how to balance competing fundamental rights, will be examined in detail in Chapter 3. The list below is an introduction to the subject.

(a) Freedom of expression.

Any action limiting access to content on the internet is a restriction on freedom of expression of the publisher of the content, and a restriction of the right to access information for the recipient of the content. The right for individuals to publish or access information is not absolute. Some content may be prohibited. But the limits on freedom of expression must be precisely defined by law and must be limited to what is absolutely necessary to achieve other important values in a democratic society. Freedom of expression is considered one of the most important individual rights in democratic society because it is a precondition for the exercise of other rights. The exchange of valuable political ideas is considered a public good, requiring government intervention to ensure sufficient production. For this reason, courts show a low tolerance for any measure undertaken by an internet intermediary that might be overbroad, *ie*. contain false positives that interfere with access to legitimate information. For example, if a technical measure designed to block images of sexual exploitation of children also accidentally blocks works

of art containing child nudity, or images from a medical journal, courts will in most cases find that the measure's adverse effects on freedom of expression outweigh the benefits derived from blocking child pornography. When an internet intermediary blocks content, the costs associated with the harm to freedom of expression will generally not be internalized by the intermediary and its customers. The harms are therefore externalities.

(b) Right of privacy.

The right to privacy and to the protection of personal data is a constitutional right in Europe. In the United States, the constitutional right to privacy is recognized, but only vis-à-vis actions taken by the government against the individual. Actions taken by private entities are covered by other legal provisions, including tort law and consumer protection law.

The right to privacy and the right to protection of personal data are not identical. The right to privacy generally refers to the right of each individual to keep aspects of his or her private life secret. The right to protection of personal data refers to the right of each individual to control how data about him or her are used, and to object to improper uses. Because the two rights overlap in many instances, I use the terms "privacy" and "data protection" interchangeably, to designate the bundle of rights that protect individuals against intrusions into their private life and/or misuse of their personal data.

Measures taken by internet intermediaries may have an impact on individual rights to privacy. Like freedom of expression, the right to privacy is not an absolute right and may be balanced against other rights. The balancing will involve a proportionality test that I will explore in Chapter 3. Some authors (Alexy, 2012, Portuese, 2013) explain that proportionality is a form of cost-benefit test. Because privacy is a fundamental right, courts will attach a high cost to any measure that poses a threat to privacy. The measure will have to be justified by important countervailing benefits in order to pass the proportionality test. In Europe, courts have criticized actions taken by internet intermediaries to stop copyright infringement on the ground that those measures create a threat to privacy. Where national security is at stake, courts may allow more intrusions into privacy than would be permitted to fight copyright infringement. In other words, the level of permitted interference with privacy may depend on the underlying content policy that is being pursued. Privacy rights can directly conflict with freedom of expression, as in the case of the so-called "right to be forgotten" under European law. The friction between the right to privacy and freedom of expression will have to be balanced on a case-by-case basis.

(c) The right to property.

The right to property is a constitutionally-protected right, meaning that actions taken by internet intermediaries to protect property interests (such as copyright) enhance a fundamental right. This aspect of internet intermediary action, protection of the right to property, will generally be counted as a benefit in the cost-benefit analysis. On the "cost" side, property rights may be infringed where a government seizes a domain name, as the United States Department of Justice did in its action against Megaupload.com.

(d) The right to create and operate a business.

European courts have also recognized the right to create and operate a business as a fundamental right. Where a government imposes measures on a particular business, such as the installation and operation of filtering equipment, or restrictions on a business model, the government interferes with the business-owner's fundamental right to operate a business. The same holds true for regulations that limit the use of advertising cookies. This interference therefore also needs to be considered in the overall costs created by the measure.

(e) The right to procedural fairness.

In both Europe and the United States individuals are entitled to procedural guarantees before being deprived by the state of any fundamental rights, including the right to free expression, property or liberty. Any measure taken by an internet intermediary that leads to a deprivation of a right, or the application of a sanction, may violate individuals' rights to procedural fairness.

The institutional safeguards accompanying any internet intermediary action, examined in Chapter 4, will in some cases mitigate the effects of internet intermediary action, by providing internet users or content providers with an opportunity to object.

7.2 Internet-specific harms

In addition to potential harms to fundamental rights, measures taken by internet intermediaries may cause other forms of negative externalities, including harm to the proper functioning of the internet, and to innovation.

(a) Harm to the good functioning of the internet.

The internet is built to avoid control points. Packets are routed through different networks and interconnection points so as to avoid congestion or blockage. Once all the packets reach their destination, they are reassembled. The content of the packets is then analyzed and the appropriate application run on the end-user's device. The network has a relatively simple routing function. Most of the intelligence for internet applications is provided by terminal devices at the edges of the network, once the packets are

reassembled at their destination. Defenders of net neutrality argue that internet access providers and internet backbone providers (collectively "ISPs") should limit their role to routing packets on a non-discriminatory basis. They should not be concerned with the content, application or services that are located inside the packets. This is referred to as the end-to-end principle of the internet. Defenders of net neutrality recognize an exception to this end-to-end principle for ISP measures to fight malware and other cyber security attacks. For other content and services, however, defenders of net neutrality believe that ISPs should remain neutral, and limit their actions to routing packets to the right destination.

One of the reasons neutrality is important is that actions by internet intermediaries could threaten the principles under which the internet has successfully functioned to date. According to net neutrality advocates, even small instances of non-neutrality should be resisted because each measure sends the message that it is okay to interfere with the end-to-end architecture of the internet. This could lead to the gradual destruction of the internet: ISPs and governments will engage in an arms race to erect barriers that will let only certain kinds of content and applications pass. To reach consumers in a given country, content providers would potentially have to negotiate with both the government and the ISPs in the country to obtain a right of passage. In regulatory terms, this would be the equivalent of seeking a broadcasting license in each country where the content is accessible. This is the nightmare scenario that proponents of net neutrality want to avoid, and which could lead to a progressive balkanization of the internet.

Some advocates of net neutrality have a tendency to exaggerate. But their arguments contain a good dose of truth. For example, when the United States Department of Justice seized the domain name Megaupload.com and altered the address corresponding to that domain name on the central DNS server of VeriSign, United States authorities disrupted the global addressing system for the internet. They may have had a good reason for doing so, but one can understand why opponents of net neutrality fear that this sort of action could set an example for other countries and internet intermediaries. The Department of Justice's action sends the message that it is no longer taboo to disrupt the global addressing system for the internet to enforce national content policies. ISPs, governments and courts may begin to take their own form of action to disrupt the addressing function or block IP addresses to promote local content policies. If this action becomes widespread, the internet will become a series of national networks with separate control points and content rules for each country.

The French data protection authority wants to ensure that the "right to be forgotten" as defined under French law is enforced by search engines worldwide, again creating a precedent for extraterritorial application of national content policies.

Preservation of the open internet is not important for its own sake, but rather to promote freedom of expression and innovation, both of which are enabled by the internet's open and global architecture. The open internet is therefore a proxy for other values and potential harms that need to be considered. The harm to freedom of expression was examined above. In the following section I touch briefly on harm to innovation.

(b) Harm to innovation.

The layered and end-to-end architecture of the internet is a strong enabler of innovation. Yochai Benkler (2006) states that the open internet permits "innovation without permission." If actions by internet intermediaries interfere with the open and end-to-end character of the internet, these actions could also disrupt innovation. Measuring harm to innovation is difficult. It would require the comparison of two situations: one in which a content and application provider must deal with separate content policies and enforcement actions by internet intermediaries, and another situation in which internet intermediaries refrain from any enforcement action linked to content policies. The amount of investment in content and application development would then be compared for these two situations. Organizing an experiment of this kind would be difficult, particularly because one could not neutralize other factors potentially affecting innovation, such as the availability of venture capital. Measuring the open internet's positive effect on innovation is beyond the scope of this thesis. Nevertheless, most scholars agree that the internet's openness has made the internet a general purpose infrastructure, which in turn enables innovation. Some of the relevant literature on regulation's effect on innovation is mentioned in Chapter 5.

As is the case for harm to fundamental rights, I will propose in Chapter 6 methods to measure the relative harm to innovation resulting from alternative regulatory proposals.

7.3 Unintended effects linked to user behavior

Enforcement action by internet intermediaries can prompt users to change their behavior in a way that reduces the intended benefits of the measure, or frustrates another important policy objective. This creates unanticipated costs. For example, a measure designed to reduce peer-to-peer exchanges of copyright-protected content might have two unintended effects. First, the measure may cause internet users to adopt other alternative technologies for content sharing such as streaming or direct download, thereby reducing the anticipated benefit of the original measure. Second, the measure may prompt larger numbers of internet users to use encryption and "dark networks" such as Thor. This phenomenon may in turn frustrate law enforcement efforts to combat crimes much more serious than copyright infringement, thereby creating new unanticipated costs.

As this example shows, technology and user behavior will often find ways to work around measures imposed by internet intermediaries. These work-arounds may create their own kinds of costs that should be considered when evaluating the costs and benefits of a particular enforcement measure.

7.4 International effects

Indirect costs should also include costs resulting from international effects, if any. If the proposed measure will affect individuals or businesses in other countries, the potential costs of this extraterritorial effect should be weighed. Katz (2000) refers to "jurisdictional externalities." Other countries may retaliate, through enactment of their own measures having extraterritorial effect. This could create a "race to the bottom" pursuant to which countries impose their own measures on internet intermediaries regardless of their extraterritorial effect.

Another cost to consider is the competitive distortion potentially resulting from certain intermediaries within the country being subject to regulatory measures while other intermediaries located outside the country are not. If the intermediaries outside the country compete for the same customers, this would create a competitive distortion penalizing intermediaries located within the country. This in turn could discourage investment in the relevant country, another potential negative externality flowing from actions of an internet intermediary.

8. SOLVING THE PROBLEM SO AS TO MAXIMIZING SOCIAL BENEFITS

To summarize, the relevant factors that policymakers must consider in the cost-benefit analysis are:

A. the kind of content policy to be enforced, its relative importance in terms of society's willingness to pay, and how "success" in enforcing the content policy should be defined;

B. the kind of internet intermediary that could be called on to help;

C. the kind of action that the internet intermediary could take, and its relative efficacy;

D. the institutional options available to increase effectiveness of the measure and reduce its adverse effects;

E. direct costs associated with the proposed measure in terms of direct costs to the internet intermediary and its customers, and costs to taxpayers, including costs of enforcement;

F. the negative externalities associated with the harms to fundamental rights, including freedom of expression and privacy;

G. the negative externalities associated with harms to the global end-to-end architecture of the internet and innovation;

H. changes to user behavior that might reduce the efficacy of the measure or create unanticipated costs.

In mathematical terms, the problem is to find the maximum net social benefit, ie. the combination of B, C and D that maximizes the sum of A (the benefits flowing from the enforcement of the content policy), minus the costs resulting from E, F, G and H. Solving the problem is challenging because A, F, G and H are qualitative, and to some extent subjective, values, which makes them difficult to measure and to compare. The purpose of my methodology is to propose a uniform way of thinking about these variables so as to approach – albeit imperfectly -- an outcome that would result if the variables were quantifiable in a more objective sense.

I present the system in Chapter 6. However, first I will present how benefits and costs to fundamental rights should be considered (Chapter 3), how institutional choices affect the costs and benefits of regulatory alternatives (Chapter 4), and how existing literature on "better regulation" affects how we approach the problem (Chapter 5).

CHAPTER 3 - BALANCING FUNDAMENTAL RIGHTS

1. INTRODUCTION

Many content policies protect fundamental rights. Laws prohibiting online copyright infringement protect the right to property, a fundamental right. Laws requiring search engines to delist certain old and irrelevant content under the "right to be forgotten" doctrine protect data privacy, a fundamental right. But those laws also restrict freedom of expression, which is also a fundamental right. Laws prohibiting content that incites racial hatred protect equality and non-discrimination, a fundamental right. When internet intermediaries take actions to enforce content policies, the actions will often favor one right at the expense of others. This requires balancing.

Courts in the United States and in Europe do this balancing routinely. In Europe, the balancing is known as the "proportionality test." The purpose of this chapter is to look at the rights that are being balanced through the lens of law and economics, as well as to examine the balancing test itself. The proportionality test examined at the end of the chapter is a form of cost-benefit analysis, even though the costs and benefits associated with fundamental rights can rarely be quantified in monetary terms. This chapter will lay the groundwork for Chapter 6, where the balancing of fundamental rights will be inserted into the methodology used to evaluate proposed regulatory measures. I will propose in Chapter 6 several mechanisms for measuring impacts to fundamental rights, including a scoring mechanism inspired by Robert Alexy (2012), examined in Section 5.7 of this chapter.

2. WHAT ARE FUNDAMENTAL RIGHTS?

2.1 Characteristics of fundamental rights

Most fundamental rights come from the philosophers of the enlightenment, who defined certain natural rights from which all human beings should benefit (Ségur, 2012). These principles first appeared in the French Universal Declaration of Human and Citizens' Rights and the United States' Bill of Rights, both adopted in 1789. After World War II, the United Nations adopted its Universal Declaration of Human Rights (December 10, 1948), and the Council of Europe adopted the European Convention on Human Rights (November 4, 1950). More recently, the European Union adopted its Charter of Fundamental Rights (December 7, 2000), which became binding on all European Member States under the Lisbon Treaty (2009).

From an economic standpoint, fundamental rights can be approached based on their characteristics.

The first characteristic is that fundamental rights arise under a legal instrument, such as a constitution, that is difficult to change (Posner 2011). Fundamental rights generally arise from a constitution, or an international treaty having a status equivalent to a constitution.

In the hierarchy of legal instruments, a constitution is at the top of the food chain. A constitution is more difficult to modify than a law. A law can be changed through consent of the government and a simple majority in the legislature. A constitution can be modified only with a supermajority vote of both houses of the legislature, plus other conditions that vary depending on the country. Because of these more stringent conditions, constitutions are difficult to modify, even by the ruling majority. Posner (2011) compares a constitution to a contract, which can only be modified with the consent of all the relevant parties. In other words, fundamental rights are legal rules that are very costly to modify, at least in a properly-functioning democracy.

The second characteristic of fundamental rights is that they are designed to constrain the actions of the respective branches of government, including the actions of the legislature itself. The constitution protects citizens against pitfalls of democracy, including abuses of the majority. Certain laws democratically adopted by the legislature could undermine the structure or ideals on which the nation is built. Constitutional rights are designed to prevent this from happening, or at least make it considerably more difficult. This aspect of fundamental rights can be compared to laws that restrain monopoly power, except that in the case of fundamental rights, the monopoly power is the power of the state. Posner (2011) calls the state the "most dangerous" monopoly. Many constitutional provisions protect individuals against actions of the state, including all its branches (government agencies, regulatory authorities, legislature or court). Monopoly power in the private sector can be constrained by antitrust laws voted by the legislature and government enforcement of these laws. Monopoly power of the state cannot be so constrained, because the persons who adopt and enforce laws are also the ones who benefit from the monopoly power. This creates a conflict of interest problem, which is why most fundamental rights protect citizens against actions of the state, as opposed to actions by other citizens. Citizens are protected against actions taken by other citizens through ordinary laws, adopted by majority vote of the legislature and enforced by the government and courts. Citizens are protected against actions taken by the state through constitutional rights. This is an oversimplification. In some cases, a fundamental right can be enforced against other individuals. For example, the right to privacy is a fundamental right recognized under the European Charter of Fundamental Rights. It requires that countries have legal mechanisms in place to allow individuals to assert their right to privacy against other individuals. The same holds true for the right to property: the state must have legal mechanisms in place to allow individuals to assert their property rights against the state and against other individuals. If a European Member State does not have those mechanisms in place, the state has violated a fundamental right. Nevertheless, it is fair to say that the primary function of fundamental rights is to protect individuals against actions of the state, including abuses of the then-governing political majority.

A third characteristic of fundamental rights is that they are generally framed as general principles, not as detailed rules. This characteristic flows from the first: if fundamental rights arise from legal instruments that are difficult to change, the rights must be drafted so that they can stand the test of time. Courts must apply rights to different circumstances; rights must survive social and technological change. Rights may also transcend geography. This is why rights are sometimes called "universal." This characteristic of fundamental right is also shared by many "ordinary" laws, which are drafted as general principles. This characteristic is therefore not unique to fundamental rights.

The last characteristic of fundamental rights is that they generally have achieved historical and international legitimacy. A fundamental right is generally not found in just one country's constitution, but in many countries' constitutions and international treaties. A fundamental right generally flows from the core values originally identified in the United States Bill of Rights and the French Universal Declaration of Human Rights of 1789. Fundamental rights share the same family tree. A country could conceivably invent a new constitutional right, such as the right for all citizens to have broadband access. Being placed in the country's constitution, the new right could arguably be considered a "fundamental right" in that country. However, in the absence of any international or historical legitimacy, the new right would probably be considered – outside the relevant country at least -- as a legal rule lacking the status of a "fundamental" right. Once the new right is recognized in several constitutions and/or in an international treaty on fundamental rights, the new right may achieve the status of a "fundamental right" internationally.

2.2 The cost of fundamental rights

Economists focus on the costs and benefits of fundamental rights. Fundamental rights are sometimes classified as "negative" or "positive" rights (de Vries, 2013). A negative right is the right to be free from action of the state, such as confiscation by the state of property without compensation. A positive right is the right to receive some benefit from the state, such as the right to receive health care. Holmes and Sunstein (1999) argue that all rights – including so-called negative rights -- require expenditures by the state. No right, including a negative right, exists without an effective enforcement mechanism, which costs money. A right to private property does not exist if there is no court system to recognize the right, and no police force available to enforce the courts' decisions. Enforcement mechanisms require state expenditures. Thus every right, whether positive or negative, can be seen as a competing claim against limited government resources. The allocation of scarce tax resources is generally determined by the legislature, by simple majority vote. A fundamental right may therefore exist in a country's constitution but become ineffective if the legislature fails to devote sufficient resources to the right's enforcement.

For example, a country may include data protection as a fundamental right in its constitution. But if the legislature of the country does not grant sufficient resources to the data protection authority, the fundamental right may have little existence in practice.

The absence of corruption is also a precondition for effective rights to exist. A fundamental right that exists on paper may dry up in practice if the financing for its enforcement is insufficient, or if the financing comes in part from graft. Fundamental rights therefore depend on taxes and on an efficient distribution of tax resources to non-corrupt courts and police authorities.

2.3 Economic vs. non-economic rights

Fundamental rights are sometimes classified as "economic" and "non-economic" rights (de Vries, 2013). An example of an economic right is the right to conduct a business, or the right to protection of property. An example of a non-economic right is the right not to be tortured, or the right to freedom of expression. The distinction between economic and non-economic rights does not necessarily render one of the rights inferior to others, but will affect the balancing tests applied by courts. Some rights, such as the right not to be tortured, are absolute and can suffer no exceptions. Most rights, however, including non-economic rights such as freedom of expression and privacy, can be restricted based on a balancing test.

Finally, certain international instruments contain two kinds of fundamental rights: rights that are directly binding, and aspirational principles that are not directly binding (De Vries, 2013). Article 25 of the European Charter on Fundamental Rights provides an example of an aspirational principle: "The Union recognises and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life." Being aspirational, this right could not be directly enforced by an individual against the state.

2.4 The expressive value of fundamental rights

Fundamental rights often have a symbolic function intended to influence social norms (Sunstein 1996). At one level, the statement "everyone is equal before the law"[21] signifies that the state may not make different laws or punishments for different people. This literal reading of the statement constrains government behavior by limiting the kind of law that the legislature can adopt. This function aims to limit abuse of government monopoly, which is the primary objective of fundamental rights.

On another level, the statement that "everyone is equal" has a larger symbolic meaning intended to send a message to society that discrimination is wrong. It attempts to push social norms in the right direction. In this sense, fundamental rights can have a strong moral component, or as Sunstein (1996) puts it, an "expressive function." The moral

[21] Article 20, European Charter on Fundamental Rights

component can, but does not necessarily, mean that the relevant right is absolute and cannot be balanced. Some rights with a high moral component, such as the right to life[22], are absolute. But other rights, such as freedom of expression and privacy, carry a strong moral component, but can nevertheless be balanced.

The expressive or moral component of fundamental rights also leads to debates as to whether fundamental rights can be integrated into a broader welfare analysis in which the objective is to maximize social welfare. Nussbaum (2000) argues that the function of rights is to preserve values that are different from the maximization of wealth typically reflected in a welfare analysis, and that violations of constitutional rights cannot be traded for benefits. Kaplan and Shavell (2006) argue on the other hand that a welfare-based approach is perfectly capable of capturing values other than maximization of wealth in a monetary sense. Welfare economics seeks to make everyone better off, and making people better off includes various indicia of happiness, including the existence and enforcement of individual rights. While these factors for happiness are difficult to quantify in a monetary sense, there is nothing inherently incompatible between an approach that seeks to maximize collective wellbeing and an approach that recognizes individual rights, including their moral or expressive component.

In an article examining enforcement of national content policies on the internet, Schultz (2008) refers to the normative role of laws, and the important social role played by court or regulatory decisions that declare certain forms of content unacceptable. The actual efficacy of the decision in preventing access to content may, in some cases, be secondary:

> *"Brutally simplified, it is one of law's functions to say what, according to the law governing and tying together a nation, is right or wrong; without necessarily punishing as a consequence."* (Schultz, 2008, p.822)

Focusing on the symbolic importance of regulatory decisions, particularly those upholding fundamental rights, can lead courts and regulators to ignore questions linked to the efficacy of their decisions in reducing a particular harm, and to the costs associated with implementing their decisions.

Fortunately, the doctrine of proportionality, examined in Section 5 below, requires regulators also to take into account the costs and benefits of their decisions, thereby bringing welfare analysis back into the equation.

---

[22] Article 2, European Charter on Fundamental Rights

3. FREEDOM OF EXPRESSION

This section takes a closer look at freedom of expression, which is the fundamental right that is the most affected by regulatory measures targeting internet intermediaries.

3.1 General limitations to freedom of expression

Although a fundamental right, freedom of expression is not absolute, and is routinely limited by other laws. Copyright, for example, allows the owner of the copyright to prevent anyone else from reciting his or her poem publicly, or even adapting it to create a new derivative work. This is a direct restriction of freedom of expression. Laws punishing defamation directly restrict freedom of expression, as do laws prohibiting the unauthorized publication of personal data, trade secrets, medical secrets, banking secrets, or state secrets. The Wikileaks and Snowden controversies illustrate the tension between freedom of expression and laws prohibiting the publication of classified information.

Dozens of laws limit freedom of expression in democratic societies. The main difference between these laws and the laws in totalitarian regimes is that the laws in democratic societies will not prohibit the publication of content that is critical of a political party, government or religion. The ability to openly criticize government is the underlying reason why freedom of expression is given so much constitutional protection. Without the ability to openly criticize government, democracy cannot exist (Post, 1996).

In economic terms, freedom of expression preserves the "marketplace of ideas", from which socially optimal solutions and democratic governance emerge (Coase, 1974). Mialon and Rubin (2007) refer to freedom of the press and freedom of political speech as the "mother of all rights" because they are essential for creating and enforcing other rights. "If government violates a right but no one can learn of the violation, then there is no cost to the government for the violation." (Mialon and Rubin, 2007, p. 11).

Courts are therefore vigilant when it comes to measures that might have an adverse impact on freedom of expression, particularly when the measures affect the internet. The internet is considered one of the most important enablers of freedom of expression since the invention of the printing press (United Nations, 2011). In the 15th century, kings and clergy attempted to regulate printing presses in order to enforce content policies. The regulation of internet intermediaries is similar, which is why courts approach such measures with caution.

3.2 Is the internet like television?

This discussion is about regulating access to harmful content on the internet. A legitimate question is: Why not just apply the same rules as for television? After all, the problem of harmful content is similar, and television rules have been in existence for decades. The

answer to this question resides in how courts apply freedom of expression principles to these two media, internet and television.

When internet first emerged as a major media, lawmakers' first reaction was to apply television-like rules. In 1997 the United States Supreme Court invalidated a law that proposed to apply broadcast-like regulation to internet content. The measure was intended to protect children. In the now-famous *Reno v. ACLU* case[23], the Supreme Court found that the internet is equivalent to a tribune in a public square, where citizens can speak or distribute leaflets freely. The court disagreed with the United States Department of Justice, which argued that the internet could be regulated like television. The court found that unlike television, which "pushes" information to passive viewers in a living room, the internet requires users actively to seek out information, as they do when they enter a library. Unlike television or radio, internet users will generally not be shocked by the information they receive, since they are actively seeking the information to begin with.

The other reason why the court refused the broadcasting analogy in 1997 is that information on the internet is not limited, whereas information on television is limited due to the scarcity of radio frequencies. Because only a limited number of television broadcasters can be licensed to provide television or radio services, the government is justified in imposing content rules on the license holders. In sum, courts are more tolerant of government efforts to regulate television and radio because of (a) television and radio's higher influence on public opinion, and (b) the scarcity of broadcasting frequencies.[24] The scarcity argument may disappear, because television is increasingly carried over broadband networks. Nevertheless, it is still generally accepted in the United States that television can be regulated more aggressively than the internet without violating the First Amendment of the United States Constitution.

European courts have followed the trend set in *ACLU v. Reno*, by according a high degree of protection to expression on the internet, similar to the protection given to print media.[25] In Europe as well, television regulation cannot be transposed as-is to internet content.

3.3 The nature of harms to freedom of expression

When examining technical measures affecting internet intermediaries, courts have identified three different kinds of potential harms to freedom of expression. The first and most direct impact is on the publisher of information whose message becomes blocked and thereby inaccessible to internet users. This is the case for example of the publisher of

---

23 *Reno v. ACLU*, 521 U.S. 844 (1997).

24 *Red Lion Broadcasting v. FCC*, 395 U.S. 367 (1969). *See also* French Constitutional Court decision n° 82-141 DC of July 27, 1982, recital 5.

25 *Yildirim v. Turkey*, European Court of Human Rights decision n° 3111/10 of March 18, 2013; *see also*, French Constitutional Council decision n° 2009-580 DC of June 10, 2009, par. 12.

a controversial video, such as "The Innocence of Muslims," whose video becomes inaccessible to large numbers of people either because the video was taken down from YouTube, or because access to the video was blocked by an internet access provider. This is also the case for the author of an article that has been subject to a delisting request under Europe's "right to be forgotten" doctrine. In the latter case, the article will be more difficult to find using certain search terms.

The second more indirect harm to freedom of expression is when a technical measure is overbroad, and prevents an internet user from obtaining access not only to the information directly targeted by the measure (eg. material the infringes copyright or that violates laws on child pornography), but also to other information that is not directly targeted by the measure. A clear example of this is where access to the entire YouTube service is blocked in a country because of the presence of a single video that violates local law. However, even measures that are less obviously overbroad attract court scrutiny. A user's inability to obtain an unauthorized copy of a recent motion picture such as "Gravity" on the internet will not be considered a restriction on that user's freedom to access information on the internet because the access would violate copyright laws. However, if the system put into place to limit access to "Gravity" might also limit access to another film with the word "gravity" in the title, or a work that parodies "Gravity" but benefits from an exception to copyright, courts will view the measure as a potentially serious restriction to freedom of expression. The Supreme Court in the United States invalidated parts of the Communications Decency Act[26] because it was overbroad: the measure targeted "sexually explicit" content, but could limit minors' ability to search for information on birth control. The European Court of Justice invalidated a measure that might inadvertently block content that does not benefit from copyright protection.[27] Any measure that is slightly overboard will generally be struck down as an excessive restriction on freedom of expression.

The third and last potential harm identified by courts is the chilling effect that some measures may cause to freedom of expression by causing publishers and intermediaries to limit their activity, to become overly careful in what they say or publish. As explained below, critical and disturbing speech is considered a public good, necessary for the marketplace of ideas to function properly. Such speech may be under produced if not protected. Courts, particularly in the United States, are critical of legal rules that might constrain unpopular speech, even through indirect effects. These indirect effects are often referred to as "chilling effects."

Some laws require ISPs or hosting providers to collect information about the identity of publishers of content so that law enforcement authorities or victims of copyright

---

26 *Reno v. ACLU*, 521 U.S. 844 (1997).

27 *Scarlet Extended v. SABAM, ECJ, Case C-70/10, 24 November 2011*

infringement can identify the author of the content and bring legal action if the content proves illegal. These mechanisms may discourage publishers of controversial content from publishing the content in the first place, or may encourage them to publish on non-public platforms. By discouraging the publication of controversial content, the measure has the effect of weakening open criticism and the exchange of ideas. The concern here is not to protect publishers of manifestly illegal content, but publishers of content that is legal but that might be close to the line, or that could lead to adverse consequences for the author. For example the composer of a musical mash-up may not be 100% sure that her work falls under the fair use exception to copyright. The author of a video revealing unfavorable information about a large corporation may fear reprisal if his or her identity is known. The absence of anonymity creates a chilling effect on free expression.

The importance accorded to chilling effects is due to the fact that much speech and ideas are public goods (Posner, 2007, p. 727). As pointed out by Mialon and Rubin (2007):

> *"[a]nything that adds to the cost of speech will then have a large suppression effect, since many of the benefits of speech accrue to others anyway. This may be especially true of political speech. Political discourse and debate tend to produce better decisions for society, but individuals often have few incentives to participate, since they do not capture most of the benefits of their own participation and incur opportunity costs, as they could spend their time pursuing personal gain instead."* (Mialon and Rubin, 2007, p. 4)

3.4 Internet intermediary liability and free speech

Liability imposed on technical service providers is also a potential source of chilling effect, because such liability prompts ISPs and other technical intermediaries to reduce their potential costs by eliminating risky, albeit legal, content from their service (United Nations, 2011, p. 11).

Schruers (2002) shows that holding internet intermediaries liable for the content posted by users would cause the intermediaries to select only low-risk users and content, leading to a general decrease in the amount of content available online, and to an elimination of risky content. This would harm the market for ideas. Laws that limit the liability of internet intermediaries are intended to reduce this chilling effect. Under the notice and takedown approach applied in Europe and the United States, internet intermediaries are generally not liable for the content uploaded by users, but must promptly remove content once they have received notice. But even the notice and takedown regime can lead to excessive removals, thereby harming the market of ideas.

Ahlert et al. (2004) conducted a "mystery shopper" experiment. First, they uploaded to several hosting platforms the work "On Liberty" by John Stuart Mill. Written in 1859, the

work is no longer protected by copyright. The authors of the study, disguising themselves as representatives of a fictitious "John Stuart Mill Foundation," then sent notices to the hosting providers asking that the work be removed because of copyright infringement. Most of the hosting providers in Europe complied, without stopping to verify whether the "John Stuart Mill Foundation" actually exists, or whether "On Liberty" is still protected by copyright. The authors of the study use this experiment to show that even under the protective rules of the European E-Commerce Directive[28], the fear of liability by internet intermediaries leads to a significant chilling effect, *i.e.* the removal of legal content that should not be removed.

Seltzer (2010) argues that the Digital Millenium Copyright Act in the United States leads to a similar chilling effect, because takedown notices related to copyright infringements are systematically followed, even if the relevant use of the content might qualify for fair use. In its recommendations on internet policy making, the OECD (2011a) underlines the need to preserve the limited liability of internet intermediaries in order to foster freedom of expression.

3.5 The *Dennis* formula and its limits

The ideology behind freedom of expression in the United States is that a vibrant "marketplace of ideas" is essential for democracy and economic progress. Expression that does not contribute to the marketplace of ideas, such as threats of violence against an individual, or commercial advertisements, will enjoy a lower level of protection. Expression that contributes to the marketplace of ideas, such as political speech, will be entitled to high protection even if the speech is offensive.

Posner (2011) describes how United States courts evaluate measures that limit freedom of expression. On one side of the equation, courts will weigh the harm caused by the relevant content, and the probability of its occurrence. The timeframe within which the harm may occur is also measured.

On the other side of the equation, courts will evaluate the harm that the measure will cause to the proper functioning of the marketplace of ideas. Measures that suppress a particular point of view, particularly in political debate, will create a large harm to the marketplace of ideas, and will almost never be permitted.

Posner summarizes this equation as follows. A measure limiting freedom of expression will be permitted if:

$B < PL / (1 + i)^n$, where:

[28] Directive 2000/31/EC.

B is the total cost to society caused by the proposed measure, including the adverse effect that the measure will have on the marketplace of ideas, in particular through chilling effects;

L is the cost linked to the adverse event that the regulatory measure seeks to prevent, eg. racist crimes or terrorist attacks;

P is the probability that the loss "L" will occur in the absence of regulatory intervention;

i is the annual discount rate;

n is the number of years before the adverse event will occur in the absence of regulatory intervention.

The formula as summarized by Posner assumes implicitly that P would be zero in the presence of regulation, ie. that the regulatory measure would be 100% effective in eliminating the risk of harm. Most regulatory measures are not this effective. They will only reduce P, but not eliminate it entirely. If we assume that the regulatory measure reduces the level of P, but does not eliminate it entirely, then the Dennis formula leads to the following:

P is the probability of the loss occurring without the regulatory measure;

P_o is the probability of the loss occurring with the regulatory measure.

$P>P_o>0$

The total cost of the situation with regulation would be: $B + P_oL(1+i)^n$

For the regulation to be justified, the total cost of the scenario with regulation ($B + P_oL$) would have to be less than the cost of the scenario without regulation (PL):

$$B + P_oL(1+i)^n < PL(1+i)^n$$

In other words: $B < \frac{(P-P_o)L}{(1+i)^n}$

Posner's formula comes from the reasoning of a United States Federal Court of Appeals in the case *United States v. Dennis*.[29] It is sometimes referred to as the "*Dennis* test." By applying this test, a regulation prohibiting the publication of information on how to make a chemical weapon at home might be justified, because of the high level of L, the relatively high level of P, and low value of n (the harm could occur soon).

Moreover, the recipe for a home-made bomb contributes little to the marketplace of ideas, so B would be low.

[29] 183 F.2d 201 (2d Cir. 1950), *aff'd*, 341 U.S. 494 (1951).

By contrast, a regulation prohibiting speech that calls for the violent overthrow of the United States government would not be justified. Although the harm caused by the violent overthrow of the government (L) is high, the likelihood of it happening (P) is low. The timeframe within which the harm may occur is also fairly remote, leading to a high value for "n." Moreover, unlike the speech in the homemade bomb case, the speech in the violent government overthrow case may contribute to the political marketplace of ideas. Prohibiting it would cause a high level of B. Mialon and Rubin (2007, p. 5) provide other examples.

The results of the *Dennis* test may vary over time. When the United States was a young and fragile democracy, violent overthrow was perceived as a real and immediate risk. P was high, and n was low. A law prohibiting content advocating the violent overthrow of the government would potentially satisfy the *Dennis* test, even though the effect on the marketplace of ideas (B) would still be high. France recently adopted a law allowing police authorities to order ISPs to block access to sites promoting terrorism.[30] The law was intended to limit access to sites that recruit vulnerable young people to join terrorist groups in Syria. Critics of the law argued:

(i) that the measure would affect not only websites that promote terrorist acts, but also sites that promote certain religious ideals. In other words, "B" would be high because of the suppression of speech that is important for the market of ideas.

(ii) that the law would not decrease P, because young people would find other technical ways to access the sites, and the outlawed sites would gain in popularity because of the blocking measure. Forbidden by the government, the sites would become even more desirable.

This last example illustrates an important point relating to the European principle of proportionality, and which is not directly reflected in the first version of the *Dennis* formula outlined above. If a measure will have a high cost on a fundamental right (a high B value), policymakers and courts should verify whether there are other alternative measures that would be just as effective -- or more effective -- in lowering P, while carrying a lower cost (B) on fundamental rights. An alternative measure with a lower B should always be preferred where possible, over a measure carrying a higher B. Proportionality requires choosing the "least intrusive means."[31] In the case of measures designed to limit the recruitment of young people into terrorist organisations, the use of traditional police investigation tools, and the arrest of group organizers, will surely be more effective than site blocking. However, the question is often not "either or," but whether the site-blocking

[30] French Law n° 2014-1353 of November 13, 2014.

[31] *See* Section 5 below.

measure, in addition to traditional police tools, will make a difference in lowering P. If it does, the measure may still be justified in spite of the high level of B.

In the case of the French site blocking law, there was to my knowledge no study estimating the impact of the measure on P. The government's impact assessment assumed that the sites should be blocked, and only examined whether the blocking should be ordered by a judge, or by officials within the Ministry of Interior.[32] For the proponents of the law, and the parliamentary majority, site blocking was assumed to be the right thing to do, but empirical evidence was not examined on the question of whether site blocking would reduce the probability "P" of the relevant bad event "L" occurring.

It is important to point out here that even if empirical evidence showed the limited utility of the measure in reducing P, lawmakers may enact the law anyway. This is because of the expressive function of law (Sunstein, 1996), *ie*. the use of law to send signals to society as to what is acceptable and what is not. In the market for law making, demand comes from voters who expect elected officials to take action with regard to socially unacceptable content (Posner 2011, Stigler 1971). The producers of laws, if they want to be reelected, must make laws that respond to this demand. A law with a high symbolic (or "expressive") effect will often satisfy this demand, even if the law has a low empirical impact in reducing "P".

Whether regulators will choose the measure that is "efficient" versus the measure that is "expressive" will depend on a number of factors, including those described by Stigler (1971) and Peltzmann (1976).

As I will explain in Chapter 7, political decision-making can result in measures that are not efficient insofar as they do not maximize social welfare. The purpose of my methodology is not to replace sometimes inefficient political decision-making with an infallible scientific formula, but rather slow down the decision-making process by imposing a questionnaire and checklist that require policymakers at least to consider alternatives that tend to maximize social welfare. If policymakers choose another alternative, the choice would at least be more explicit.

3.6 Law and economics explanations for the high protection given to freedom of expression

Freedom of expression, particularly in the United States, targets actions taken by the state. According to constitutional theory in the United States, the government is particularly ill-qualified to select "good" and "bad" ideas. The government will have an inherent conflict of interest, favoring ideas that pose the least threat to the political *status*

[32] Impact assessment (*Etude d'impact*) relating to the proposed law strengthening the fight against terrorism (*projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme*) NOR : INTX1414166L/Bleue-1, July 8, 2014.

quo. By influencing the marketplace of ideas, the government can affect the proper functioning of democracy itself, creating an intolerably high cost to society (Breton and Wintrobe, 1992). When it comes to choosing ideas, the government is the "most dangerous monopoly" (Posner, 2011).

Coase (1977) takes exception with this reasoning, arguing that the high protection accorded to the marketplace of ideas under United States law results simply from successful lobbying by the intellectual elite, who are the main "producers" of ideas affected by content regulation. Like any other producer of goods or services, the intellectual elite will lobby for a market in which their production is not limited by regulation. The intellectual elite are also particularly effective at making sure their interests are protected in the legislature and courts. This view echoes Stigler's (1971) public choice approach.

If unregulated, the free marketplace of ideas can create problems of adverse selection:

> *"If listeners cannot distinguish ideas in terms of their truth content, they must regard the ideas as containing an average proportion of truth."* (Mialon and Rubin, 2007, p. 6)

This could lead to a general decrease in the quality of ideas in the marketplace, which suggests that screening out bad ideas could be efficient. Listeners to ideas also have limited attention, which may lead to congestion. Listeners may not be able to hear good ideas over the noise of bad ideas. Here, too, screening out bad ideas appears attractive. However, the cost of screening, and the risk of error, are high. Moreover, as noted above, the government would not be a reliable entity to perform the screening (Mialon and Rubin, 2007).

As noted above, Posner (2011) and Mialon and Rubin (2007) argue that good ideas have the characteristics of public goods, and will be under-produced by the market without support mechanisms. To avoid under-production of ideas, the state must take affirmative measures, including measures that reduce "chilling effects" that might create costs for the creation and exchange of ideas.

3.7 Freedom of expression and self-regulatory measures

Although the United States First Amendment targets laws and regulations adopted by the government, Kreimer (2006) explains that government action can take other more indirect forms that affect freedom of expression, including applying pressure on internet intermediaries to contribute voluntarily to content policies. Kreimer draws a parallel with action taken voluntarily by private media companies in the 1950s during the McCarthy era. At the time, United States media companies fired and/or boycotted individuals who refused to testify before the House Committee on Un-American Activities. This resulted

not from direct regulation, but from indirect government pressure on companies. Companies responded to the pressure by applying "voluntary" measures. Kreimer uses this example to illustrate the fact that self-regulatory measures taken by internet intermediaries can result from government constraint and lead to harmful effects on freedom of expression.

Garfield (1998) and Benkler (1999) argue that in spite of the "state action" requirement of the First Amendment of the United States Constitution, freedom of expression principles can apply to private contracts. They argue that "state action" is present when the government creates laws and courts that enforce private property and private contracts, and that the enforcement of a contractual clause restricting expression can also be considered as a government action.

This consideration is important when evaluating self- or co-regulatory measures applied by internet intermediaries to enforce national content policies. Although not imposed by direct government constraint, self or co-regulatory measures can in some cases interfere with freedom of expression. The intensity of this interference will generally be lower than in the case of government regulation.

4. PRIVACY

This section examines the second fundamental right that is most frequently affected by technical measures: privacy.

4.1 Privacy and data protection as fundamental rights

"Privacy" and "data protection" refer to two closely-related rights: privacy is the right to protection of one's private life against outside interference. It is the right to be "left alone" (Warren and Brandeis, 1890). Data protection is the right to control how personal data is used. The two rights often overlap. Americans often use the term "privacy" to designate both privacy and data protection rights. Europeans often use the term "data protection" to designate both rights. For purposes of this discussion, I will use the terms privacy and data protection interchangeably, to designate all privacy (or data protection)-related rights.

In Europe, the protection of one's private life, and the protection of one's personal data, are both considered fundamental rights. They are protected by the European Convention on Human Rights and by the European Charter on Fundamental Rights. In the United States, the right to protection against government intrusion into privacy is a fundamental right, embodied in the Fourth Amendment to the United States Constitution. However, the United States constitutional right is limited to situations that are equivalent to government searches of one's private home. Over time, United States courts have extended the Fourth Amendment to different situations, including private telephone conversations, the inside (and sometimes outside) of private vehicles, and the outside of a private homes.

Mialon and Mialon (2008) studied the effect of the Fourth Amendment on police conduct, and more particularly the effect of the exclusionary rule, which prohibits the use of any evidence obtained from illegal searches. They concluded that the exclusionary rule reduces the number of government searches conducted without sufficient justification ("probable cause"), but also leads to an increase in crime. The effects on welfare are ambiguous. This conclusion also applies to government actions to increase surveillance. Privacy legislation will decrease the level of abusive surveillance by the government of innocent people, but will also increase the risk of actual terrorists escaping surveillance. The weight of these two effects will be difficult to measure with certainty. The purpose of the proportionality test examined in Section 5 is to force regulators to at least try to evaluate the effects (positive and negative) of their measures, and thereby make measures more effective with fewer adverse effects on fundamental rights. The SURVEILLE project described in Chapter 7 attempts to do this by proposing a standard methodology against which to evaluate police surveillance measures. These methodologies do not replace political decision-making, including the adoption of sometimes inefficient but symbolically expressive laws. But the methodologies would obligate policymakers to conduct more meaningful impact assessments prior to proposing new laws or regulations, thereby making choices more explicit.

In the United States, the protection of individuals against privacy (or data) intrusions by other individuals or private entities is not a fundamental right. However, the protection is provided either by specific laws, or by common law tort principles (Whitman, 2004; Maxwell, 2014).

As is the case for freedom of expression, privacy is a fundamental right that can be interfered with. In Europe, interference with privacy is possible if the measure passes the proportionality test, which will be examined later in this chapter. In the United States, courts will apply a similar balancing test to measures that affect individuals' rights to be free from unreasonable surveillance. Most measures involving internet intermediaries will have an impact (positive or negative) on privacy rights, which is why an understanding of privacy rights, and of the proportionality test, are essential in order to build a methodology for assessing measures affecting those intermediaries.

4.2 Privacy rights in law and economics literature

Posner (1981) distinguishes three separate meanings for privacy. The first is the right to conceal information about oneself. The second is the right not to be bothered. The third is privacy as part of a broader right to individual freedom and autonomy. Posner argues that the right to conceal personal information creates inefficiencies that make everyone worse off. If unfavorable information about a product must be disclosed to a prospective buyer,

so should unfavorable information about a person, when the person is the "thing" being sold, as is the case in an employment context:

> *"The basic point I wish to assert is the symmetry between "selling" oneself and selling a product. If fraud is bad in the latter context (see Michael Darby and Edi Karni) – at least to the extent that one would not think it efficient to allow sellers to invoke the law's assistance in concealing defects in their goods – it is bad in the former context for the same reasons: it reduces the amount of information in the market, and hence the efficiency with which the market – whether the market for labor, or spouses or friends – allocates resources."* (Posner, 1981, p. 406)

Posner concludes that most privacy legislation has a redistributive function, subsidizing classes of individuals whose personal information is unflattering, *eg*. persons with a criminal history, but at the expense of other individuals (sellers) and buyers in the market, who would benefit from transparency.

United States law recognizes the invasion of privacy as a common law tort, involving four separate privacy rights:

- the right to object to the use of one's name or image in advertising;

- the right not to be portrayed in a "false light;"

- the right to prevent the collection of personal information using intrusive means (trespass, eavesdropping);

- the right to prevent the publication of intimate facts about oneself.

Posner argues that the first three privacy torts are economically efficient. The first confers a form of property right over an individual's personal information when used for advertising, which will have the effect of maximizing the value of the information and ensuring its best usage. The second right ("false light") increases the amount of correct information in the market, thereby making transactions more efficient. The third right ("intrusive means") is similar to trespass, and has the benefit of encouraging people to speak frankly on the assumption that they will not be listened to. This favors the free exchange of information, and avoids wasteful investment in privacy-enhancing technology, such as high walls around a garden, or building a communications technology that cannot be intercepted.

The last tort relates to concealment of true information, which Posner explains can be either efficient or inefficient depending on the transaction. If the concealment is done to mislead a contracting party on a matter that is material for a transaction, Posner believes

that concealment should not be protected by law. However, if the concealment relates to information that has no possible value to the transacting parties, then the rule is efficient.

Stigler (1980) also asserts that rules allowing individuals to conceal unfavorable information about themselves are inefficient because (i) they will reduce the accuracy of categorization, *ie*. people will still be placed in categories, but the categories will be less accurate, and (ii) transacting parties will turn to more costly and potentially less reliable means to obtain the information they seek, thereby increasing search costs and lowering the quality of the information obtained.

Varian (1996) highlights the annoyance caused by certain privacy violations, such as being bothered by unwanted telephone or e-mail solicitations. These intrusions create significant costs for consumers by using up the consumer's scarce attention. But these costs can be reduced if the advertiser has more information about the consumer, not less. If the advertiser knows exactly what the consumer is interested in receiving, the annoyance costs for the consumer will decrease because the consumer will only receive solicitations that he or she is interested in. In this sense, the merchant's and the consumer's interests are aligned. The consumer will benefit by letting the merchant know exactly what the consumer is interested in. A mutually profitable bargain can emerge. The situation changes, however, for secondary use of personal data, such as where the original merchant sells its mailing list to a third party. In that case, the purchaser of the mailing list will create costs for the consumer that are not reflected in the price paid for the mailing list, thereby creating negative externalities. To correct this, Varian suggests that consumers have the ability to control secondary use of their information, such as permitting secondary use only in exchange for a payment, or only for certain purposes, or only for a certain time. Varian's suggestion comes close to the "purpose limitation" rule that exists under European data protection law, with the important exception that European law has not yet established a means to organize a market for the right to secondary use against payment. European law is also generally hostile to the idea that individuals possess a tradeable right to use personal data.

Varian addresses the problem of open data, highlighting privacy objections that have been raised against making public records, previously available through a manual search, available online. Varian asserts that each situation requires a cost-benefit analysis, to determine whether potential benefits from eliminating manual search costs outweigh the additional threat to privacy. One alternative is to impose a fee for online searches that approximates the previous cost of conducting the search manually, including travel and photocopying costs. The fee could be used to help defray the cost of making the information available online, and would result in the same search costs as those that existed before records were available online.

Laudon (1996) suggests the creation of a National Information Market that would serve as a clearing house for managing consumers' authorizations to use personal data. The National Information Market would aggregate payments and distribute the payments to consumers who participate in the collective system. Laudon's system resembles the collective management of copyright.

4.3 Behavioral economics and privacy

Much of the Chicago School's analysis of privacy is based on the assumption that individuals are able to make rational choices about the use of their personal data, provided they receive sufficient information. This rational choice assumption permeates data privacy laws in the United States and Europe today, both of which focus on full information and individual consent.

In the mid-2000s, economists began to question this rational choice assumption. Beales and Muris (2008) challenged the "notice and choice" philosophy of United States consumer privacy laws:

> *"The reality that decisions about information sharing are not worth thinking about for the vast majority of consumers contradicts the fundamental premise of the notice approach to privacy. To be an effective approach, some significant number of consumers must not only read privacy notices for the businesses with whom they currently deal, they must also consider the privacy practices of alternative service providers and choose the provider whose practices best match their privacy preferences. There is no reason to think that this currently happening, or will ever happen."* (Beales and Muris, 2008, p. 114)

Acquisti, John and Loewenstein (2009) show how individuals' choices on privacy vary based on psychological effects studied in behavioral economics. In particular, Acquisti's experiments show a significant difference between consumers' willingness to pay (WTP) for additional privacy protection, and their willingness to accept (WTA) payment to give up pre-existing privacy protections. WTP is systematically lower than WTA. These differences are due to several effects, including the endowment effect (*ie*. what I currently have is more valuable than what I would pay to acquire it), loss aversion and status quo bias. Individuals' choices may also depend on the order in which the choices are presented. Brandimante, Acquisti and Loewenstein (2012) also showed that contrary to the assumptions of most privacy laws, individuals behave more recklessly when they have more tools at their disposal to control their privacy.

Borgesius (2013) studied the ramifications of behavioral economics on consent, concluding that "insights from behavioural economics cast doubt on the effectiveness of informed consent as a privacy protection measure. Many people click ‘I agree’ to any

statement that is presented to them." (Borgesius, 2013, p. 58). Borgesius suggests that the law should impose certain default rules protecting consumers against the most intrusive forms of tracking (*eg*. tracking based on health data), and make the default rules "sticky" by adding transaction costs if the consumer wants to opt out. A minimum number of mouse clicks, a telephone call or registered letter would be required to override the default rule for certain intrusive forms of tracking. Other forms of tracking (*eg*. tracking of children) might be prohibited altogether.

Posner (2008) makes the useful distinction between a person's "pure" interest in concealment of personal information and a person's "instrumental" interest, which is based on fear that the information might be used against him. Many individuals will not hesitate to share highly personal information about themselves with strangers, for example when chatting on an airplane. This tends to show that the revelation of highly personal information in itself creates no damage for an individual, and may indeed create a benefit, otherwise the person would not share the information. The benefit is presumably the ability to learn similar information about the other person and improve one's own information level and well-being. However, if the information is then used to embarrass or blackmail the individual, a harm will materialize. It is the harm from misuse that creates the harm, not the harm from disclosure itself. Posner (2008) emphasizes that the two should not be confused.

4.4 Cost-benefit analysis applied to data protection

In the field of privacy law, explicit cost-benefit analyses are rare. One exception is application of the concept of "unfair or deceptive practices" by the United States Federal Trade Commission (FTC).

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[33] The FTC has used this provision to enforce data protection principles against a broad range of companies in the United States, including in the internet sector. The FTC has developed what Solove and Hartzog (2014) call a "new common law of privacy." The FTC's enforcement actions, guidelines, and settlement agreements provide details on how the FTC applies the broad principles set forth in the FTC Act to particular facts. This process is similar to what courts do when adjudicating common law tort claims. By examining how claims have been dealt with in the past, observers can anticipate how a standard such as "fairness" will be applied in the future.

Beales (2003) describes how the fairness test has been applied by the FTC from 1938 to present. In the 1970s, the FTC used its authority to prohibit unfair practices in a broad variety of circumstances, relying in part on broad public policy criteria. Critics - - and in particular the United States Congress - - became concerned that the unfairness standard

[33] 15 U.S.C. 45.

was too subjective. In 1980, the FTC clarified its approach by adopting its "Unfairness Policy Statement" (FTC, 1980). Congress then inserted the FTC's methodology into the FTC Act itself in 1994. The United States Congress wanted to make sure that the FTC would limit itself to an objective methodology when evaluating "fairness," and not rely solely on public policy considerations.

The 1994 revision to the FTC Act creates a balancing mechanism to determine whether a practice is "unfair:"

> *"The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."*[34]

United States law therefore requires that the FTC conduct a cost-benefit test to determine whether a practice is "unfair." If the practice causes substantial injury to consumers that consumers cannot reasonably avoid, and the injury is not offset by corresponding consumer benefits, then the practice will be deemed unfair. The unfairness test is separate from the FTC's analysis of whether a practice is "deceptive." According to Beales (2003), a "deceptive" practice is a subset of the larger category of "unfair" practices. Under the FTC's methodology, a deceptive practice would not require a cost-benefit analysis, and would be presumed to be unfair. This is understandable because a deceptive practice is tantamount to lying to consumers, and such conduct is not likely to have any offsetting consumer benefits.

In the field of data protection, the FTC has used the theory of deceptive practices to sanction companies that do not honor their own privacy policies. In the case where a company has not broken any of its own promises, the FTC will not be able to punish the company for being deceptive. The FTC will have to show that the practice is "unfair." To do this, the FTC must first find that the practice causes or is likely to cause substantial injury to consumers. A substantial injury can result from a large injury to a small number of consumers or a small injury to a large number of consumers.

Consumer injury for privacy violations is often difficult to measure and has been the focus of much debate in the U.S, where the concept of privacy as a fundamental human right is not as ingrained as in Europe (Whitman, 2004). The injury to each consumer taken

---

[34] 15 U.S.C. §45(n).

individually can be extremely small. For example, the excessive collection of data may marginally increase the risk that a given consumer will fall victim to identity theft or receive unwanted advertisements. The individual injury in these situations would be difficult to quantify. Nevertheless, the FTC has stated its belief that these practices may create a substantial injury to consumers (Solove and Hartzog, 2014). Also, any practice that limits a consumers' autonomy and choice may be considered to create a substantial injury. For example, a default setting in software that leads to unexpected sharing of personal computer files was held to be unfair because it hindered consumer choice.[35]

The injury must also be one that cannot be reasonably avoided by consumers. This element of the equation captures the cost of accident avoidance present in the Hand formula for torts: where the cost for the victim of taking measures to avoid the accident is sufficiently low, it is economically efficient to allow the activity to continue and impose the cost of avoidance on the potential victim. This ties in with the FTC's mission to ensure that consumers are sufficiently informed and have the opportunity to make choices relating to their privacy. Any hidden or unexpected collection or uses of personal data could be deemed unfair because the consumer did not have a reasonable opportunity to make a choice in the matter.

The last step in the unfairness test requires that the FTC evaluate any countervailing benefits. This step requires that the FTC inquire whether the practice in question generates new valuable services, or lower prices, for consumers. In this connection, the FTC must compare the situation that would exist in the absence of any regulation by the FTC to the situation that would exist if the practice were stopped or regulated. The difference represents the costs associated with the FTC's own regulatory action, and conversely, the benefits associated with leaving the practice unregulated.

In summary, the practice would be prohibited if and only if $H-H_A > W_A-W_P$

Where:

H is total aggregate consumer harm created by the practice;

H_A is aggregate harm that consumers can reasonably avoid;

W_A is total consumer welfare when the practice is allowed;

W_P is total consumer welfare when the practice is prohibited.

In each case W would be calculated without deducting H.

[35] In re Sony BMG Music Entertainment, FTC complaint n° C-4195, 28 June 2007.

The FTC's unfairness test can best be understood through an example. Imagine that the FTC is considering the practice of setting third-party advertising cookies on users' computers when the users open a webpage. Is there a substantial consumer injury (H)? There may be, because the third-party ad cookies could lead to embarrassing situations such as when a user is presented an advertisement that is related to his or her browsing history and the user would prefer to keep the browsing history secret. The user may also find such tracking "creepy" making the consumer less inclined to use certain internet services in the future (Tene and Polonetsky, 2013). The FTC could view reduced consumer trust in online transactions as a form of harm. Consumer harm (H) is certainly present, even if its quantification will prove challenging.

Can the injury be reasonably avoided by the consumer? This may depend on the level of disclosure provided to the consumer and the availability of easy-to-use tools to block third-party advertising cookies. Good disclosure and an easy, one-click, blocking tool might cause H_A to approach H. The cost of avoidance would be low.

Finally, is the consumer injury offset by consumer benefits? This step would require the FTC to evaluate the benefits that flow to consumers from the widespread use of third-party advertising cookies. These benefits would consist principally of the wider availability of free online services, which in turn increases consumer choice and freedom of expression. The FTC would have to consider the costs associated with a prohibition of third-party cookies or the imposition of a consumer opt-in mechanism. These costs would be the difference between consumer welfare when the practice is allowed (W_A) and consumer welfare when the practice is prohibited (W_P). If the costs associated with these regulatory remedies (W_A-W_P) exceed the costs associated with the consumer injury that cannot reasonably be avoided (H-H_A), then the relevant practice would not be considered unfair.

To date, the FTC has more readily alleged unfairness in data security-related enforcements (for example, data breaches where companies are alleged to have had unreasonable security practices that put personal information at risk of misuse) than it has in pure privacy-related enforcement actions (for example, where the issue is not security but a company's decision to share personal information or to target ads to consumers in alleged unexpected ways). Despite this, the FTC has expressed an increased willingness to utilize unfairness even for privacy enforcement.

The FTC's fairness test relies explicitly on a cost-benefit analysis, comparing the aggregate harm caused by a given practice to its aggregate benefits. Where the aggregate harm outweighs the benefits, and avoidance costs are high for the victim, the practice is unfair. Conversely, where the aggregate benefits outweigh the injury (after taking into account reasonable injury prevention measures taken by the victim), the

practice is fair. This approach reflects the traditional law and economics approach to tort law, based on the so-called Hand formula (Posner, 2011). Under the Hand formula (named after Justice Learned Hand), a person is negligent if he or she expends costs on injury prevention ("B") in an amount less than the amount of the injury "L" multiplied by its probability "P". When calculating "P", the injuring party can assume that the victim will also take reasonable steps to avoid injury. Under this approach, not all injuries are prevented, only a reasonable level of injuries. In its simplest form, the Hand formula means that person will be negligent if, but only if, $B < PL$. A more refined expression of the Hand formula compares expected costs of harm and expected costs of prevention at the margin. The optimal level of prevention costs occur where an additional dollar of prevention (*B*) would yield at least a dollar of reduction in harm (*PL*).

From a social welfare standpoint, the objective is to minimize the sum of total costs of prevention (*B*) plus the total costs of harm (*PL*).

Graphically, this occurs where the lines *PL* and *B* intersect:

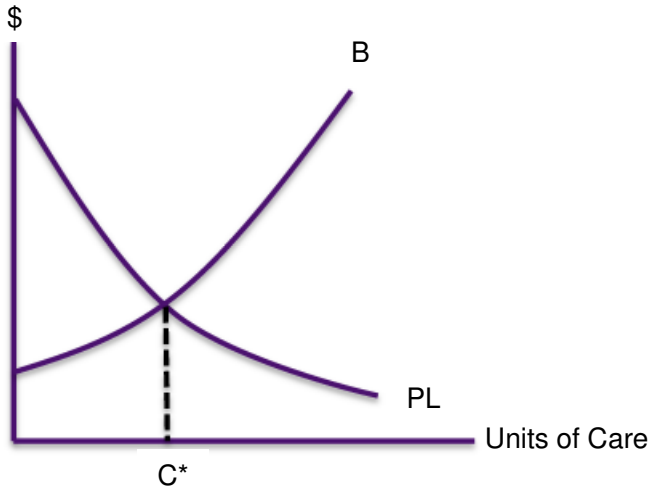


Figure 4, showing the changes in costs in harm (*PL*) and in prevention (*B*) associated with different levels of care. C* represents the optimal level of care. (Source: Posner, 2011)

This approach comes as close as possible to a negotiated outcome if there were a perfect market for buying and selling risks and injury prevention measures (Coase, 1960). The total costs of injury, plus the total costs of injury prevention spent by the injuring party and the victim are minimized, thereby achieving an efficient outcome from a welfare economics standpoint.

The European approach to fair processing in the privacy field focuses not on a cost-benefit analysis, but on the level of information provided to the data subject and the data subject's ability to exercise his or her individual autonomy. The FTC's approach is a

welfare economics approach, whereas the European approach is an individual rights approach. These two approaches are not necessarily incompatible, although the subject is hotly debated (Kaplow and Shavell, 2006).

4.5 How to measure costs and benefits in privacy

Let us focus on the particular problem of conducting a cost-benefit test in data protection. How should costs and benefits be measured? Alessandro Acquisti (2010) and Adam Thierer (2013) explore this difficulty. Thierer's focus is on conducting cost-benefit analyses in the context of regulatory proposals, following the United States rules on good regulation that I examine in Chapter 5.

Acquisti (2010) and Thierer (2013) point out that privacy is an intangible - - and in many cases immeasurable - - right, similar to the right to pursue happiness. Privacy is often based on consumer emotions, not economic considerations, making economic evaluation difficult. Individuals say that privacy is important, but traditional economic measurement tools, such as willingness to pay (WTP) and willingness to accept (WTA), show that individuals in fact attach a low value to privacy in practice. There is a considerable gap between what people say, and how they actually behave when given a choice to acquire (or forego) privacy protection in exchange for a price (ENISA, 2012). This paradox may lead to an under-valuation of privacy harms, if the harms are measured using traditional willingness to pay tests.

In some cases privacy violations can lead to measurable harm, such as when a company loses credit card records. A loss of credit card information requires banks and consumers to take steps to avoid fraud. Those steps create costs that can be measured. The receipt of unwanted spam also creates harm that can be quantified, as does the loss of data that might facilitate identity theft. Even if an actual case of identity theft cannot be traced to a given data breach, the data breach increases the probability of identity theft, and that probability can be estimated. Moreover, the increased risk of identity theft may require that consumers take preventive action to address the increased risk, and the cost of those measures can be quantified.

The most difficult harms to quantify are those associated with the feeling that certain data practices are "creepy" (Tene and Polonetsky, 2013). Another way of looking at "creepy" data practices is to call them practices that go beyond what a consumer would reasonably expect. "Creepy" data practices may cause consumers to reduce the level of their activity online, thereby creating a social cost similar to the cost created by excessive government surveillance, which would cause people to communicate less (Posner, 1978).

In many cases, the data protection harm can be linked to inadequate information provided to the data subject. Lack of information reduces consumer choice, and is a frequent

justification for privacy regulation. Solove and Hartzog (2014) examine several cases where the FTC has based its unfairness findings on inadequate information to consumers, including cases involving non-obvious default settings in software.

After looking at the costs, and if possible quantifying them, regulators must look at the benefits of the relevant practice. Benefits of a potentially unfair practice are equal to the costs associated with stopping or regulating the practice. This means that regulators must consider two situations: a situation where the practice is unregulated, and a situation where the practice is regulated or prohibited, and compare the two situations. The difference between these two situations is the opportunity cost of the regulation, or put differently, the benefit of no regulation. Like privacy harms, benefits are difficult to quantify. Widespread use of advertising cookies generates increased advertising revenues through targeted advertising, which in turn brings more free services and information to consumers. Goldfarb and Tucker (2011) attempted to measure the effect of the EU cookie regulation on the effectiveness of online advertising. They found that Europe's opt-in rule for cookies had a significant adverse effect on the online advertising market:

> *"First, privacy protection will likely limit the scope of the advertising-supported internet. However, it also crucially suggests that the types of content and service provided on the internet may change. In particular, without the ability to target, website publishers may find it necessary to adjust their content to be more easily monetizable. Rather than focusing on political news, they may focus on travel or parenting news because the target demographic is more obvious. Furthermore, without targeting it may be the case that publishers and advertisers switch to more intentionally disruptive, intrusive, and larger ads." (Goldfarb and Tucker, 2011, p. 18)*

Goldfarb and Tucker also argue that privacy regulation has an effect on innovation, which should be considered in any cost-benefit exercise. Thierer (2013) points out that privacy regulation can also affect other individual liberties, such as freedom of expression. Like harm to innovation, harm to freedom of expression is difficult to quantify. But the existence of these harms should be considered, at least from a qualitative standpoint.

As we will see in Chapter 5, cost-benefit tests of this kind should be performed for any proposed new regulation. The European Commission and the UK government conducted regulatory impact assessments with regard to the proposed European General Data Protection Regulation, but those assessments did not go into this level of detail.

5. FUNDAMENTAL RIGHTS AND PROPORTIONALITY

Both in the United States and in Europe, fundamental rights are routinely balanced in order to adopt socially optimal rules. In Europe, the balancing is done in the context of the so-called

proportionality test; which we will examine in this section. Any measure imposed on internet intermediaries in Europe will have to satisfy the proportionality test if the measure affects one or more fundamental rights.

5.1 The three-criteria test of the European Court of Human Rights

The European Court of Human Rights has developed three criteria that must be cumulatively satisfied whenever governments introduce measures to limit fundamental rights such as freedom of expression or privacy (Callanan *et al*., 2009). These three criteria appear in one form or another in all the court decisions relating to limitations of fundamental rights, including technical measures that address content policies such as fighting online copyright infringement. This proportionality test must form part of any methodology used to assess regulatory measures designed to deal with illegal content on internet.

First criterion: the measure must be provided for in a law that is understandable and has been adopted pursuant to democratic procedures.[36] This is the first safeguard for individual rights. When the legislature has adopted a law that specifically allows for a technical measure that could have an impact on a fundamental right, there is a presumption that the measure has been subject to a democratic debate and that the outcome of that debate between elected officials already represents a balance of competing interests and rights. The law must specifically envisage the restrictive measure in question in order to pass this first test. A law that gives broad but unspecified powers to the courts, to the government or to an administrative agency to impose restrictive measures is less likely to pass this first test. Consequently any law adopted to put into place a regulatory framework for fighting illegal content on the internet must explicitly identify the measures that the regulator may apply and how the regulator should apply the measures. In other words, the law must provide criteria to be applied by the decision-maker and a framework for determining when the technical measures are justified. The regulator in charge of applying the measure cannot be given a blank check. The law must be clear, and easy to understand, to avoid the risk of arbitrary application.

The first criterion is explained by the European Court of Human Rights in a well-known decision dealing with the blocking of the Google Sites service in Turkey[37]:

> *"In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any*

---

36 Opinion of the Advocate General in the ECJ, *Scarlet v. SABAM* case n° 70/10.

37 *Ahmet Yildirim v. Turkey*, ECtHR n° 31111/10, December 18, 2012.

> *such discretion and the manner of its exercise."* (ECtHR case n° 31111/10, par. 59)
>
> *"[J]udicial review of such a measure, based on a weighing-up of the competing interests at stake and designed to strike a balance between them, is inconceivable without a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression (see RTBF v. Belgium, cited above, § 114).*[38]

Second criterion: the measure must seek to achieve a legitimate objective. This second test will in most cases be satisfied. Restrictive measures adopted in democratic societies generally seek to promote a legitimate objective such as protection of youth, protection of property rights, privacy, cultural diversity or public security. For example, the protection of copyright is recognized as a form of protection of property, which is itself a constitutionally recognized right. Consequently, any measure adopted to limit online copyright infringement will necessarily pursue a legitimate objective and satisfy this second test. Measures intended to protect privacy, to protect children against exploitation, or to protect the public against terrorist attacks, will also satisfy the second test.

Third criterion: the measure must be necessary in a democratic society. This test is the most difficult to pass, and goes to the heart of the proportionality review. To satisfy the third test, the measure must be narrowly tailored to achieve the desired objective without affecting more than absolutely necessary other fundamental rights. It is this third test that must form the core of the analysis for any measure taken by an internet intermediary designed to implement a content policy on the internet.

These three criteria appear in various forms in court decisions and in international documents dealing with fundamental rights, such as a recent United Nations report on the promotion and protection of the right to freedom of opinion and expression (United Nations, 2011), which summarizes the three-step test as follows:

> *"1. The restriction must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);*
>
> *2. The restriction must pursue one of the purposes cited in Article 19(3) of the International Covenant on Civil and Political Rights, ie. respect of the rights or reputations of others, protection of national security or of public order, or of public health or morals (principal of legitimacy);*[39]

---

[38] *Id.,* par. 64

[39] Article 19 of the United Nations International Covenant on Civil and Political Rights (ICCPR) provides as follows:
1. Everyone shall have the right to hold opinions without interference.

3. The restriction must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality)."

The best way to understand how the proportionality test works is to examine a court decision explaining each step in the process.

One of the most interesting decisions is that of the British High Court in the BT TalkTalk case.[40] Two British ISPs, BT and TalkTalk, challenged the legality of the UK Digital Economy Act (DEA) on several grounds, including violation of several European directives. What is significant for purposes of this chapter is the claim that the DEA failed the proportionality test. According to BT and TalkTalk, the restrictive measures envisaged by the DEA affected more than necessary other fundamental rights and therefore failed the third branch of the proportionality test. The British government prevailed on this issue: the lower court held that the DEA satisfied the proportionality test. On appeal, BT and TalkTalk did not raise the proportionality argument again. Consequently, the lower court's analysis remains valid. Below is a short analysis of the lower court's reasoning on the question of "necessity."

5.2 Should a court give deference to lawmakers' balancing?

An important threshold question raised by the court in the BT TalkTalk case was to what extent the court should second-guess balancing that was already done by the legislature. Should the court approach the question anew, or should the court give deference to the balancing that was already done by lawmakers? This point connects back to the first step in the three-part test, *ie.* that the restrictive measure be adopted in a law that has been subject to democratic debate. If the balancing test was done *via* the compromises adopted through the legislative process, a court should hesitate before second-guessing the outcome of that balancing.

In the BT TalkTalk case, the court found that where the balancing of interests relates to broad social values and benefits, the court should defer to the legislature because: (i) the legislature is more accountable to citizens than courts are,[41] and (ii) the legislature will

---

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
a. For respect of the rights or reputations of others;
b. for the protection of national security or of public order (*ordre public*), or of public health or morals.

40 *BT/Talk Talk, supra* note 5.

41 "First, there is considerable support in the case law for the proposition that the Courts should afford particular deference to elected and accountable decision makers where the decision concerns subject matters that are regarded as within the particular province of the political branches…. 'greater deference will be due to the democratic powers where the subject matter in hand is peculiarly within their constitutional responsibility.'" *BT/TalkTalk, supra* note 5, at para. 210.

generally have better access to relevant information on societal balances than the court will.[42]

The court said it would apply closer scrutiny if the relevant measure consisted in restricting a fundamental right without a clear countervailing fundamental right being promoted on the other side. This ties back with the second step in the three-part test, *ie*. that the restrictive measure be adopted for the purpose of promoting a legitimate objective. Protecting another fundamental right is a legitimate objective, and therefore satisfies this test.

Giving some deference to the legislature does not mean blindly accepting its conclusions. It means instead that where the balancing test is close, the court will accept the legislature's conclusions and not substitute its own. The level of deference might be lower if the institution doing the balancing was a regulatory authority instead of a legislature. A regulatory authority is less accountable to citizens than are elected members of parliament. Consequently the court's scrutiny of the regulator's balancing might be more intense than the scrutiny of the parliament's balancing. In appeals of regulatory decisions, courts generally give some deference to the technical findings of regulatory authorities, particularly in areas where regulatory authorities have special expertise. However, for questions relating to the balancing of fundamental rights, courts will generally apply their own balancing anew, without giving deference to the conclusions of the regulator.

5.3 Identification of the conflicting rights and interests

After determining what level of scrutiny should be applied to the measure (high, medium or low), the court proceeded to explore the content of the balancing test as applied to the DEA.

The court listed the relevant rights and interests in competition with each other. The court identified three different kinds of rights and interests at stake in the DEA:

First, the rights of content owners to protect their copyright against unlawful activity on the internet;

Second, rights of internet intermediaries to enjoy exemptions from liability and freedom of regulatory burdens in connection with their activity;

Third, the rights of users to enjoy unrestricted access to information on the internet.

---

42 "Secondly, Parliament struck the challenged balance after a lengthy process of consultation of all interested parties, which took account of the representations made by those parties, and after a voluntary, non-legislative scheme was tried out. That process is likely to have provided the decision maker with an insight and capacity that the court is unlikely to enjoy." *Id.*, at para. 212.

The court stressed that the rights to be balanced were all recognized as fundamental rights:

…this is not a case where, on the one side, there is a human right, or a fundamental EU freedom, and on the other side the State is seeking to restrict or interfere with that right on the grounds of general utility or welfare.[43]

5.4 Balancing the relevant interests

Citing the *Promusicae* judgment of the CJEU[44] and case law of the ECHR, the British High Court concluded that copyright is an important right of property and that its enjoyment and exploitation is recognized as a fundamental right.[45] The court stated that some fundamental rights suffer no restriction, such as the right to life or the prohibition of torture and inhuman or degrading treatment or punishment. However, the right of freedom of expression, although it is a fundamental pillar of a democratic society, is subject to some restrictions. The right to the protection of privacy may also be restricted using a balancing test.

The court then proceeded to balance the various competing interests. To quote the court, a measure designed to limit copyright infringement may restrict fundamental rights:

> *"provided that the restrictions in fact correspond to objectives of general interest and do not, taking account of the aim of the restrictions, constitute disproportionate and unacceptable interference, impairing the very substance of the rights guaranteed."*[46]

The court here restates the second and third parts of the three-step test discussed above. The terms "disproportionate and unacceptable" used by the court appear redundant: A restriction that is "disproportionate" would necessarily be "unacceptable." The phrase "impairing the very substance of the rights guaranteed" provides an example of when a restriction would be disproportionate (and therefore unacceptable): Any restriction that makes the exercise of a fundamental right difficult or impossible, and not just less convenient, would be disproportionate, and therefore unacceptable. Respect for the "essence of the right" is also reflected in Article 52(1) of the European Charter of Fundamental Rights, which provides that:

> *"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only*

---

43 *Id.*, at para. 215

44 *Promusicae v. Telefonica*, Case C-276/06, CJEC Jan. 29, 2008.

45 *BT/TalkTalk, supra* note 5, at para. 215

46 *Id.*, at 217, quoting the European Court of Justice in *Schmidberger v. Republik Österreich*, Case C-112/00, CJEC June 12, 2003.

> *if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."*[47]

The test was also well summarized by the High Court of Ireland, in its June 27, 2012 decision *EMI Records v. Data Protection Commissioner*:

> *"…the nature of the injunction sought; the limitation to and the duration of any monitoring; the breadth or narrowness of scope of any order; the nature of the equipment to be used; the potential for the interference of that equipment with the proper use of the existing systems of the intermediary; the balance of burden as to equipment and personnel and cost; the intrusiveness of any remedy into legitimate privacy and entitlement to communicate; and amalny potential data protection impingements, together constitute the main factors in a court determining where the proportionality of a remedy to the mischief of the improper use of intellectual property online is to be struck or whether an injunction application is to be refused, despite legal compliance, on discretionary grounds."*[48]

5.5 Absolute versus relative proportionality, cost-benefit analysis

Portuese (2013) demonstrates that the proportionality principle as applied by European courts is in reality a form of cost-benefit analysis. Portuese argues that the case law of the United States Supreme Court also reflects similar principles, although they are not known by the name "proportionality." Portuese points out that the European proportionality test includes two aspects: an absolute efficiency test, under which the benefits of the rule should outweigh the costs for all stakeholders involved. In addition, proportionality includes a comparative efficiency test, under which the net benefits derived from the measure should be higher than those from all possible alternative measures. In terms of balancing fundamental rights, Portuese characterizes the cost-benefit analysis as ensuring that the marginal benefit reaped from the increased enjoyment of a fundamental right is greater than the marginal cost of restricting another human right. In addition, the measure that is selected should be the one that generates the highest net social benefits after taking into consideration all other legally and factually possible alternatives (Portuese, 2013).

Hickman (2008) distinguishes between overall proportionality and relative proportionality. Overall proportionality is an overall cost-benefit analysis to verify that the costs of the measure in interfering with individual rights are more than offset by benefits to society. Relative proportionality consists of comparing several alternative measures and choosing

---

47 Article 53, Charter of Fundamental Rights of the European Union, 2000/C 364/01, OJEC Dec. 18, 2000, C364/1 (hereinafter the "EU Charter").

48 *EMI Records v. Data Protection Commissioner*, High Court (Ireland), 2012/167 JR, June 27, 2012, para. 8.10

the one with the highest net social benefit. The focus here is in choosing the alternative with the highest marginal utility, in a Kaldor-Hicks sense. Rivers (2006) argues that the focus on relative proportionality should result in Pareto optimal result, whereas Hickman argues that the optimal choice will be Kaldor-Hicks efficient.

Hickman points out that a measure that satisfies the overall proportionality test may not satisfy the relative proportionality test, and vice versa. The two tests should be cumulatively satisfied. Hickman regrets that the current approach to proportionality does not clearly recognize these two tests, resulting in an absence of a clear methodology. According to Hickman, "proportionality can either become the fig leaf for unstructured judicial decision-making or it can become a powerful normative and predictive tool in public law" (p. 716). Hickman refers to the relative proportionality test as the "minimum impairment" or "least injurious means" test (Hickman, 2013, p. 701)

The difference between "overall" and "relative" proportionality lies in whether the costs of a given measure include opportunity costs, *ie*. the costs associated with the best other alternative. When opportunity costs are taken into account, the two tests yield the same results. To illustrate, imagine two regulatory measures "1" and "2" designed to fight online copyright infringement. Let us assume that the benchmark scenario, the scenario of no regulation, corresponds to a level of protection of copyright of 10, and a level of protection of privacy of 10.

Regulatory alternative 1 increases the level of protection of copyright to 15, but reduces the protection of privacy to 8, yielding a net benefit of 3 (I assume here for simplicity that each unit of copyright protection has the same value as a unit of privacy protection).

Regulatory alternative 2 increases the level of copyright protection to 16, but reduces the protection of privacy to 5, yielding a net benefit of 1.

Both regulatory alternatives appear to yield positive net benefits compared to the baseline scenario. Both would appear to satisfy the "overall" proportionality test. If opportunity costs are considered, however, regulatory alternative 2 would fail the test. The costs of regulatory alternative 2 in that case must include the forgone net benefits flowing from regulatory alternative 1, the best other alternative. The net benefits of alternative 1 are equal to 3. When opportunity costs are included, the costs of regulatory alternative 2 increase from 5 to 8, thereby exceeding the benefit flowing from alternative 2 (+6). This yields a negative result, meaning that alternative 2 would fail the cost-benefit test when opportunity costs are considered.

Proportionality is a form of cost-benefit analysis, requiring the selection of the measure that generates the lowest impairment of fundamental rights while permitting a reasonable level of enforcement of the desired policy objective. I will propose in Chapter 6 a system

to include proportionality in the overall methodology used by policymakers when evaluating possible measures affecting internet intermediaries.

5.6 Proportionality and the "least injurious means" test

The "least injurious means" test was articulated in the European Court of Justice's *Queen v. Ministry of Agriculture* case:

> *"The Court has consistently held that the principle of proportionality is one of the general principles of Community law. By virtue of that principle, the lawfulness of the prohibition of an … activity is subject to the condition that the prohibitory measures are appropriate and necessary in order to achieve the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued."*[49] (underlined by the author)

Tranberg (2011) analyses several cases of the European Court of Justice, concluding that the court's rule of proportionality requires national authorities to consider several alternatives and select the one that has the lowest adverse impact on fundamental rights while still attaining the desired objective. This methodology is strikingly similar to the one used in regulatory impact assessments examined in Chapter 5. For example, in the *Hüber* case, the ECJ considered German legislation requiring that data regarding immigrants be held in a centralized database. The purpose of the database was to help protect immigrants against discrimination. However, the database also created risks for privacy, particularly due to its centralized character. In his opinion, Advocate General Maduro indicated that a centralized database would be proportionate only if it is the only effective method of applying the national provisions on migration and residence. If there are less risky alternatives, such as a decentralized database, those alternatives should be used, even if they are marginally less convenient and effective.[50]

In the *Schecke* case[51], the CJEU considered EU legislation designed to enhance government transparency by publishing the names of recipients of agricultural subsidies. Here the court found that the European institutions had failed to apply the proportionality test because they did not consider alternative measures that would have achieved the desired objective of transparency with a lower interference with individuals' rights to privacy. This case shows that proportionality is not only concerned with the outcome, but also the process: authorities must consider several alternatives and evaluate whether less intrusive measures are available that would still attain the desired objective.

---

49 CJEU, *The Queen v. Ministry of Agriculture, Fisheries and food, ex parte FEDESA and others*, Case C-331/88, paragraph 13, quoted in Tranberg (2011).

50 European Court of Justice, *Hüber*, Case C-524/06, Advocate General Opinion, para 16.

51 European Court of Justice, *Volker and Marcus Schecke Eifert*, Cases C-92 and C-93/09, November 9, 2010, para. 81.

The "least intrusive means" approach to proportionality could be expressed in the form of an algorithm. The algorithm would identify the measure that has the lowest aggregate level of interference with individual rights while still leading to results that fall within a range of acceptable outcomes. For the algorithm to work, policymakers must first define a range of acceptable outcomes, bearing in mind that a level of 100% enforcement of a content policy will be neither achievable nor desirable as it would come at an inordinate cost in enforcement resources and in terms of individual rights. If policymakers define a range of outcomes going from a perfect outcome (which will generally not be achievable) to second best, third best, and fourth best outcomes, it will then be possible to measure different enforcement measures against these outcomes. If an enforcement measure required to achieve the second best outcome creates large additional costs on fundamental rights compared to a measure that achieves the third best outcome, policymakers should prefer the measure that achieves the third best outcome. On the other end, if the difference in cost is negligible between achieving the second best and third best outcome, then it would be reasonable to adopt the measure that achieves the second best outcome.

The difficulty at the outset would be to define the range of acceptable outcomes. When important content policies are at stake, such as protection against child pornography, it may be difficult for policymakers to admit that anything less than perfect protection is acceptable. The reality is, however, that for any form of enforcement, including enforcement measures to prevent serious crimes such as murder, the level of enforcement will not be complete (Shavell, 1993).

When proportionality is viewed as a cost-benefit test (Portuese, 2013) requiring consideration of several alternatives in order to choose the least intrusive (Tranberg, 2011), the proportionality test begins to look like a regulatory impact assessment. Chapter 5 will present the principles governing regulatory impact assessments, and Chapter 6 will attempt to merge the proportionality principle for fundamental rights into a broad impact assessment for measures designed to limit access to harmful content. The main lesson from this Chapter 3 is that proportionality tests for fundamental rights are not necessarily incompatible with "better regulation" principles and methodology used for conducting cost-benefit analyses and regulatory impact assessments. Harms and benefits to fundamental rights can rarely be quantified in monetary terms, but the relative benefits and harms of different measures can be compared, allowing a regulator to select the measure that creates the lowest *relative* harm while still achieving the desired objective.

5.7 Robert Alexy's balancing test

Alexy (2012) explains that when one fundamental right is impaired, the impairment must be more than counterbalanced by the benefit derived from satisfying another

countervailing right. Alexy created a weighting formula to measure the level of impairment and the level of benefit:

$$W_{i,j} = \frac{I_i \times W_i \times R_i}{I_j \times W_j \times R_j}$$

Where:

i and j relate to two competing rights or principles (P_i, P_j) that must be compared.

I is the intensity of the interference with, or the promotion of, the relevant principle P_i or P_j.

W is the abstract weight of the relevant principles Pi or Pj.

R is the level of reliability of the assumptions leading to I and W.

For example, if P_j represents a content policy relating to the protection of children against sexual exploitation, and P_i represents individuals' right to privacy, the denominator in the equation would attempt to capture:

- the relative weight of the principle of fighting child pornography (W_j);
- the expected level of attainment of that principle resulting from the relevant measure (I_j);
- the uncertainty (R_j) relating to I_j and W_j, in other words the degree of reliability of the empirical assumptions concerning what the measure in question means for the non-realisation of P_i. Put more simply, R is the risk of error.

In this formula, the denominator represents that right that is being protected and the numerator is the right that is being interfered with. The numerator would attempt to capture:

- the relative weight of the principle of protecting privacy (W_i);
- the expected level of interference with that principle through the relevant measure (I_j);
- the uncertainty (R_i) relating to I_i and W_j, ie., the risk of error.

R would generally be between 0.5 and 1; W would be 1, 2, 3 or 4; I would be 1, 2, 3 or 4. Alexy suggested using a three-level scale, based on a geometric progression. A "low" level of interference would be given the number 2^0 (*ie.*, 1); a "medium" level of interference would be given the number 2^1 (*ie.*, 2); a "high" level of interference would be given the number 2^2 (*ie.*, 4). Similar values would be given to the weighting variable "W", corresponding to the relative importance of the fundamental right. This would permit high

levels of interference (I = 4) with important fundamental rights (W = 4) to stand out in the numerator, by creating a product of 16.

A low value of $W_{i,j}$, and in any event a value less than 1, would be necessary to justify a measure.

In the practical examples given by Alexy (2014), the "R" factor rarely comes into play. The essence of Alexy's formula boils down to attributing a score to the importance of the right in the abstract (*W*), and then attributing a score to the level of interference with the right (*I*).

In the context of an EU-funded research project called "SURVEILLE", researchers adapted the Alexy formula and applied it to surveillance measures designed to fight crime and terrorism (Scheinin and Sorell, 2015). The objective of the SURVEILLE project is similar to mine: define a standard methodology against which proposed measures can be assessed, particularly in light of their efficacy in attaining the intended objective, and the level of interference with fundamental rights.

In the context of the SURVEILLE project, Grazia (2013) examines each fundamental right potentially affected by government surveillance measures, dividing those rights into their key attributes. Grazia then attempts to distinguish between the "essence" of the right, which may not be interfered with, and the peripheral attributes of the right, which in most cases can be interfered with, provided there is a good reason for doing so.

The SURVEILLE approach will be examined in more detail in Chapter 7.

5.8 Nussbaum's ethical filter

Nussbaum (2002) argues that certain basic entitlements cannot be balanced in a cost-benefit analysis:

> *"[S]ome costs have a distinctive nature; they are bad in a distinctive way. No citizen should have to bear them."* (Nussbaum, 2002, p. 1036)

The definition of the minimum level of entitlements can prove difficult, but conceptually, for each fundamental right, there is a red line that cannot be crossed, regardless of the countervailing benefit. In European proportionality reviews, this concept is reflected in the requirement that interference with fundamental rights must not destroy the "essence" of the right. Nussbaum warns that cost-benefit analyses can lead to morally wrong decisions. One suggestion is to attribute an infinitely high cost (Nussbaum refers to a "tragedy tax") to certain interferences with fundamental rights, so that any proposals involving unacceptably high interferences are eliminated.

In the methodology I propose in Chapter 6, the "tragedy tax" would be reflected in the additional constraints applied after the initial cost-benefit analysis is completed. Any proposals that include a "severe" or "extremely high" interference with a fundamental right would be eliminated, regardless of the level of countervailing benefits.

5.9 Fundamental rights and the Hand formula

Most fundamental rights are not absolute, and can be balanced against other rights and interests. The balancing is called the "proportionality test" and is applied by courts to measures that limit access to information on the internet.

The proportionality test represents a form of cost-benefit analysis, where the costs and benefits correspond to impacts on fundamental rights. These costs and benefits cannot generally be reduced to monetary values. However, a scoring mechanism or other techniques can be used as a rough substitute. (I will propose methods in Chapter 6.)

Under the proportionality test, policymakers must choose the "least intrusive means" to achieve the desired objective. This involves not only comparing the costs and benefits of the proposed measure, but also taking into account opportunity costs, *ie*. the net benefit that is forgone from not choosing the best available alternative.

If we compare harm to fundamental rights as a kind of accident that generates monetary damages, then the Hand formula could apply:

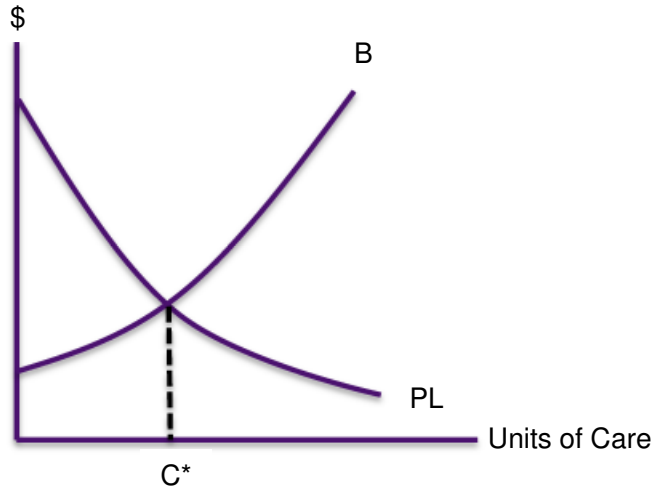


Figure 5 illustrating the Hand formula and the optimal level of accident prevention measures. (Source: Posner, 2011)

PL would represent the costs associated with violation of the fundamental right that is being protected by the relevant policy measure, *eg*. the right to privacy. The more units of prevention that are devoted to protecting the right to privacy, the lower the costs associated with privacy-right violations. This is illustrated by the downward slope of PL.

B would represent the costs resulting from the regulatory measure designed to protect privacy, *eg*. harm to freedom of expression. The more units of prevention that are devoted to protecting privacy, the higher the costs associated with violation of freedom of expression. This is illustrated by the upward slope of B.

Under the Hand formula, total accident costs should be minimized, *ie*. the sum of B and PL. When applied to fundamental rights, the test leads to a similar result, *ie*. the total costs of interference with fundamental rights, *B + PL*, should be minimized.

Conceptually this appears simple. In practice, it will be difficult to reach any consensus on where to place the PL and B curves on the graph. However, keeping the graph in mind will help policymakers avoid the mistake of assuming that measures designed to protect a fundamental right (*eg*. privacy) must necessarily be situated on the far right-hand side of the x-axis. Moreover, the use of a scoring mechanism similar to Alexy's can give a general indication on how the respective curves should be placed, leading to the emergence of one or two alternatives that are not too far from the theoretical optimum.

CHAPTER 4 - INSTITUTIONAL ALTERNATIVES FOR REGULATING ACCESS TO INTERNET CONTENT

1. CATEGORIES OF INSTITUTIONAL OPTIONS

This chapter will focus on the institutional alternatives that can be considered when imposing measures on technical intermediaries.

There exist four main categories of institutional frameworks for regulating access to internet content.

(i) General liability or property rules enforced by the courts (court regulation);

(ii) Detailed regulatory rules developed and enforced by an administrative or regulatory body (administrative regulation);

(iii) Self-regulatory regimes, which can involve unilateral regulation by each firm through individual terms of use (unilateral self-regulation), and regulation through collective codes of conduct (multilateral self-regulation);

(iv) Co-regulatory regimes, where the government delegates some regulatory functions to the regulated enterprise, which the regulated enterprise conducts under the government's supervision.

These four institutional frameworks often coexist with and complement each other. Indeed the first framework, general liability or property rules enforced by the courts, almost always exists, either by itself or as a backstop for other regulatory measures. In the shadow of liability rules and court enforcement, private actors use unilateral self-regulation, regulation through contract, to govern their relationship with users. The question then is whether supplemental institutional alternatives – administrative regulation, multilateral self regulation, or co-regulation -- are useful.

This chapter does not have the ambition of trying to identify an optimal institutional framework. Brousseau (2007), Marsden (2011) and Weiser (2009) examine various forms of internet co-regulation, Brousseau focusing in particular on "multi-level" regulation. (I discuss Brousseau's approach in Section 6 below.) This chapter is less ambitious. It seeks simply to illustrate how the four different institutional frameworks operate (and interoperate) in the internet environment, and identify the principal advantages and disadvantages of each alternative.

2. GENERAL LIABILITY OR PROPERTY RULES ENFORCED BY THE COURTS

The most basic institutional structure consists of laws that are then enforced by the courts. The vast majority of economic activity is governed by general principles of law that are then applied on a case-by-case basis by the courts. In civil law systems, the general principles of law are defined in a code, such as France's Civil Code. In common law systems, the general principles are developed through judicial decisions. However, even in common law jurisdictions such as the

United States, most legal principles are now reflected in laws enacted by the legislature and organized in codes.

Sound legal principles are general in nature, and not linked to any economic sector or technology. A good law is one that can survive over time and is flexible enough to adapt to new circumstances and technologies (Conseil d'Etat, 2016). The court's job is to apply the general principle to new circumstances.

2.1 Advantages and disadvantages of regulation by courts

The court system is designed to conduct fair adjudication of individual disputes, and performs this function very well. The judges who decide disputes are independent, and the procedures they use are designed to ensure that both sides of the case are given a full opportunity to be heard. The risk of error is reduced by an appeal mechanism. Obviously, not all judges are truly independent, and the procedural safeguards do not always work the way they should. Nevertheless, the court system is designed to come as close as possible to an ideal adjudication system for individual disputes. The judicial system benefits from high legitimacy because it is anchored in the country's constitution. Both the decision-makers and the decision-making process are respected. Industry capture of course is less likely to occur than within specialized regulatory agencies where regulators have a close on-going relationship with regulated entities. Decisions that come out of the court system are generally perceived as fair. The court system is a public service -- judges and their staff are paid by the state, not by the parties to the dispute. As we will see below, litigation before courts can be expensive, but the cost is not due to the fees of the judges or their staff.

Courts are flexible: their job is to apply a law to new circumstances, and find an outcome in each case that is fair and promotes the objectives of lawmakers. As noted below, this flexibility can be defeated if the law is poorly drafted.

In matters involving fundamental rights, courts are considered the most legitimate -- and in some cases the *only* legitimate -- decision maker. This is why courts will always be involved in any institutional framework dealing with internet content. Their presence is unavoidable because they guaranty that regulatory authorities (or self-regulatory initiatives) do not violate laws or constitutional rights of individuals. Because courts are unavoidable in any regulatory framework dealing with internet content, the only question is whether courts are sufficient by themselves, or whether additional institutional layers are necessary or useful.

Courts have several disadvantages. First, courts are designed to adjudicate disputes relating to events that occurred in the past. For example, the court will determine whether an internet platform acted promptly enough in removing illegal content once it received a notice. The court's focus is on something that happened months, maybe even years,

earlier. Courts generally do not conduct forward-looking analysis when adjudicating individual disputes, or ask what the ideal rule would be for development of the internet ecosystem for the future. The courts may conduct this analysis as part of their examination of the case, but it is not their primary focus. Their primary job is to determine who was right or wrong when the event occurred in the past. As we will see below, this is quite different from the role of administrative regulators, whose jobs are to monitor a given sector and adopt decisions that move the sector in the direction desired by lawmakers.

Second, the primary job of the courts is to render justice between two parties in an individual case. The purpose of court decisions is generally not to design rules that will affect the behavior of an entire sector. Court decisions can of course have this effect indirectly. Economic agents will observe court decisions and adjust their behavior accordingly. But this is not the primary objective of the court. The court's objective is to render justice between two parties in a given fact situation. The effect of the decision on behavior of other industrial actors is a secondary consideration that courts may in some cases take into account. But it is not the job of courts to make law or regulations, and courts may in some cases be oblivious to the effect of their decision on other economic actors. Moreover, because every individual dispute involves different facts, court decisions can be inconsistent with each other, thereby sending contradictory messages to the market.

Third, judges depend on the parties to the dispute for access to information. Judges generally cannot undertake independent investigations, and at the beginning of a case they are ignorant about the economic and technological context of the dispute. The result is that judges are dependent on the parties for access to information, and the information provided to them can be limited and biased.

A point related to judges' lack of information is the fact that judges are generally not expert in complex technical or economic issues. This can be a disadvantage in some cases, but an advantage in others. A lack of specialization can mean that the judge must devote considerable time to understanding some of the basic technical and economic parameters of a sector. Not possessing expertise, the judge can make mistakes that an expert would not make. On the other hand, a lack of specialization can render the judge free from accepted industry thinking. A non-specialist will more easily be able to think creatively and draw on examples from other sectors. Moreover, not all judges are generalists. In certain larger court systems, judges are assigned to specialized subject matters such as copyright or internet disputes. These judges acquire considerable expertise during their career on subjects such as notice and takedown for internet sites.

A major disadvantage of the court system is that the adjudication of individual disputes is generally slow. Courts have the ability to act fast in certain circumstances, in particular where there is danger of irreparable harm. However, these urgent proceedings are

available only in exceptional circumstances. The normal mode of functioning for a court is to examine the case over a period of several years. This long time period can be attributable to the large backlog and shortage of judges. In other cases, it can be attributable to procedural manoeuvres deployed by one party to delay the lawsuit. The delay inherent in court decisions creates several drawbacks. If the dispute is between a new entrant and a large well-established incumbent, the new entrant may perish while the case is being adjudicated. Even if the new entrant is right, the court decision will come too late to be of any use. The market will have moved on, the new entrant will have gone bankrupt or have had to change its business model.

To the extent a court decision is intended to send signals to the market, a delay of several years for adjudication is a drawback because it prevents the decision from having an effect on the market when it is most needed. This is especially true in a fast-moving market such as the internet. In addition, a court decision may not be final. As noted above, court decisions can be appealed and may contradict each other, leaving the market uncertain until the matter reaches the country's highest court. The process may take a decade.

In the area of notice and takedown, it took ten years for certain issues to be clarified, such as the kind of internet platform that can benefit from the liability safe harbor. Some questions are still unsettled because of inconsistent court decisions. Internet platforms manage this uncertainty. It is difficult to know whether the slow development of rules on notice and takedown created significant social costs compared to an alternative scenario in which detailed rules would have been developed at the outset through a regulatory authority.

Last, once a decision is rendered, courts generally do not conduct ongoing supervision over a given actor or situation. The court can only react to specific requests raised by litigants, and cannot itself supervise the application of its decisions over time. As we will see below, regulatory authorities can more easily conduct on-going supervision of market actors.

2.2 Summary table

The main advantages and disadvantages of relying solely on liability or property rules with court enforcement can be summarized as follows:

Advantages

- Judges have a high degree of independence, with a lower risk of conflict of interest or industry capture than other regulatory bodies.
- The court system is procedurally fair: both parties have the right to be heard and a right to appeal.

- Court decisions generally lead to the fairest outcome *for the individual dispute*.
- Courts are accustomed to applying legal principles to new circumstances.
- Courts are perceived as the most legitimate forum for disputes involving fundamental rights.

Disadvantages

- Courts create rules to apply to things that already happened. The rules are not forward-looking.
- Courts' first priority is to find the right rule for the individual dispute at hand, and not necessarily the right rule for the industry.
- Because decisions are focused on particular fact situations, court decisions are often inconsistent with each other.
- Court decisions require several years to be issued, even more in case of an appeal.
- Judges depend on the parties for access to information.
- Judges generally lack expertise in specialized technical or economic issues.
- Courts cannot easily conduct on-going supervision of market actors.

3. ADMINISTRATIVE REGULATION

3.1 Division of responsibilities between the lawmaker and the regulator

The traditional method of regulation of a particular sector (*eg*. banking or telecommunications) is for the legislature to enact a law setting out high-level legal principles for the sector and then to entrust the application of those principles to a regulatory authority. The regulatory authority will generally have the ability to adopt recommendations or binding rules that apply the legal principles to actors in the market, and sanction actors that ignore the rules. The regulatory authority may have an adjudication function pursuant to which parties can ask the regulatory authority to resolve disputes. The regulatory authority will generally have investigatory powers allowing it to gather information or even conduct dawn raids. Decisions of the regulatory authority – whether rule-making decisions, sanctioning decisions or dispute resolution decisions – are almost always appealable to courts. The regulatory authority is never a substitute for courts. Courts retain the ultimate power to determine the legality of the regulator's actions.

3.2 General versus detailed legislation

In the field of measures to limit access to illegal content on the internet, lawmakers have a dilemma. On the one hand, given the sensitivity of the issues and the careful balancing that must accompany any measure, lawmakers will want to draft detailed legislation in order to get the balance right. Detailed legislation will permit lawmakers to do the balancing themselves, contributing to the measure's legitimacy. The legislature is arguably the best institution to balance sensitive rights and interests, because the

legislature is directly accountable to citizens. Also, lawmakers may wish to avoid delegating regulatory authority for something as politically sensitive as measures to limit access to content on the internet. However, a careful balance struck after detailed legislative debate and compromise will result in a text that is perfectly adapted to the technology, business models and social context that existed at the time the debate took place. But when the law is actually applied, the balance struck by the legislature may already be outdated, overtaken by technological change and new social or business trends. The law will be ineffective, derided by critics as creating risks for fundamental rights, costing taxpayer money, without yielding any of the benefits that were supposed to be part of the original equation. A good example if this is the American Home Recording Act (AHRA), in which the United States Congress enacted detailed rules to deal with copyright infringement via digital audiotape recorders.[52] Digital audiotape recorders never became popular, and AHRA was quickly obsolete. Another example is the French HADOPI law. The law and its implementing decrees had peer-to-peer file sharing in mind. But when users turned to streaming and direct download, the HADOPI's regulatory framework proved ill-adapted to the new technology and usage patterns.

Another choice for legislatures is to write laws that are so general that they cannot become outdated. This option has advantages. A general law is more likely to stand the test of time, because courts or regulatory authorities can interpret the law in light of new technological developments and fact situations. Section 5 of the Federal Trade Commission Act, which prohibit "unfair and deceptive practices," is a good example of a provision that is general enough to be applied to many different circumstances. A regulatory authority such as the FTC can apply the "unfair and deceptive" standard to almost any situation that might arise on the internet, and the standard will never be outdated. The disadvantage of a general law is that it can create an unpredictable environment for stakeholders, who will have difficulty guessing in advance whether their own conduct falls within the standard or not. To address this shortcoming, the FTC issues guidelines so that market actors understand how the FTC intends to interpret the "unfair and deceptive" standard in various contexts.

In sum, a law that is too precise will have the advantage of being predictable, but runs the risk of becoming obsolete. A law that is too general will better stand the test of time, but will create uncertainty for stakeholders.

A third potential route --- one used in the European framework for regulation of electronic communications -- is for the legislature to adopt a detailed balancing methodology and entrust an independent regulatory authority with its application. This option permits the law to evolve with technological changes, and provides more predictability than the situation in which a bare standard, such as "unfair and deceptive," is used.

---

[52] 17 U.S.C. 1001 *et seq.*

3.3 Regulatory authorities have better access to information and industry expertise

Regulatory authorities have several advantages over courts. Like courts, regulatory authorities are dependent on regulated entities for access to information. Consequently, the level of information is far from perfect. However, regulatory authorities have more tools at their disposal to gather information than courts do. Regulatory authorities routinely issue public consultations and questionnaires to gather information from market players. Regulatory authorities can use their investigatory powers to gather information. Regulatory authorities also conduct forward-looking economic studies and market analyses, something that courts do not do.

Regulatory authorities have in most cases a higher level of subject matter expertise than do courts. Regulatory authorities have staffs of economists, engineers and lawyers who are specialized in the relevant industry. Judges do not have access to these resources.

Regulatory authorities have a forward-looking mission. Their objective is above all to ensure that a given market sector moves in the direction desired by lawmakers. Events of the past are only relevant insofar as they affect future market trends. The regulatory authority may in some cases be called on to sanction past behaviour or adjudicate private disputes. But the main objective of the regulator is elsewhere: to send signals to the market so that economic agents adapt to their behavior in a way that furthers the objectives defined by lawmakers.

Regulatory authorities are in many cases able to act more quickly than courts. A regulatory authority can adopt industry guidelines in less than 12 months. Some regulatory proceedings take much longer than this, and can even exceed the time needed for court proceedings. However, the time period for regulatory decision-making is supposed to be shorter than in the court system. This permits the regulatory authority to have a quicker effect on the market than would an individual court decision.

Finally, regulatory authorities are able to adjust their decisions and eliminate rules that are no longer needed. This provides flexibility to adapt rules to changing markets and technology.

3.4 Risk of industry capture

Regulatory authorities are more prone to industry capture than are the courts. Regulatory authorities have an ongoing relationship with players in the regulated industry. Regulators depend on industry players for access to information and for participation in regulatory hearings. Where regulated entities voluntarily comply with regulatory guidelines, the regulator can avoid adopting binding rules or imposing sanctions, which in turn helps the regulator avoid long and potentially damaging[53] court battles. Regulatory

[53] A court challenge carries considerable risk for a regulatory authority, because an unfavorable decision on the scope of the regulator's powers could undercut a considerable part of the regulator's work.

authorities have many incentives to coax market participants into voluntary compliance, instead of trying for force compliance through legal force.

Most regulatory authorities have rules prohibiting a member of a regulatory authority from working for a regulated entity for a certain time after their employment as a regulator. Nevertheless, many employees of a regulatory authority see employment with a regulated entity as a possible career path for the future. There are many reasons why regulators will want to maintain a good relationship with regulated industry players. Consciously or not, the regulatory authority will not want to take actions that seriously disrupt the players it regulates. The regulator will prefer gradual change over sudden disruptions in regulatory policy. This may lead to a situation where the regulatory authority adopts positions that have the effect of protecting existing market players against disruptive new entrants, technologies or economic models. In this respect, regulators can unconsciously impede innovation and favor the *status quo*.

Regulatory capture may be less of an issue for regulators that deal with a broad range of industries. Competition authorities, consumer protection and privacy authorities (such as the FTC in the United States or the CNIL in France) deal with a multitude of industries and players. They do not need the same close relationship with a given industry sector as does a sector-specific regulator such as a regulator of telecommunications or financial services.

3.5 Risk of regulatory creep

Regulatory authorities will have a natural inclination to take actions that increase their own power. When given a choice between a regulatory decision that gives the regulatory authority a greater role in regulating the industry, and a decision that lightens or removes regulation, the regulatory authority will naturally prefer the first option because it will keep the regulatory authority with a job. This phenomenon is referred to as "regulatory creep." Consciously or not, regulators will be reluctant to withdraw existing regulation because doing so could reduce demand for the regulator's services. The more natural path for regulators to follow is to increase regulation and their regulatory power. This path will reinforce the perception of the regulator's importance, potentially giving the regulator access to more budgetary resources from the government. Regulators compete with other branches of government for limited budgetary resources. In the market for access to budgetary resources, each regulator must convince lawmakers that that regulator's job is more important than that of its peers. A regulator who adopts a deregulatory policy will disadvantage itself in the competition for scarce resources.

3.6 Territorial limitations to regulators' powers

Regulatory authorities are inherently national in character. They exist because a country's legislature created them and gave them powers. Consequently a regulator

generally has no power outside its own country, and may have difficulty regulating an entity located outside the regulator's country even if the entity's actions have effects within the country. This is one of the principal challenges of regulating players in the internet ecosystem. Content and service providers can be located almost anywhere and provide their services worldwide via the internet. The actions of individual regulatory authorities are often ineffective against such entities.

3.7 Example of administrative regulation: the FTC's regulation of privacy

Section 5 of the Federal Trade Commission act empowers the Federal Trade Commission to take action against any "unfair and deceptive practice" in commerce. The FTC has interpreted this provision as giving the FTC broad authority to take action against companies that process personal data of consumers in ways that are misleading or unfair. For certain sectors of industry, the United States has enacted detailed data privacy laws that impose specific requirements on market actors. An example is the United States HIPAA legislation, which closely regulates how hospitals, clinics and insurance companies handle personal health data.[54] Detailed rules of this kind also exist for financial services, telecommunications services, cable television, credit reporting in the United States. By contrast, the United States rules on "unfair and deceptive practices" are quite general in nature. These terms give the FTC a great deal of flexibility to adopt the guidelines, and bring sanction procedures in a wide variety of contexts. Because a number of industrial sectors in the United States are not covered by sector specific data privacy rules, the FTC has filled the void by applying the "unfair and deceptive practice" principle to data privacy issues in the United States.

Because the FTC deals with a broad range of different industries, it is less prone to industry capture than a specialized regulatory authority in the energy sector for example. The FTC has a number of tools at its disposal to do its job as a regulator. The first tool involves conducting individual investigations and entering into settlement agreements with violators. When the FTC investigates a given violation and concludes a settlement, the findings of the FTC will be made public so that other companies can learn from the experience. In this way, the FTC sends a message to all market players as to how the FTC interprets the "unfair and deceptive" standard in given factual circumstances. This function is not unlike that of a court, whose decisions will be scrutinized by all market actors in an effort to understand how the court applied a general legal principle to a specific fact situation.

Finally, the FTC organizes public hearings, consultations and issues recommendations in an attempt to gather information from the market and adopt guidelines that reflect to the greatest extent possible and industry consensus. This activity is quite different from that of a court, in that the FTC will attempt to develop interpretations of the legal principle after a

[54] Pub.L. 104-191.

broad collection of data from the market. As we saw above, a court will typically only be able to collect data from parties to the litigation, and will not be as concerned with making a ruling that reflects industry consensus. The FTC by contrast will prefer industry consensus as it will tend to make regulations more effective and enforceable.

3.8 Summary table

The main advantages and disadvantages of administrative regulation are as follows:

Advantages

- Regulatory authorities can collect market information from various sources: investigations, consultations, and industry questionnaires.
- Regulatory authorities have subject-matter expertise and can rely on multidisciplinary teams (engineers, computer scientists, economists, lawyers).
- Regulatory authorities try to develop industry consensus and adopt rules reflecting consensus when possible. This in turn helps compliance and enforcement.
- Regulatory authorities have a broad set of tools at their disposal to influence market actors: workshops, guidelines, binding rules, sanction proceedings, settlement agreements.
- Actions by regulatory authorities are in most cases faster than court actions.
- Regulatory authorities follow a road-map defined by lawmakers, thereby giving legitimacy to regulators' action.

Disadvantages

- Regulatory authorities depend on market players for access to information.
- Regulatory authorities can be subject to industry capture, particularly where the regulatory authority deals with a single sector.
- Regulatory authorities will have a tendency to increase their own powers (regulatory creep).
- A regulator's authority is limited to a single country.

4. SELF REGULATION

4.1 Self-regulation and the internet

Most of the rules surrounding how the internet functions are developed through self-regulation. The technical standards used on the internet as well as the domain name system are developed and enforced principally through self-regulatory mechanisms. During the 1990s some scholars speculated that rules relating to content on the internet might be governed by a form of *lex mercatoria*, similar to the self-regulatory regime applied by merchants in the Middle Ages (Reidenberg, 1998). Because the internet was developed through private rules and codes of conduct, it seemed reasonable to suppose

that issues relating to content on the internet could also be governed by a global body of private rules, similar to the acceptable use policies one sees today in social media platforms. Early internet users, who were almost all academics at the time, observed "netiquette," a code of conduct that prohibited use of network resources for commercial purposes.

Let us examine the classic cases where self-regulation works, before examining two forms of self-regulation: unilateral self-regulation (contractual terms of use), and multilateral self-regulation (codes of conduct).

4.2 Self-regulation works well in groups with stable membership

In certain contexts, self-regulatory regimes are extremely effective. In the right circumstances they can achieve high levels of compliance while generating few enforcement costs. In successful self-regulatory regimes, public courts and police are unnecessary. Professional guilds are an example of this kind of self-regulatory situation.

Bernstein (1992) studied diamond merchants in New York and concluded that the success of the self-regulatory structures among diamond merchants is based on the fact that the membership of the group is relatively stable. Entry and exit from the group is difficult, which means that the cost of violating the group's internal rules is high. A member of the group who is sanctioned and excluded from the group will not have access to the resources and business opportunities associated with group membership. Because rules are enforced by members of the group, the use of the state's enforcement power is unnecessary to achieve compliance. The group finances its own enforcement mechanisms, making recourse to courts unnecessary in most cases. While the self-regulatory regime cannot use the power of the state to impose punishment (*eg.* imprisonment), the self-regulatory body can order exclusion from the group. Where the costs of exclusion are sufficiently high, self-regulatory bodies can achieve high levels of compliance with internal rules without recourse to state enforcement mechanisms.

Dixit (2009) underlines the problems of enforcement in multilateral self-regulation environments. Good enforcement generally requires a stable community with many ongoing interactions, and good information flows about members' behavior. Enforcement by other members of the group may give rise to some private costs. Punishment actions undertaken by certain members therefore becomes a public good and individuals have the temptation to free ride just as in any other context of private provision of public good. The communication channels that are needed for members to enforce rules against each other become weaker as the size and scope of the group expand. Successful governance in a large group or one with a large geographic or social spread eventually requires a shift toward more formal methods of governance.

4.3 Self-regulation works well where the self-regulatory organization (SRO) controls access to a scarce resource

Effective enforcement is also possible where the self-regulated group controls a scarce resource. In the case of a bar association or medical board, the scarce resource is the license to practice law or medicine. In the case of the internet domain name system, the scarce resource is domain names.

4.4 The difference between unilateral self-regulation and multilateral self-regulation

There are two main categories of self-regulation. Self-regulation can take the form of contractual rules imposed by a service provider on its customers. We will call this "unilateral" self-regulation. Unilateral self-regulation is present everywhere: tennis clubs impose rules on their members; internet platforms impose their terms of use on users of the platform. In unilateral self-regulation, the contract with users is the regulation.

Self-regulation can also take the form of rules developed by a group of stakeholders in a given industry to govern the conduct of the stakeholders themselves. We will call this "multilateral" self-regulation. Examples of multilateral self-regulation include professional guilds, such as bar associations and medical associations. The self-regulatory bodies created to deal with internet policy are the result of multilateral self-regulation. Multilateral self-regulation can take the form of nonbinding recommendations, or of binding rules. Multilateral self-regulation often requires the creation of a governance body charged with applying the rules.

We will examine briefly below an example of unilateral self-regulation, and an example of multilateral self-regulation. The example of unilateral self-regulation will be the terms of use of internet platforms. The example of multilateral self-regulation will be the self-regulatory organizations created by stakeholders in the advertising industry.

4.5 Unilateral self-regulation by internet platforms

(a) Internet platforms control membership privileges

Popular internet platforms have the power to exclude users from the platform, and the cost of exclusion is high for users. By entering a social media platform, a user agrees to abide by the terms of use, much like a travelling merchant in the Middle Ages would agree to abide by the rules of a local market place when entering the market. Like a professional guild, a social media platform can enforce its terms of use simply by withdrawing access to the platform. A high degree of enforcement can be achieved with minimal or no action being necessary from the government. In this respect, internet platforms would appear to have the ability to enforce internal rules effectively, with low cost to the state.

The situation is more complex in reality. Regulation through terms of use raises questions regarding the legitimacy of the underlying rules. Who makes the rules and why? Second, regulation through terms of use raises difficult enforcement issues, because internet platforms may suffer from conflicts of interest in enforcement. The platform's terms of use will generally prohibit users from posting illegal content or otherwise making use of the service in a way that would violate the law. A failure to comply with the terms of use will give the operator the right to terminate the user's membership privileges, but the platform may not systematically enforce the rules.

One reason why enforcement is not systematic is the sheer volume of content uploaded by users. Conscious of the impossibility for platforms to monitor all the content that is uploaded, lawmakers in Europe and United States provided platforms with a liability safe harbor that protects them from liability as long as they promptly remove content once they have received notice of its illegal character. Platforms rely almost exclusively on users to identify and notify the platform of content that is illegal or otherwise of violates the platforms' terms of use. On Facebook alone, users send more than 2 million notifications to the platform each week.

When a platform receives a notification from a user, the platform must review the content identified in the notice to determine if it in fact violates the terms of use and should be removed. The vast majority of notifications received by platforms are dealt with unilaterally by the platform, based on the platform's own determination as to whether the relevant content violates the platform's terms of use. Few cases go to court. The platform's job is relatively easy when the content objectively violates one of the platform's terms of use, such as the prohibition of nude photos. The situation becomes more complex when the illicit character of the content is not obvious. Under United States and European legal principles, an internet platform need not make difficult decisions relating to borderline case. Where there is doubt as to the legality of the content, the platform can either do nothing, and wait for a court order instructing the platform to remove the content, or decide to unilaterally remove the content relying on the platform's contractual terms of use.[55]

Complex situations arise when the content is considered illegal or shocking in one region of the world, but not in the country where the platform is based. This situation occurs most frequently in connection with certain kinds of hate speech that are illegal in France and other European countries but permitted in the United States under the First Amendment of the United States Constitution. Other examples involve content that is considered as blasphemous in some countries of the world, but as legitimate political or religious criticism in other countries.

[55] European and U.S. "notice and takedown" rules differ slightly in this regard.

Jeffrey Rosen's article entitled "The Delete Squad" illustrates how platforms handle complex questions linked to conflicting international legal norms (Rosen, 2013). Instead of blindly following United States First Amendment principles, global internet platforms are increasingly sensitive to non-US content laws. Other things being equal, the platforms will want to champion First Amendment principles and foster freedom of speech worldwide. However, the platforms make exceptions to the rule, such as where content is manifestly illegal under a local law and was posted by a user located in the country where the content is illegal. In those cases, the platform may decide to make the relevant content inaccessible only in the country where it is illegal. The platforms may also permit certain content to remain on the site in spite of a local law violation if the content is clearly a form of political or religious criticism.

(b) Advantages of unilateral self-regulation

The contractual rules established by internet platforms do not require a costly institutional framework to administer. Each platform applies its rules to users in accordance with the platform's own enforcement policy, without any formal procedures or methodology. In creating the rules and enforcing them, internet platforms will take into account their own risk of liability, but also the expectations of platform users. By putting into place a system pursuant to which users can identify unacceptable content by sending notices, platforms delegate to the users part of the job of enforcing the terms of use. The resulting notices will necessarily reflect the expectations and cultural norms of users. The system is a form of "bottom up" enforcement, which is decentralized and scalable. The platform's enforcement policies also are not constrained by national boundaries. Because the platform controls the servers on which content is posted, it makes no difference where the user who posted the content is located. He or she may be located in France, Russia or India, and the platform will still be able to exercise jurisdiction over the person based on the platform's terms of use combined with the platform's control over infrastructure.

The ability of platforms to enforce content policies on a global basis puts platforms at an advantage over national regulatory authorities, who typically do not have power outside their own national jurisdiction. This can lead national regulatory authorities to consider platforms as convenient proxies through which authorities can extend their own territorial power. This has occurred in France, for example, where the French data protection authority ordered Google to delist certain search results even for users outside of France. The reasoning of the French regulatory authority is that if a given search result violates the data protection rights of a French individual, those search results should be outlawed even outside France. The counter argument is that if France begins using platforms as a proxy to apply French content rules worldwide, other countries will do the same, resulting in every country in the world regulating what people in other countries see on the internet.

The point of this illustration is to highlight the tension that can exist between the technical ability of a platform to enforce a content policy worldwide, and the legal jurisdiction of regulatory authorities, which is generally limited to enforcement within a country's national borders.

The last advantage of unilateral self-regulation in the internet sector is that the terms of use put in place by each internet platform give the platforms the flexibility to apply ad hoc remedies in complex cases, such as by disabling access to content in certain parts of the world while keeping the content visible in other parts. This flexibility leads to solutions that are pragmatic and that in many cases reflect what a judge would do when confronted with the same complex fact pattern.

(c) Disadvantages of unilateral self-regulation

Alhert *et al.* (2004) illustrated the potentially over-zealous application by certain platforms of notice and takedown rules. The authors conducted a "mystery shopper" test among several large internet platforms. The authors posted a text of John Stuart Mill that is in the public domain, and then sent bogus notices to the platforms claiming that the text violated copyright. The platform located in the EU systematically removed the content, while the platform in the United States did not. The authors attribute this difference to variations in how the notice and takedown regime is drafted in the United States and in the EU. The example in the EU shows, however, that unilateral actions by platforms can be manifestly incorrect.

(d) Summary table

The main advantages and disadvantages of the unilateral model of self-regulation can be summarized as follows.

Advantages

- Little or no institutional costs, no institutional structure to administer;
- Enforcement is decentralized and scalable via user notice and takedown mechanisms;
- Competitive constraints ensure that enforcement policies are sensitive to user interests;
- Enforcement policies will be pragmatic and flexible, without the need to justify based on any regulatory methodology or procedure;
- Not constrained by national boundaries.

Disadvantages

- Terms of use are drafted unilaterally by the internet platform without any form of stakeholder debate.

- Enforcement of terms of use can lead to inconsistency, with cases of over- or under-enforcement.

4.6 Multilateral self-regulation and SROs

Multilateral self-regulation generally involves some form of governance structure, including the creation of a self-regulatory organization (SRO). Governance procedures and procedural safeguards of the SRO help enhance the credibility and legitimacy of the SRO's actions. The creation of the substantive rules by the SRO will typically be preceded by a debate among industry stakeholders, giving the normative output of the SRO more legitimacy than policies adopted unilaterally by a single enterprise. SROs can achieve high levels of compliance where their actions are backed by government authorities, and/or where compliance with the SRO code of conduct is a precondition to obtaining access to a scarce resource, such as television advertising inventory. Funded entirely by its members, an SRO will create few administrative costs for the state. SROs will be able to act relatively quickly.

4.7 Conflicts of interest in SRO enforcement

The disadvantages of multilateral self-regulation schemes include their inability or unwillingness to enforce compliance against their members. Because the SRO is entirely funded by its members, the SRO can be crippled by a conflict of interest when it comes to enforcing rules against members. This problem is attenuated when the SRO controls access to a scarce resource. In that case, compliance with the code of conduct is necessary for members to have access to the scarce resource. Compliance is also easier to achieve when the actions of the SRO are supported by government authorities. The threat of government sanctions can therefore motivate SRO members to comply with SRO rules. The SRO and its members will want to effect just enough enforcement to pre-empt government enforcement (DeMarzo et al. 2005).

4.8 Self-regulatory rules may not represent the public interest

Another defect of multilateral self-regulation schemes is that the rules are developed by industry stakeholders, often without the interests of consumers and citizens being represented at the bargaining table. Some SROs include consumer groups and defenders of civil liberties in the governance structure, so as to ensure that the rules adopted by the SRO also take consumer and citizen interests into account. However, this is the exception rather than the rule. Multilateral self-regulatory regimes frequently only involve economic players in a given industry.

4.9 Self-regulation and legislative threat

The state can also encourage the emergence of self-regulatory systems by exercising its power of legislative threat (Halftech, 2008). Governments often use the threat of legislation as a tool to encourage industry stakeholders to develop self-regulatory systems. Typically the government will present a policy problem that requires some form of regulation, and will encourage industry to find stakeholder-led solutions. The OECD (2011a) recommendations on internet policy making give preference to stakeholder-led regulatory solutions wherever possible. To motivate industry to find a solution quickly, the government will often announce its intention to introduce legislation or detailed regulations if a satisfactory industry-led the solution is not put in place. Like any threat, the legislative threat only works if there is a perceived probability that the threat will be applied. For issues creating political controversy, such as online copyright infringement and data privacy, legislative threat can be ineffective, because industry stakeholders are aware that enacting legislation on such sensitive topics is difficult for any government to achieve.

Legislative threat, if credible, can force stakeholders to take into account consumer interests. The signals sent by government can also result in a form of implicit co-regulation, where the government's objectives are implicitly taken into account in self-regulatory policies. I discuss co-regulation in more detail in Section 5 below.

4.10 Example of multilateral self-regulation: the advertising industry

(a) Advertising SROs control access to television advertising inventory

The advertising industry relies extensively on self-regulation. The advertising industry has developed self-regulatory codes in dozens of countries around the world. In addition, the advertising industry has organized self-regulatory organizations (SROs) to enforce the codes of conduct and arbitrate disputes. The SROs in the advertising field are organized in such a way as to give the appearance of independence in their decisions. Typically, bodies that make decisions relating to whether certain advertising content complies with the code or not will include independent members, including representatives of consumer protection bodies.

Like any self-regulatory organization, the advertising SROs do not have the same powers as a court. SROs cannot impose fines directly enforceable by a court, or impose imprisonment. Nevertheless, the level of compliance with advertising industry codes of conduct is high, particularly for television advertising.

There are several reasons why compliance in the context of television advertising is high. First, television broadcasters are themselves regulated entities. The media regulator in each country generally has rules on advertising with which television broadcasters must comply. The failure to comply with advertising rules could subject the television

broadcaster to fines or even the loss of its broadcasting license. Because of this threat, television broadcasters generally require that all television advertisements first be screened by the advertising industry SRO before the advertising is aired. To have access to advertising time on television, advertisers and advertising agencies must go through the SRO before the advertisement can be broadcast. This gives the SRO control over a scarce resource, *ie*. access to television advertising inventory. The SRO's control of television advertising makes use of the SRO, and compliance with its rules, unavoidable and effective. The second reason why SROs in the advertising industry are relatively effective is that major advertising agencies are a relatively small and stable group of enterprises who will have many repeat transactions in the advertising world. Like diamond traders (Bernstein 1992), or members of the legal profession, advertising agents have an interest in structuring their profession such as to make it difficult for unscrupulous operators to stay in the profession for any length of time. Bad actors threaten the reputation of the profession as a whole.

(b) Advertising SRO enforcement becomes more difficult on the internet

The internet is bringing about the vast changes in the advertising industry. The traditional role of the advertising agency is being challenged by new technical tools that allow advertisers to have direct access to advertising inventory on websites. The characteristics that make self-regulation successful in the advertising industry – television broadcasters' insistence that advertising be approved by an SRO before being aired, the relatively small and stable number of advertising agencies in the profession – may not apply in internet advertising. Web publishers are not regulated by a media regulatory authority, so there is little pressure on them to have advertising copy vetted in advance by an SRO. An increasing amount of internet advertising occurs in transactions directly between advertisers, internet advertising service providers, and Web publishers. Advertising agencies are no longer an obligatory go-between for advertising transactions on the internet. Consequently, the characteristic of a "stable group of industry players with multiple repeat transactions" may not hold true in the field of internet advertising.

(c) Advertising SROs are heavily influenced by state regulation

One interesting aspect of advertising self-regulation is its relationship with laws and regulations enacted by the state. The codes of conduct developed by the advertising industry are not developed in a vacuum. They reflect legal norms applicable in the relevant country. Those legal norms generally exist in the form of statutes requiring that advertising be truthful, not misleading, and that certain kinds of advertising, such as advertising for cigarettes, shall be prohibited. Laws and regulations in the field of advertising generally remain at a fairly high level of generality. The advertising SROs carry out an essential role of interpreting the general rules in specific circumstances. They go from the general to the specific. Without specific rules, actors in the advertising

industry would be left guessing as to whether a particular advertisement complies or not with the general legal principle. The work of the SRO helps eliminate legal uncertainty.

Unlike other industries, the advertising industry has not seen the emergence of state-created regulatory authorities. Instead, the role of regulatory authority has been assumed by the SROs. The codes of conduct created by the advertising industry, as well as the functioning of the SROs, complement the legal statutes.

The relationship between advertising SROs and the underlying legal framework is well summarized by the European advertising standards alliance (EASA, 2016):

> *"Self-regulation is also an alternative to detailed legislation, but not to all legislation. It is now widely accepted that self-regulation works best within a legislative framework. The two complement each other, like the frame and strings of a tennis racquet, to produce a result which neither could achieve on its own. The law lays down broad principles, e.g. that advertising should not be misleading, while self-regulatory codes, because of their greater flexibility and the fact that they are interpreted in spirit as well as the letter, can deal quickly and efficiently with the detail of individual advertisements. Framework legislation therefore creates a legal backstop which self-regulation will need to invoke when dealing with fraudulent and/or illegal practices (like for example pornography) as well as rogue traders – those operators who repeatedly refuse to abide by any laws."*[56]

The tennis racket "frame and strings" metaphor can apply to each of the institutional frameworks we examine in this chapter: self-regulation, co-regulation and administrative regulation. In each case, law serves as the "frame" for the more detailed and flexible regulatory measures.

By assuming a regulatory role, the advertising SROs have made it unnecessary for states to create administrative regulatory agencies for advertising. Media regulatory authorities, which have jurisdiction over television and radio broadcasting, could theoretically adopt detailed rules regarding the content of television and radio advertising. In a number of cases, however, media regulatory authorities have unofficially delegated this regulatory function to the SROs. The SROs communicate closely with the media regulatory authority and try to ensure that the SRO code of conduct meets the expectations of the media regulator. To the extent the media regulator influences the creation of the SRO codes of conduct, it would be more appropriate to speak of co-regulation rather than self-regulation.

(d) Advertising SROs and data privacy

Advertising SROs are attempting to create codes of conduct relating to data privacy, also in the hope of creating a self-regulatory environment that would pre-empt detailed privacy

[56] EASA website: "what are the benefits of self-regulation" http://www.easa-alliance.org/About-SR/Self-regulation-in-Europe/page.aspx/124

regulations. The SROs' efforts in this field are for the time being less successful than in the field of television regulation. This is partly because the underlying privacy norms applicable to internet advertising are still open to vigorous debate. Because the underlying normative context is in flux, SRO attempts to create acceptable codes of conduct for internet privacy have not met with general acceptance by the privacy regulators. The SROs' failure to reach consensus on mechanisms such as "do not track" is not surprising given the vastly different interpretations that national data protection authorities have of the notion of user consent, for example. Another difficulty is that some data protection authorities are already producing detailed guidelines, supplanting the role of SROs. Where state-created rules are detailed, SROs have little room to interpret the rules and create value through voluntary codes of conduct. The regulatory authority has already put strings on the frame of the racket.

SROs may not be able to thrive where they are in competition with administrative authorities. The role of advertising SROs is openly embraced by media regulatory authorities, who give their implicit approval of the codes of conduct and clearance procedures put in place by the SROs. The implicit support of the government or of a regulatory authority give SROs a state-like legitimacy. To market participants, a code of conduct developed by the advertising SRO will be viewed as the equivalent of a regulation adopted by the government or by a regulatory authority. SROs with state support come very close to co-regulatory systems that we will examine in the next section.

4.11 Summary table

The main advantages and disadvantages of the multilateral self-regulatory regime are as follows.

Advantages

- SRO governance structures provide higher legitimacy than is the case in unilateral self-regulation regimes;
- Rules are developed by stakeholder debate, leading to more balanced normative output than in the unilateral self-regulation regime;
- The level of compliance can be high where an SRO enjoys government support, and/or controls access to a scarce resource, and/or members of the group are stable;
- SRO rule-making is relatively fast and flexible;
- SROs are not necessarily constrained by territorial boundaries.

Disadvantages

- SROs are subject to an inherent conflict of interest that can hamper the SRO's willingness to enforce rules against its own members;
- SROs can be ineffective where there are a large number of actors and entry or exit from the group is easy;
- SROs can be ineffective where the underlying normative context is confused or in flux, and/or where the SRO is in competition with state regulatory authorities;
- SRO codes of conduct are generally developed by industry stakeholders only. They do not generally incorporate the views of consumers and citizens. They therefore lack legitimacy compared to co-regulation or administrative regulation;
- SROs can have anti-competitive effects.

5. CO-REGULATION

5.1 The role of the state in co-regulation

Co-regulation is a system under which a state-sponsored institution, such as a government agency or independent regulatory authority, creates a framework within which private actors discuss and if possible agree on regulatory measures. Co-regulation is like self-regulation except that in co-regulation the government or regulatory authority has some influence over how the rules are developed and enforced. The involvement of the state is supposed to make the rulemaking process more legitimate and effective compared to purely self-regulatory solutions. It is more legitimate because the process is supervised by officials who are accountable to the democratically-elected legislature. It is more effective because the resources of the state can be used if necessary to enforce the rules.

The distinction between self-regulation and co-regulation is not always clear. As mentioned above, certain advertising SROs have no official connection with broadcasting regulators, but *de facto* work very closely with them and receive their implicit and in some cases explicit support.

5.2 Co-regulation and accountability

"Accountability" is a form of co-regulation, because it consists in the development of internal rules by companies that are then verified and/or enforced by government entities. Popular in data privacy regulation (*see* Section 5.6 below), accountability permits private actors to develop their own processes for achieving public policy objectives. Because companies have the best information as to what works within their own organization, they are in a much better position than regulators to design the regulatory compliance

processes within their organization. To ensure that the processes are applied, government regulators will have an audit right to evaluate the effectiveness of the procedures. In some cases, the verification process can be delegated to a third party accountability agent. In that case, the government would only become involved if and when a violation occurs, *ie*. one of the public interest objectives defined at the outset is violated. Accountability requires strong internal structures within the corporation to create appropriate monitoring and enforcement functions. This may not always be feasible, particularly for smaller organisations (Balleisen and Eisner, 2009).

Examples of accountability will be presented in Section 5.6 below, dealing with co-regulation in data privacy.

5.3 Preservation of public interest objectives

The presence of the government in the discussion also ensures that the self-regulatory measures that emerge from the discussions satisfy public interest objectives, objectives that may not be given sufficient weight in self-regulatory regimes.

As we have seen, one of the defects of pure self-regulatory approaches is that some stakeholders or interests will be under-represented at the bargaining table. Representatives of consumers and defenders of civil liberties may have fewer resources than industry to make their voices heard at self-regulatory discussions. Oversight of the discussions by a government agency or regulatory authority will help ensure that any bargaining asymmetries among stakeholders are neutralized. In addition, the regulatory authority or agency will ensure that bargained-for solutions stay within limits defined by the legislature.

5.4 Enhanced legitimacy of the rules

Co-regulatory structures tend to yield solutions that are perceived as being more legitimate than self-regulatory structures. Under co-regulation, the solutions that emerge from the discussions of stakeholders are either explicitly or implicitly approved by the regulator or government. This approval helps legitimize the outcome for the reasons mentioned above: the regulatory authority or agency will ensure that consumer and citizen interests are represented, and that the outcome from bargaining is consistent with public interest objectives. The perceived legitimacy of the rule will help compliance and enforcement.

An agency's approval of the co-regulatory measure also helps enforcement because third parties will know that if they ignore the rule, the regulatory authority is likely to bring enforcement actions against them. Because the state is involved, co-regulatory solutions can take longer to develop than purely self-regulatory rules. This is particularly true when the co-regulatory rules have a binding nature.

5.5 Co-regulation in telecommunications regulation

Co-regulation has long been used in the telecommunications sector. National regulatory authorities have authority under the European directives on electronic communications to impose on operators that hold significant market power certain obligations relating to access and interconnection. Those obligations include the publication of a reference interconnection offer, and the obligation to enter into interconnection agreements with other operators. The French national regulatory authority for electronic communications, ARCEP, created an interconnection committee within which details of France Telecom's interconnection products, and its reference interconnection offer, were debated. The interconnection committee involved a representative from the national regulatory authority, a representative from France Telecom, and representatives from France's main competitive operators. The interconnection committee permitted the national regulatory authority to nudge market players toward consensus on difficult interconnection or access issues linked, for example, to local loop unbundling.

The information exchange can be a valuable by-product of co-regulatory regimes. As we will see below, one of the main sources of inefficiency for a classic state-run regulatory structure is lack of information by the regulatory authority. The lack of information can lead to poor regulatory decisions. A co-regulatory system should be designed to allow the regulatory authority to gather information from stakeholders.

In questions relating to interconnection of telecommunications networks, the organisation of a co-regulatory discussion forum did not foster information exchange because participants were concerned about revealing business secrets. But two benefits emerged. First, the discussions held in the interconnection forum permitted competitive operators to have advance information relating to changes to the incumbent operator's reference interconnection offer, and to discuss and potentially influence the proposed changes. Second, discussions within the forum can help a consensus emerge on contentious issues such as interference levels and technical standards. The compromise solutions are then better accepted by the market, reducing the likelihood of disputes.

5.6 Co-regulation in data privacy

Data protection authorities in Europe are distrustful of purely self-regulatory arrangements, and prefer co-regulatory solutions in which the data protection authority (DPA) is involved in both the formation of rules and their enforcement. DPAs in Europe emphasize binding corporate rules (BCRs), which evidences this co-regulatory preference. Under the European legislation, companies are prohibited from sending personal data outside the EEA to countries that have not been recognized by the European Commission as providing an adequate level of data protection. The United States currently is not viewed as providing an adequate level of protection of personal data. One of the ways companies can overcome the prohibition is by adopting BCRs.

BCRs are a set of internal procedures that guarantee a high level of protection of personal data throughout the organization, including in parts of the organization located in countries without "adequate" protection. BCRs must be developed in close cooperation with DPAs in Europe. A multinational group can propose BCRs following a template adopted by the Article 29 Working Party, but ultimately the content of the BCRs must be negotiated point by point with one of Europe's DPAs. Once the lead authority is satisfied with the content of the BCRs, the file is then sent to two other co-lead DPAs who in turn scrutinize the content of the file to ensure that the BCRs meet European standards. Once the BCRs have been approved, they confer rights on third parties who can sue the company for any violation of the BCRs. Likewise any breach of the BCRs can give rise to sanctions by DPAs.

BCRs constitute an example of co-regulation because they are developed by private stakeholders within a framework established by regulatory authorities, and once they have been adopted, the BCRs can be enforced by regulatory authorities in the same way as classic regulations.

The Federal Trade Commission's (FTC) extensive reliance on negotiated settlement agreements can also be seen as a form of co-regulation. The FTC conducts investigations and begins enforcement action against companies that have violated the "unfair and deceptive practices" rule, as well as other privacy violations such as violation of the US-EU safe harbor framework. One of the procedural options that the FTC can propose is a settlement agreement with the company, which binds the company to put an end to the relevant practices as well as submit itself to on-going accountability obligations similar to those one sees in BCRs.

The individual settlement agreements provide for procedural and structural safeguards to help prevent violations of data privacy commitments.[57] Like European BCRs, the negotiated settlement agreements provide for both internal and external audit procedures, training programs and periodic reporting to the FTC. The settlement agreements last for 20 years, giving the FTC the ability to co-regulate major internet companies over a long period of time. The FTC settlement agreements are public, thereby permitting the FTC to use the settlement agreements as a means of sending signals to all companies in the relevant sector. Although the settlement agreements are not binding on companies that are not signatories, the settlement agreements provide to third parties guidance on what the FTC considers to be the state of the art in privacy compliance. The settlement agreements inform third parties on practices that the FTC is likely to view as unacceptable, as well as compliance measures that the FTC is likely to consider as optimal.

[57] For an example, see the Facebook settlement agreement here: http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

The FTC settlement agreements can have wide ranging effects. First, if the settlement agreement binds a major internet platform such as Facebook, the settlement agreement will have an impact on a large portion of the internet industry simply because the platform serves a large part of internet users. Second, the settlement agreement will have indirect effects on all other players in the internet industry, by showing best practices and FTC expectations. The FTC's settlement agreements serve a pedagogical function, thereby contributing to overall compliance with regulatory best practices in the industry.

The United States government is trying to encourage other co-regulatory solutions for data privacy. The United States administration refers to this as the "multi-stakeholder process." Under the multi-stakeholder process, the National Telecommunications and Information Agency, the NTIA, convenes stakeholders in an effort to develop codes of conduct. The role of the NTIA is to convene multi-stakeholder meetings, facilitate the exchange of information, and apply the threat of mandatory regulatory measures should the stakeholders fail to agree on consensual measures. The NTIA acts as a maieutic regulator (Curien, 2011), helping to nudge stakeholders toward a consensus. The presence of the government in the discussion also ensures that the self-regulatory measures that emerge from the discussions satisfy public interest objectives, and in particular, the protection of privacy rights. The multi-stakeholder process yielded draft recommendations on transparency in mobile applications (NTIA, 2013).

The convergence of United States and EU co-regulatory philosophies will be tested in connection with efforts to create a compatibility system between European BCRs and Cross Border Privacy Rules (CBPR) developed under the APEC framework (APEC, 2013). Like BCRs, CBPRs represent a set of data protection obligations that companies can subscribe to, and that will be enforced by data protection authorities in participating APEC countries. Application of the rules is verified by an "accountability agent." The purpose of subscribing to the CBPRs is to demonstrate compliance with the APEC Privacy Framework principles, and thereby facilitate data flows among APEC economies.

5.7 Summary table

The main advantages and disadvantages of a co-regulatory regime are as follows.

Advantages

- The involvement of the government or of a regulatory authority gives co-regulatory solutions added legitimacy;
- Co-regulation leads in theory to solutions in which the interests of all stakeholders, including consumers and citizens, are represented;
- Co-regulation facilitates the exchange of information between industry and regulatory authorities, thereby enhancing the authorities' ability to avoid mistakes;

- Compliance with co-regulatory solutions is high because industry stakeholders have participated in the development of the relevant solutions. Moreover, the violation of the relevant rules can lead to sanctions from the regulatory authority.

Disadvantages

- Co-regulatory solutions are more time-consuming than self-regulation because the state is involved.
- The involvement of the state will create institutional costs for taxpayers.
- Because state authorities are involved, co-regulation will be closely anchored to national (or regional) laws.

6. BROUSSEAU'S MULTILEVEL APPROACH TO GOVERNANCE

In a 2006 paper, Brousseau (2006) examines the interaction between centralized rules, such as those administered by the state, and decentralized rules, such as those administered by internet intermediaries or by users themselves.

Citing Lessig (1999), Brousseau notes that digital technologies allow actors to create their own systems of property rights and enforce them through encryption and access control. This is more efficient than a centralized property rights system because the system can be matched to each individual's needs. Brousseau also points to collective information spaces, such as social media platforms, and the ability of these platforms to efficiently enforce collective rules by excluding users who do not obey them. The technical ability to track individual users, to detect violation of the rules and efficiently exclude them from the platform overcomes some of the traditional limitations to collective self-regulation.

Examining multilevel governance, Brousseau asks whether it is better for the measurement and enforcement of property rights to be performed by a central authority such as the state, or on a more decentralized level, via self-regulation for example. According to Brousseau, the new institutional economics approach shows that it is inefficient for the establishment and operation of a property rights system to be totally centralized, or totally decentralized. There should be a combination of both.

> *"Agents build complementary contractual arrangements, self regulations and general institutions to solve the various dimensions of their coordination problems in relation to the optimal centralization/decentralization trade-off for each of these dimensions." (p. 628)*

There needs to be a complementarity between the various levels of governance, a system of checks and balances. For example, the central institutional level should ensure that the

lower decentralized level is not captured by monopolists. The central level is also necessary to assist in the enforcement of rules created at the decentralized level, since only the government can exercise legitimate force.

By the same token the decentralized and private governance arrangements allow innovation that would not be possible under the centralized rules, as well as a mechanism to limit the discretionary power of the central institutions. The ability of private actors to "bypass and even overcome the public order constrains public institutions not to be overly inefficient." (p. 629)

Brousseau points out that in any multilevel governance scheme, there must always be a centralized last resort regulating entity that should overhang all the norm setting entities beneath it. The last resort entity is:

> *"in charge of avoiding incompatibilities among norms and maximizing positive network externalities among them, as well as avoiding the capture of norms by individuals or groups seeking to exercise dominance….It is also responsible for guaranteeing the enforcement of locally set orders as long as they contribute to collective efficiency." (page 629).*

Brousseau refers to a bargain between the centralized norm center and the local norm centers pursuant to which the centralized authority lends assistance to the enforcement of the rules created by the decentralized entities. In exchange the decentralized entities accept the constraints imposed by the last resort regulator in exchange for this support. This allows each level of regulation to reinforce each other.

Brousseau mentions that states still have a significant regulatory role. The power of private norm centers is limited. Many interactions on digital networks have a material and therefore located dimension. States can therefore easily regulate them. Even for interactions that occur purely on the internet, states can try to apply national legislation through technical intermediaries such as ISPs. Finally, citizens look to national governments to guarantee security and protection of fundamental rights.

Brousseau indicates that norm centers on the internet, be they governments or private actors, have an incentive to negotiate and cooperate to solve conflicts between norms. For private norm centers this negotiation is important in order to be able to attract users to the norm and for the norm to be a success. As noted above, governments also need to consider private norms when governments evaluate the efficiency of their own centrally created rules. Governments are motivated to do this in order to create optimal conditions for development of the knowledge-based economy. For Brousseau, the problem lies in coordinating between the various international *fora* involved in standards setting for the internet. Brousseau suggests the creation of a common blackboard, such as those used in many online communities, in order to share experience and best practices.

> *"It allows those who are in charge of setting collective orders to learn about the inefficiencies of the solution they implement. In addition, the way the conflict is solved can provide the to norm centers with solutions to avoid future conflicts." (page 648).*

Two key lessons emerge from Brousseau's work that are relevant for this thesis:

First, Brousseau's work highlights the interdependencies between state-imposed norms and self-regulation, particularly for internet-related activities. State-imposed norms constitute the necessary backstop against which private norm-setting and enforcement operate. By the same token, state-imposed norms must take account of self-regulatory norms in order to remain relevant and credible in digital environments.

Second, the "blackboard" approach recommended by Brousseau shows the importance of exchanging best practices and encouraging review and criticism of regulatory solutions.

The system for regulatory impact assessments I propose in Chapter 6 attempts to integrate these two key elements, *ie*. to take account of self-regulatory measures as a complement to state-imposed norms, and to ensure that impact assessments are shared so that best practices emerge.

7. INTERNET REQUIRES A "RACKET AND STRINGS" REGULATORY APPROACH

Court regulation and unilateral self-regulation are omnipresent. Internet service providers will always have terms of use that govern the rights of the service provider and the user, and that permit the service provider to terminate a user's account in certain circumstances. Service providers generally apply these terms of use with pragmatism and flexibility, basing their decisions on user complaints and on anticipated court enforcement of liability rules. Currently much of the way internet content is regulated is based on this two-pronged approach: courts enforce liability rules, *ie*. the notice and takedown rule combined with the liability safe harbor for internet intermediaries, and platforms develop and enforce their terms of use in the shadow of these court decisions. This reflects Brousseau's (2006) "multilevel" governance structure, where a centralized organization (generally the state) creates and enforces norms that constitute a backstop for private norms.

Policy makers debate today whether this two-pronged approach is sufficient to cover all situations. Italy, for example, has entrusted the independent regulator AGCOM with the responsibility for administering the notice and takedown regime. In France one regulatory authority (ARJEL) deals with blocking access to illegal gaming sites, and another (HADOPI) deals with applying the graduated response regime for online copyright infringement. A third authority, the CNIL, deals with "right to be forgotten" claims. An

institutional approach that cannot learn from its errors will create costs of its own in the form of regulatory failure.

A number of institutional options are available in addition to relying solely on court adjudication and unilateral self-regulation. The option being studied now in a number of domains, including data privacy, is co-regulation. Co-regulation attempts to overcome two of the main drawbacks of administrative regulation, ie. the limited access to information and the lack of flexibility in administrative regulatory solutions. Co-regulation also attempts to correct the main drawback of multilateral self-regulation, which is the absence of legitimacy and public interest objectives in the formation and enforcement of the underlying rules. The involvement of a state regulatory authority or agency will ensure that the underlying rules reflect public interest objectives while permitting flexibility. Many internet regulatory solutions may gravitate toward this co-regulatory approach.

The purpose of this chapter is not to propose an ideal institutional framework for dealing with access to harmful content on the internet. There are far too many moving parts for there to be a single institutional solution to fit all cases. As pointed out by Brousseau (2006), the ideal solution will generally incorporate some combination of centralized and decentralized rules. The institutional alternatives have to be considered in a broader context, taking into account fundamental rights and "better regulation" analysis, which will, among other things, attempt to measure harm to the internet ecosystem and the effectiveness of the proposed measure. This chapter's objective was to list the different types of institutional alternatives that currently operate in the internet field, and identify their principal strengths and weaknesses. By understanding the strengths and weaknesses of each institutional solution, it will be easier for policy makers to insert the institutional dimension into a broader methodology and thereby contribute to a more balanced framework for dealing with regulatory solutions.

CHAPTER 5 – PRINCIPLES OF BETTER REGULATION APPLIED TO THE INTERNET

1. INTRODUCTION

After the chapters on fundamental rights and institutional alternatives, this chapter focuses on the science of "better regulation," which is a methodological approach that focuses on the costs and benefits of regulation, including a consideration of other more effective alternatives. The key requirement of "better regulation" principles is the preparation of a regulatory impact assessment. "Better regulation" is now a major policy priority for the OECD, the United States and Europe. Better regulation methodology is exemplified in the European directives on regulation of electronic communications, to which I often refer in this thesis. However, the methodology can apply to any sort of regulatory proposal, including proposals to limit access to harmful content on the internet. This chapter will introduce the reader to "better regulation" principles under the guidelines issued by the OECD, the United States White House, and the European Commission. The chapter will close by mentioning some of the criticisms of better regulation methodology.

2. LITERATURE ON BETTER REGULATION

2.1 Early scholarship: Breyer, Morrall, Hahn, and Sunstein

The idea of "better regulation" was first examined in the 1980s by Stephen Breyer, then professor at Harvard Law School and soon to become a justice at the United States Supreme Court. Breyer argued for a more scientific approach to developing regulation, an approach that would take into account the effectiveness of the proposed regulatory measure, and the measure's anticipated costs compared to other alternatives (Breyer, 1982). Breyer identified some of the key factors of good regulation, including the level and costs of enforcement, transparency in the regulatory process, the legitimacy of the proposed measure, the need to involve stakeholders, and the measure's flexibility and simplicity. Breyer argued for a holistic approach to regulation, including the use of alternatives to classic "command and control" regulation. Those alternatives include liability rules, property rights, and taxes. Breyer underlined the informational asymmetries from which regulatory authorities suffer: regulators will necessarily have incomplete information when they adopt a regulatory measure, which means that such measures can be inefficient. Regulatory standards that specify the desired output ("performance standards") rather than specifying the techniques to be used to achieve the output ("designed standards") give flexibility to regulated entities, but may be more costly to enforce.

In an influential 1986 article, John Morrall III (1986) compared the cost-effectiveness of several regulations, measuring in each case the cost per life saved. Morrall found that the cost per life saved varied from $100,000 for regulation of automobile steering columns, to

$72 billion for regulation of formaldehyde. Morrall's work highlighted the huge differences in the cost effectiveness of regulatory measures, leading subsequent scholars, such as Robert Hahn and Cass Sunstein, to propose systematic scorecards and cost-benefit analyses to guide regulatory choices.

Professor at the University of Chicago, Cass Sunstein was also one of the early scholars promoting a scientific approach to developing regulatory proposals. Sunstein later became director of the United States Office of Information and Regulatory Affairs (OIRA), thereby becoming the United States's "regulatory czar". Sunstein's scholarship focused particularly on regulatory measures designed to protect the environment and to enhance safety (Sunstein, 2002; Hahn and Sunstein, 2002). Sunstein compared the costs of various regulatory measures, converting the costs into a common unit of measurement, such as "dollars per life saved". Sunstein argued that where resources are limited, they should be devoted in priority to measures that have the highest expected benefit per dollar spent. Sunstein also highlighted adverse effects that flow from certain well-meaning regulatory measures, such as the absolute prohibition of asbestos in the United States which led to a higher level of traffic deaths because of less effective braking systems. Imposing 0% cyanide content in drinking water creates inordinately high costs compared to a norm that would tolerate low yet harmless levels of cyanide.

2.2 Dieter Helm examines the meaning of "good regulation"

Helm (2006) criticizes policies under which better regulation is synonymous with deregulation. Helm cites the objective in the Netherlands to reduce the total amount of regulation by 25%, calling such an objective arbitrary. Helm likewise criticizes the UK better regulation task force's objective of eliminating one regulation for every new regulation adopted. This is referred to as a so-called "one in, one out" policy.

Helm's article takes a step back and asks the question how do we determine what the optimal level of regulation is?

Helm begins by explaining that regulation is deemed necessary when there is some identifiable market failure considered to be so great that intervention to correct it will be efficient, in the sense that the cost of intervention will be lower than the costs of the relevant market failure. Helm points out that the objectives pursued are not all efficiency objectives. Protection of equity and freedom, of horizontal equity (non-discrimination between individuals), and future equity *ie*. concern for future generations, are also objectives that regulation seeks to achieve. Helm points out that efficiency is not even a necessary condition for regulation. As an example, Helm indicates that large data sets of health information or publicly available medical research would advance science thereby improving the quality of healthcare. However, the protection of personal privacy counterbalances the efficiency argument to a large extent, resulting in regulations that

protect personal health records, sometimes at the expense of medical research and public health.

Helm explains (p. 172) why regulation is generally produced in excess supply. Helm analyzes the supply and demand of regulation, the effects of interest groups and the phenomenon of regulatory capture. The demand for regulation comes from well-defined constituencies with in some cases a powerful influence over regulators. Strong demand is fueled by risk aversion of the public and politicians' desire to do something about an identified risk. On the other hand, the demand for removing costly regulation is highly diffuse. Helm calls this the "dangerous dogs phenomenon": if a dog bites a child, regulation is called for; if, however, after the imposition of dangerous dogs regulation, dogs do not bite children any more, or less frequently, there is no demand to deregulate dogs. This aspect is also highlighted by the French Conseil d'Etat in its 2016 on the quality of laws and law making (Conseil d'Etat, 2016).

Helm also points out that regulators have indirect incentives to maintain a high supply of regulation. Their careers and budgets will depend on regulators being seen as providing an important resource to society.

Helm points out that markets themselves have public–good characteristics. Markets do not arise spontaneously, but require a legal framework to ensure trust and legal enforceability of contracts. Regulation is also needed to prevent anticompetitive behavior and to correct informational asymmetries. Public goods regulation is often a necessary condition for economic activity. Excess regulation can increase costs and reduce productivity. However, too little regulation also can have this effect. Helm, like the Conseil d'Etat (2016), argues that the design of regulation, rather than its level, is what matters most.

Regulation is justified if there are serious market failures, and if those failures are expected to have a greater efficiency cost than the cost of the intervention – government failure. (Helm, 2006, p. 177)

Helm cites a number of well-known market failures. On the demand side, consumers may lack adequate information or may express preferences that are not rational. This justifies many forms of regulation such as regulation of advertising, product safety, and the kinds of products that are available to minors. On the supply side, market power, pollution externalities are examples of market failures requiring regulation. As regards of the coordination of markets, Helm again reminds us that markets themselves have public goods characteristics and require regulation to function. Property rights are a precondition for markets, and their enforcement is itself an act of regulation.

Helm then examines cost-benefit analysis as a way to evaluate the relative benefits and costs of regulation. Cost-benefit analysis itself generates a cost, which sometimes

explains why cost-benefit analyses are not applied more broadly. Moreover, cost-benefit analysis does not always please politicians or regulators who have a preconceived idea of what is the right kind of regulation for a given problem.

In contrast to cost-benefit analyses, regulatory impact assessments generally focus on qualitative measurements of the expected costs and benefits. Helm criticizes the UK's better regulation task force which has identified five general principles that regulations should meet. Those principles include proportionality, accountability, consistency, transparency, and targeting. Helm indicates that these principles are so obvious as to be meaningless. Importantly, as long as it is a regulator that conducts the regulatory impact assessment, there is unlikely to be an objective evaluation. Regulators have a conflict of interest if they evaluate their own proposals.

Command-and-control regulation tends to create more opportunities for regulatory capture and therefore inefficient regulation.

> *"Market – based instruments have the significant advantage over command-and-control in that they tend to reduce the amount of information required to set the instrument, and hence to reduce the scope for capture"* (p. 179).

Any regulation that is informationally-demanding will be prone to regulatory capture.

Helm then turns to the design of regulatory institutions. According to Helm, independence works best when there are clear and separate objectives, and clear and separate instruments, and these objectives command a wide political consensus. But where objectives are multiple and conflicting, the trade-offs are best managed through the political process. Where a regulatory authority has a broad range of competing duties, the delegation of these duties creates scope for the exercise of discretion, thereby creating uncertainty. This reduces the predictability of regulatory decision-making, and affects the cost of capital.

3. OECD PRINCIPLES OF BETTER REGULATION

3.1 OECD 2012 Recommendation on Regulatory Policy

At an international level, better regulation methodology is reflected in the 2012 OECD recommendation on regulatory policy and governance (OECD, 2012). The OECD recommendation first includes an institutional requirement: There should exist within the government an institution that is independent of political influence whose sole job is to evaluate the quality of regulatory impact assessments that have been prepared by sponsors of proposed legislation and regulation. The independent body must have the support of central government and be able to reject proposals that are not accompanied by satisfactory regulatory impact assessments. The OECD recommendation states that the independent oversight body should have responsibility for providing training and

guidance on impact assessment to other parts of government. The existence of an independent review agency is also recommended by the French Conseil d'Etat (2016). The independent institutional review mechanism is what I later refer to as the peer review mechanism, which is critical to any "better regulation" process.

The OECD recommendation then provides guidance on how a regulatory impact assessment should be performed. First, the regulatory impact assessment should be conducted early in the process of decision-making so that it has a real influence on the debate. Ideally, the impact assessment should be done prior to public consultation and published as part of the consultation process. The OECD recommendation, like the United States government and European Commission guidelines we will examine below, states that the impact assessment must first start with describing the outcome that regulation seeks to achieve, such as the correction of a market failure or the need to protect citizens' rights. The OECD states that the impact assessment should then evaluate alternative ways of achieving the outcome including regulatory and non-regulatory actions, as well as preparing a baseline scenario of doing nothing. The alternative approaches should also include combined approaches such as using regulation in conjunction with education measures, and voluntary standards.

When a series of alternatives has been identified, the regulatory impact assessment should then assess the costs, benefits and risks associated with the alternatives. The regulatory costs should include direct costs and indirect costs borne by businesses, citizens and government. For impacts that are difficult or impossible to quantify, the regulatory assessment should provide qualitative descriptions of the expected impact. The objective of the impact assessment is to identify the approaches that are likely to deliver the greatest net benefits to society, i.e. the highest benefits at the lowest cost. (In Chapter 6 I will discuss ways to deal with hard-to-quantify benefits and costs.)

If a regulatory option might have an adverse effect on competition, authorities should look to alternative approaches that would have a lower adverse impact. (Breyer's work highlighted the effects of regulation on competition (Breyer, 1982)). Finally, the OECD recommendation notes that the impact assessment should evaluate whether international instruments would more effectively address the policy objective. The OECD recommendation states that government should take into account international standards, frameworks for cooperation, and the likely effect of national regulatory measures on entities outside the jurisdiction. This aspect is particularly important for measures affecting the internet. A national measure targeting internet intermediaries can easily have extraterritorial effects.

The 2012 OECD recommendations concern regulation in all sectors of the economy. In 2011, the OECD issued recommendations specifically targeting regulation of the internet.

3.2 OECD 2011 recommendations on internet policy making

The 2011 OECD recommendations on internet policy making emphasize the need for governments to take a due account of the open and globally interconnected nature of the internet when they adopt national rules designed to protect or enforce national norms on fundamental rights and acceptable content (OECD, 2011). The recommendations emphasize that the creation of rules should wherever possible respect the multi-stakeholder approach that has heretofore been used successfully for the creation of internet rules. National policy makers should wherever possible seek to make their rules compatible with the global norms established for the internet. The recommendations state that rules should be technologically neutral. Any national measures should respect the fundamental principle of allowing cross-border provision of services, which is central to the success of the internet. The recommendations state that barriers to the location, access and use of cross-border data facilities and functions should be minimized (OECD, 2011, page 7). The recommendations urge national policy makers to consider in priority self-regulatory measures such as codes of conduct that are backed-up by appropriate accountability measures. The codes of conduct should encourage and facilitate voluntary cooperative efforts by the private sector to respect the freedoms of expression, association and assembly online and to address illegal activity. Where self-regulation does not reach the desired result, other regulatory measures can be envisaged, but only as a second step.

The OECD recommendations call for data-driven policies, including using empirical evidence to evaluate the proportionality and effectiveness of regulatory measures. The recommendations point out that protection of intellectual property is necessary for innovation to continue to thrive on the internet, but that protection of intellectual property needs to be balanced with the need for robust competition and the protection of freedom of expression.

The recommendations note that the protection of internet intermediaries against liability for content provided by third parties is a key factor promoting innovation and creativity, the free flow of information and in providing the incentives for cooperation between stakeholders. The recommendations call for an assessment of the social and economic costs and benefits of any regulatory measure, including impacts on internet access, use and security. The evaluation of various policy options should be considered including their compatibility with the protection of all relevant fundamental rights and freedoms, and their proportionality in view of the seriousness of the concerns at stake. Any proposed legislative or regulatory measure should be assessed in light of its effective enforceability and its compatibility with fundamental rights.

In summary, the 2011 OECD recommendations on internet policy making, combined with the 2012 OECD recommendations on better regulation, contain all the principles that I will

attempt to operationalize in Chapter 6. In particular, the OECD guidelines require a precise diagnosis of the problem that regulation is supposed to cure, and an evaluation of the alternative methods available to cure the problem, including their respective costs.

4. BETTER REGULATION METHODOLOGY IN THE UNITED STATES

The first executive order imposing on the Federal government a methodology for testing regulatory proposals was issued in 1981 under the Reagan administration.[58] That executive order was then updated by subsequent executive orders, signed by Presidents Bush, Clinton and Obama. The idea of testing proposed regulation against a cost-benefit methodology has been supported by both Democratic and Republican presidents in the United States. Under Republican presidents, the better regulation methodology was presented as a means to reduce the amount of federal regulation. Under Democratic presidents, the methodology was presented as a way to get more benefit from federal regulatory intervention.

As described on the Office of Information and Regulatory Affairs' (OIRA) website:

> *"Regulatory analysis is a tool regulatory agencies use to anticipate and evaluate the likely consequences of rules. It provides a formal way of organizing the evidence on the key effects -good and bad - of the various alternatives that should be considered in developing regulations. The motivation is to (1) learn if the benefits of an action are likely to justify the costs or (2) discover which of various possible alternatives would be the most cost-effective."*[59]

4.1 Peer review by OIRA

An important aspect of the United States better regulation system is that it imposes peer review by a special office in the White House, called the Office of Information and Regulatory Affairs (OIRA). For any regulatory proposal, the government agency that sponsors the proposal must draw up a cost-benefit analysis that follows the methodology imposed by the executive order and by Circular A4 issued by the White House. The cost-benefit analysis is then submitted to the OIRA for review. If the OIRA is not satisfied with the analysis, the OIRA can ask for further analysis or even reject the proposal. OIRA's responses are called either "return letters" or "review letters." The OIRA website contains a dashboard showing the number of regulations under review.[60] However, the website displays very few "return" or "review" letters.[61]

This system of institutional peer review by OIRA is similar to the system put in place in Europe for the review of telecommunication regulations that Member States propose to implement. Each proposal must be submitted to a so-called Article 7 Task Force within

---

58 White House Executive Order 12291.

59 White House Office of Information and Regulatory Affairs (OIRA) Q&As, https://www.whitehouse.gov/omb/OIRA_QsandAs accessed February 28, 2016.

60 On April 7, 2016, there appear to be 126 regulations under review: http://www.reginfo.gov/public/jsp/EO/eoDashboard.jsp

61 http://www.reginfo.gov/public/jsp/EO/letters.jsp

the European Commission, and the Article 7 Task Force can require further justifications, or even veto certain measures.

The United States better regulation methodology only applies to regulatory proposals generated by federal government agencies. The rules do not apply to proposals generated by independent regulatory authorities such as the FCC or the FTC (Fraas and Lutter, 2011). This means that regulatory proposals that affect the internet are generally not subject to the White House's better regulation rules. Fraas and Lutter (2011) showed that few regulations issued by the FCC and the FTC contained any cost-benefit analysis. United States law would therefore have to be modified to permit OIRA to review internet-related proposals. The OIRA review mechanisms also do not apply to legislative proposals debated in Congress.

Circular A4 provides guidance on how the cost-benefit analysis should be applied. The next sections will describe these guidelines.

4.2 Creating a baseline scenario

According to Circular A4, the first step is to establish a baseline scenario, or counterfactual, against which alternative options can be compared. The baseline scenario represents the situation that would exist if no new regulation were adopted. This baseline scenario does not represent a fixed picture of the status quo, but rather a forecast of what is likely to happen in the absence of a new regulatory solution. In the field of internet regulation, the baseline scenario might take into account the fact that other existing legal provisions such as competition law, consumer protection law or class actions might expand to address the relevant harm. In the United States, the Federal Trade Commission Act contains a provision prohibiting any unfair or deceptive practice. It is possible that the Federal Trade Commission could apply this broad provision to issues relating to net neutrality, for example. When evaluating the baseline scenario, this kind of phenomenon should be considered before developing alternative scenarios.

4.3 Identifying the relevant harm

Another critical starting point for the cost-benefit analysis is to define precisely the problem that needs to be addressed. The harm that regulation is intended to address should if possible be classified in terms of a market failure. Circular A4 characterizes different kinds of market failures that may require regulation. The first form of market failure is the existence of externalities that may arise from high transaction costs and/or poorly defined property rights that prevent people from reaching efficient outcomes through market transactions. Limited public resources, such as electromagnetic spectrum or national parks, may require regulation in order to avoid becoming overused. Public goods are likely to be under-produced by the market and therefore may require regulatory intervention in order to ensure an optimal level of output. Examples of public

goods are national defense or basic scientific research. Posner (2011) characterizes good political ideas as a public good that are likely to be under-produced in the absence of regulation protecting freedom of expression.

Another form of market failure results from the exercise of market power, either unilaterally or collectively. This form of market failure is generally addressed by competition law. Inadequate or asymmetric information can also result in a market failure because consumers will make sub-optimal choices based on their inability to access information, or their inability to make rational decisions based on information available to them. This latter aspect relates to behaviorial economics and the "bounded rationality" of humans (Kahneman, 2003; Thaler and Sunstein, 2008). Informational measures such as labeling may be required to address this form of market failure.

Circular A4 mentions additional objectives of regulation that may not necessarily be characterized as a market failure but that are important to enhance the protection of fundamental rights. Several law and economic scholars characterize inadequate protection of fundamental rights as a form of market failure, because the market produces a sub-optimal level of protection of the relevant right without regulatory intervention (Posner, 2011). For example, rules on freedom of expression are often characterized as necessary to assure the proper functioning of the market for ideas. Circular A4 characterizes fundamental rights objectives as something other than market failures. The question of whether inadequate protection of fundamental rights is a "market failure" does not have to be resolved here. The outcome does not affect our proposed methodology. The point rather is that the proponent of a regulation must carefully describe the problem that the regulation is intended to address. The relevant harm can in most cases be characterized as a form of market failure.

4.4 Identifying regulatory options

The next step in Circular A4's cost-benefit methodology is to identify a number of options that would permit the treatment of the relevant harm. During this stage, policymakers should keep an open mind and identify all potential regulatory and non-regulatory solutions that would address the problem. Solutions might include increased enforcement of competition law, increased enforcement of existing consumer protection law, or use of liability rules to address the relevant harm. When examining the alternative approaches that might be used to address the market failure, the proponent of regulation should consider market-oriented approaches, such as marketable permits, changes in liability or property rights or even insurance rules that would nudge market actors toward the desired result. Other alternatives may include informational measures (*eg.* labeling) to ensure that relevant information is available to consumers. Informational measures may include standardized tests or labeling requirements.

Circular A4 emphasizes that performance standards should be considered in preference to design standards. Performance standards specify the relevant output to be achieved but do not impose a particular method or technology for achieving that output. Performance standards are technologically neutral and give flexibility to firms to achieve the desired result in the manner that is most efficient for them.

Circular A4 does not say that self-regulatory measures should be considered as an alternative. For internet regulation, however, self-regulatory or co-regulatory solutions, including policycentric governance structures, are often the preferred means of regulation, for the reasons explained in Chapter 4. Consequently, although self-regulation and co-regulation are not expressly mentioned in Circular A4, any consideration of regulatory alternatives would necessarily include self-regulatory or co-regulatory solutions designed to limit access to harmful content on the internet. Indeed in most cases, any new regulatory proposal designed to address market failures relating to harmful content on the internet would have to be measured against existing self-regulatory arrangements, such as those already in place to fight child pornography or online copyright infringement.

4.5 Applying cost-benefit analysis to each alternative

Once a range of alternatives has been identified, the third and most critical step under Circular A4 is to apply a cost-benefit analysis to the various approaches. Circular A4 identifies two methodologies that can be used: Either a benefit-cost analysis (BCA) or a cost-effectiveness analysis (CEA). According to the circular, the CEA should be used where benefits are difficult or impossible to quantify or monetize. The CEA compares the costs of several approaches and determines which one achieves the desired (but unquantifiable) objective at the lowest cost. A BCA, on the other hand, requires a comparison of the total benefits of a given approach to the total costs. The approach with the highest net benefit should be given preference over other alternative approaches. Circular A4 points out that the benefits of a measure affecting public health should be converted into some kind of measurable unit, such as the number of equivalent lives (ELs) saved or quality adjusted life years (QALY) saved. In the context of measures designed to limit access to harmful content on the internet, measuring the benefits of any regulatory alternative will be almost as challenging as measuring the value of human life. The expected output of the regulation would be improvement in the protection of human dignity and/or the protection of national security. Converting these benefits into measurable units will be difficult, but not necessarily impossible. The benefits flowing from reduced online copyright infringement will be easier to measure. I will examine the problem quantification in more detail in Sections 4.6 and 4.7 below. In Chapter 6, I recommend that benefits which cannot be converted into monetary units be converted into some other measurable units, or "success factors". This would permit a CEA to be applied.

Circular A4 then points out that any regulatory analysis should describe separately the distributional effects that would flow from the various alternatives. Distributional effects relate to whether certain classes of consumers or businesses will be more impacted by the alternatives than other classes. Distributional effects may require that transfer payments be organized to ensure that the burden of a given regulatory measure is distributed equitably among members of the population.

4.6 How to quantify costs and benefits

The remainder of Circular A4 then concentrates on how to quantify various costs and benefits flowing from a given regulatory approach. The first task in measuring costs and benefits is to develop a baseline model, or counterfactual, against which other alternatives can be measured. As noted above, the baseline model consists of the option of no regulatory intervention. Doing nothing does not consist simply of a snapshot of the *status quo*. On the contrary, the baseline model should attempt to project how the market will evolve over time under the "no regulation" approach. This would include taking into account evolution of the market, possible technological disruption, and the evolving application of existing laws such as competition law and liability rules. In the field of internet regulation, developing a baseline scenario would be particularly challenging given the uncertainties surrounding technological and market developments. A service may appear to dominate the market today, but in two years the service may be completely displaced by a new disruptive solution (Shelanski, 2013).

The alternatives selected for analysis should then be presented according to their level of stringency. The most stringent alternative would be the one that achieves the highest output, such as the highest level of enforcement of the desired policy objective. That high level of enforcement would presumably be accompanied by a high level of cost. In the field of limiting access to harmful internet content, the most stringent alternative might be the systematic use of deep packet inspection to detect and block the relevant content. However, this most stringent option will create high costs. In the case of deep packet inspection, the costs would correspond to the deployment of equipment, but more importantly the unacceptable threat to the right of privacy and freedom of expression for internet users.

Other alternatives should then be presented in decreasing order of stringency. By presenting the alternatives according to their level of stringency, it may be possible to measure the incremental difference in costs and benefits between each level of stringency, as well as reject solutions that generate manifestly unacceptable costs.

The appropriate concept for measuring benefits and costs is the opportunity cost of choosing one alternative over another. The quantification of benefits and costs should correspond to the willingness to pay (WTP), which is the amount an individual would be

willing to pay to benefit from a certain outcome. Circular A4 also mentions that willingness to accept (WTA) can be another yardstick for measuring the value of a certain benefit. As mentioned in Chapter 3, willingness to pay and willing to accept do not always coincide. Experiments in behavioral economics show that once people possess a certain benefit, they will insist on a fairly high price to give it up. This is referred to as the endowment effect. By contrast, a person who does not hold the benefit would in some cases not be willing to pay a high amount in order to obtain it. Thus the willingness to pay may be smaller than the willingness to accept. As mentioned in Chapter 3, this has been shown to hold true in the context of measures to protect privacy. However, the endowment effect is a more general phenomenon extending well beyond the field of privacy.

Circular A4 indicates that costs and benefits should be valued wherever possible through reference to actual market behavior, *ie*. "revealed" preferences based on actual market transactions. However, in many cases there may lack market data to conduct a revealed preference study. Preserving the environment or cultural amenities are benefits that are not traded directly in markets. In some cases it may be possible to use the prices of other goods and services as a proxy for benefits such as a clean environment. This is called hedonic pricing. For example, differences in real estate prices may provide some indirect evidence of the value people attribute to a healthy environment.

Circular A4 distinguishes between use values and non-use values. A use value arises where an individual derives utility from the actual use of a resource, such as the pleasure of swimming in a clean river. Nonuse values correspond to the value that an individual attributes to a given situation even though he or she will not directly use the relevant resource. For example, an individual may attribute value to the preservation of an endangered species, even though the individual herself will never see or otherwise benefit directly from the species.

Where revealed preferences cannot be determined from market transactions, the qualification of the cost or benefit may have to be derived from stated preferences. Stated preferences are based on questionnaires designed to get people to express as honestly as possible what they would be willing to pay for a given benefit. Surveys need to be designed carefully so that individuals take into account in their answers their own expenditure limitations and the availability of other alternative goods and services. The stated choices expressed in the questionnaire would therefore come closer to an individual's actual behavior in a market transaction. The stated preferences method was recently used in a study commissioned by BEREC to determine what value individuals attribute to net neutrality (WIK Consult *et al.*, 2015).

Where it is possible to conduct neither a revealed preference study nor a stated preference study, Circular A4 states that a "benefit transfer" method can be used as a last resort. The benefit transfer method consists of using studies conducted in other contexts,

and then trying to extrapolate the results of these studies to the current situation. For example, a study estimating the value of a saved human life might be used to help estimate the value of certain fundamental rights (*see*, Chapter 6 below).

4.7 Benefits and costs that are difficult to monetize

Circular A4 contains a section focusing on benefits and costs that are difficult to monetize. Even if they cannot be transformed into monetary units, benefits should be converted into some kind of measurable units so that various regulatory options can be compared. For example, an internet regulatory alternative that provides a high degree of protection of user privacy might be given a privacy score of five out of five, whereas another alternative that is less protective of privacy might receive a score of only two out of five on the privacy scale. (This is roughly what Robert Alexy proposes in his fundamental rights weighting formula. *See,* Chapter 3, Section 5.7.) Benefits and costs that are difficult to quantify should be described in detail so that the reader of the cost-benefit analysis can understand the nature, timing, likelihood, location, and distribution of the unquantified benefits and costs.

In the field of internet regulation, one of the most difficult costs to measure is the negative impact that a regulatory choice might have on innovation. We know that light-handed regulation of the internet is one of the factors contributing to the high level of innovation. However we do not know with any certainty how much innovation would be lost by moving the regulatory needle in the direction of more regulation. The effect of regulation on innovation is examined in Section 6 below.

The remainder of Circular A4 examines the particular problems associated with monetizing health and safety benefits and costs. Unlike safety regulations designed to reduce traffic fatalities, Internet regulation designed to limit access to unlawful content does not always have a direct link to health or to life expectancy. Much of the discussion of the value of statistical life or of statistical life years extended will have little applicability to our subject. Thus other approaches to measurement are needed.

The estimate of costs and benefits over time should take into account changes in technology. In the field of internet regulation changes in technology and markets can often treat a market failure without the need for regulatory intervention (Shelanski, 2013). As noted above, evaluating technological change is particularly important when developing the baseline scenario of doing nothing. Serious consideration should be given to the likelihood of technology bringing an answer to the relevant market failure without regulatory intervention.

Finally, Circular A4 describes how the cost-benefit analysis should treat uncertainty. The principal rule is that any tool that is used to integrate uncertainty must be fully disclosed so that an outside reader can understand the relevant choices made. The author of the

cost-benefit analysis should present an estimate of the probability distribution of regulatory benefits and costs. The cost-benefit analysis should contain a numerical sensitivity analysis to examine how outcomes change with variations in the underlying assumptions. Robert Alexy's weighting formula described in Chapter 3 also contains an uncertainty coefficient designed to discount certain estimates based on the level of uncertainty associated with the estimate.

5. BETTER REGULATION METHODOLOGY IN EUROPE

5.1 European better regulation guidelines

Proposed legislation drafted by the European Commission must undergo an impact assessment before being presented to the European Parliament and European Council for consideration. The European Commission first established the impact assessment process in 2002. The process was updated in 2009, and once again in 2015. The impact assessment is based on a cost-benefit analysis. Unlike the United States cost-benefit analysis, which only applies to regulatory measures adopted by the United States government, the European system applies to legislative measures, including legislation addressing broad policy issues. Renda *et al*. (2013) point out that this makes the application of cost-benefit analyses particularly challenging, because it requires an economic analysis not just of technical implementation measures, but of laws affecting societal values.

In addition to the European Commission's cost-benefit analysis, certain member states have established their own rules for impact assessments. The UK and the Netherlands are leaders in the field, with rigorous impact assessment procedures for their own national legislation. France has a formal requirement for an impact assessment, but the assessment to date is largely qualitative.

European legislative proposals are created in the first instance by the European Commission. Under the Commission's better regulation procedures, legislative proposals must be accompanied by an impact assessment. The impact assessment must comply with the Commission's 2009 Guidelines on Impact Assessments. The impact assessment is then submitted to the Commission's Impact Assessment Board (IAB) for peer review. Like the OIRA in the United States, the IAB evaluates the adequacy of the impact assessment in light of the Commission's guidelines. The IAB may send the proposal back to its authors because of inadequate analysis. According to the IAB's 2014 report, this occurs roughly 40% of the time (IAB 2014).

5.2 European Commission guidelines assessing fundamental rights in impact assessments

The Commission has published a number of operational guidelines on how to assess various kinds of impacts of proposed legislation. Importantly for internet regulation, the

Commission published in 2011 guidelines on how to assess impacts on fundamental rights (European Commission, 2011). The 2011 guidelines refer to the Commission's fundamental rights checklist, which the Commission says must be considered in connection with each legislative proposal:

> **"Fundamental Rights 'Check-List'**
>
> *1. What fundamental rights are affected?*
> *2. Are the rights in question absolute rights (which may not be subject to limitations, examples being human dignity and the ban on torture)?*
> *3. What is the impact of the various policy options under consideration on fundamental rights? Is the impact beneficial (promotion of fundamental rights) or negative (limitation of fundamental rights)?*
> *4. Do the options have both a beneficial and a negative impact, depending on the fundamental rights concerned (for example, a negative impact on freedom of expression and beneficial one on intellectual property)?*
> *5. Would any limitation of fundamental rights be formulated in a clear and predictable manner?*
> *6. Would any limitation of fundamental rights:*
> *- be necessary to achieve an objective of general interest or to protect the rights and freedoms of others (which)?*
> *- be proportionate to the desired aim?*
> *- preserve the essence of the fundamental rights concerned?"*

The guidelines require that the impact assessment first make a list of the fundamental rights that are affected, either positively or negatively, by the regulatory initiative. Any fundamental rights that are absolute, *ie.* that cannot be interfered with under any circumstance, should be identified. As explained in Chapter 3, absolute fundamental rights include the right not to be tortured. Where the proposal deals with fundamental rights that can be interfered with given an appropriate justification (which include the key rights we are concerned about here), the author of the proposal must describe in concrete terms how a given right is affected.

The guidelines focus on the transparency of the measure. In other words, is the extent of the interference clearly understood and limited in the proposal, or is the interference subject to different and potentially arbitrary interpretations? The guidelines also require a consideration of alternative mechanisms that would have a lesser negative impact on the relevant fundamental right, and a precise description of safeguards that will be included in the proposal to mitigate the adverse effect on fundamental rights.

The effects on fundamental rights must be quantified wherever possible, and included in the general cost-benefit assessment under one of the three categories defined in the Commission's Impact Assessment Guidelines: economic, social or environmental impacts. The guidelines emphasize that the cost-benefit analysis of fundamental rights should not be inserted in a separate standalone section of the impact assessment. This is because a limitation or promotion of a fundamental right will generally have an economic

or social effect. The effect should therefore be measured in one of those two sections of the impact assessment.

5.3 2015 European toolbox for better regulation

On May 19, 2015 the European Commission released a new version of its better regulation documents, including a detailed toolbox to assist in completing impact assessments (European Commission, 2015). The Commission's toolbox requires first that for any regulatory proposal, the proponents of the regulation verify the existence of a problem, analyze the causes of the problem, who is affected, and the likelihood that the problem will persist without regulatory intervention. The toolbox requires that the impact assessment identify the "drivers" of the problem, so that a linkage can be created between the drivers or causes of the problem and the targeted regulatory intervention. The analysis of the current problem requires development of a baseline ("counterfactual") scenario, i.e. an evaluation of how the problem will evolve over time without regulatory intervention, taking into account recent trends and implementation of existing policy at all levels.

(a) Underlying drivers of problems

When identifying the underlying causes of problems requiring regulatory attention, the toolbox points to four potential situations.

(i) Market failures.

The toolbox identifies six different situations that fall within the category "market failures". The first is externalities, i.e. where market prices do not reflect how one activity produces costs or benefits for other activities. The second market failure is the problem of public goods. Public goods are typically undersupplied by the private market because private producers will not earn a sufficient return on investment. National defense, public health and welfare programs, preparedness for natural disasters are examples of public goods. As we saw in the chapter on fundamental rights, good political ideas can also be considered a public good, which are underproduced in the absence of laws protecting freedom of expression.

A third situation within the category of market failures is non-existent or weak competition. Where there is weak competition, prices may be excessive or the market may produce suboptimal levels of certain goods or services. Competition issues are generally addressed by competition law, or in some justified cases (e.g. telecoms) targeted economic regulation. The fourth subcategory of market failures is the case where markets are missing or incomplete. This is a situation where goods or services that are needed by society are not produced at all. The toolbox gives the example of a major new infrastructure project that cannot be financed through market forces because user

charges would be insufficient to permit a return on investment. Another example cited by the toolbox is the need for a student loan, which may not be met by the market alone.

The fifth category of market failure is the problem linked to principal / agent misalignment. This form of market failure arises when there is a misalignment of incentives between market actors. For example, when a tenant is responsible for paying heating bills, the landlord will have no incentive to provide insulation.

The last form of market failure is imperfect information. For markets to function efficiently, market participants need information on product quality and prices. Information asymmetries can lead to suboptimal market outcomes. For example, inadequate information about product quality can lead purchasers to assume that all products have a low level of quality (Akerlof, 1970). This in turn penalizes producers of higher quality goods and will lead the market in general to move toward low quality products only, creating a so-called "lemons" market.

(ii) Regulatory failures.

After market failures, the next category of situations that can cause a problem requiring regulatory attention is a "regulatory failure". A regulatory failure occurs where a government intervention fails to achieve the desired objective. This may occur because the regulation, or the regulator, ends up being unduly influenced by certain industry groups. This phenomenon is known as "regulatory capture". Regulatory failure may occur also because of unanticipated side effects flowing from the regulation. For example, a regulation designed to reduce online copyright infringement might have the side effect of encouraging large number of internet users to use encryption, thereby making law enforcement more difficult. Another cause of regulatory failure may be that an existing regulation exists, but is poorly implemented and/or enforced. Or the regulation may simply be out of date, and be ill-adapted to market and technology developments.

(iii) Equity.

A third situation requiring regulatory attention may be equity considerations. Equity considerations may include inadequate protection of fundamental rights, or excessive discrimination based on race or sexual orientation. Equity failures may also be considered forms of market failures, because the market produces insufficient amounts of certain socially-desirable rights, such as equal access to education.

(iv) Behavioral bias.

The fourth and last category listed by the European Commission's toolbox is inefficient market outcomes due to behavioral bias and bounded rationality of consumers. A classic example of this is the fact that most consumers will not change the default options presented on a website even though rationally it would be in their interest to do so.

Some of these categories of underlying problem drivers could likely be considered forms of market failures. For example, the problem of behavioral bias could likely be classified as a form of market failure instead of put in a category of its own. The categories mentioned by the European Commission are not important in themselves -- what is important is the requirement that policymakers carefully identify the underlying failure – be it a market failure, regulatory failure or equity failure - that creates the problem that policymakers want to address.

(b) Quantify the risk, and determine an optimal level of risk reduction.

Under the toolbox's methodology, after identifying the problem and the key drivers for the problem, the sponsor of a regulatory proposal should attempt to characterize the negative outcome that the identified problem will cause, its level of severity, and the likelihood of the harm occurring. The resulting risk (hazard multiplied by the probability of its occurrence) should then if possible be quantified. The impact assessment should then attempt to define tolerability criteria, including levels that would be considered an intolerable risk, a tolerable risk, or an acceptable risk. According to the Commission's toolbox, policymakers should seek an optimal level of risk reduction. This optimal level is found where the marginal costs of risk reduction equal the benefit derived from the marginal reduction in risk. The risk management approaches can focus on reducing the severity of the hazard, or limiting the likelihood of its occurrence, or a combination of both.

(c) Identify policy options.

The next step described in the toolbox is to identify a wide range of possible policy options to address the problem, and then narrow down these options to a small handful that merit in-depth analysis. When making the first selection of available policy options, the proponents of regulation should "think outside the box", and choose a wide range of instruments, from less intrusive to more interventionist alternatives. Classical regulatory tools should be envisaged as well as newer cutting-edge methods such as those that flow from a study of behavioral economics. According to the Commission's toolbox, the range of possible policy options should always include the baseline scenario of no new regulation. Under the baseline scenario, existing law would be applied to the problem. International standards should be taken into account and included as one of the policy options so as to promote international consistency of rules. Self-regulatory or co-regulatory solutions should be considered as well as market-based incentives.

The better regulation toolbox identifies four main categories of regulatory instruments that should be considered:

- "Hard" legally binding rules;
- "Soft" regulation;

- Education and information;
- Economic instruments.

The toolbox describes the main characteristics of each of these kinds of legal instruments referring where appropriate to additional European Commission guidance and best practices. The Commission's toolbox includes within the category "economic instruments" the use of tax and liability rules as well as marketable property rights as ways to influence behavior of economic agents. The Commission points out that each of the legal instruments might be used in combination, to support one another. For example, liability rules may be used as a backstop to supplement self and co-regulatory solutions. Finally, the Commission emphasizes that ideas for effective policy instruments could emerge from the study of behavioral economics.

(d) Narrowing the choice of available options.

Once all options have been put on the table, the proponent of regulation must select a small package of options that merit more in-depth analysis. According to the toolbox, the baseline scenario must always be included in this final line-up of options. Regulatory options that are not legally feasible or that would disproportionally harm fundamental rights should be discarded from the outset. The impact assessment should focus on a group of realistic policy options in addition to the baseline scenario. The toolbox emphasizes that the initial selection process should explain the reasons for discarding certain regulatory options so that the relevant stakeholders who suggested those alternatives can understand why they were eliminated. Moreover, the drafter of the impact assessment should avoid including an option that is a "straw man" alternative, i.e. an alternative whose only purpose in the impact assessment is to lead the reader to reject it and prefer another alternative.

5.4 **The Renda study on cost-benefit analyses**

Renda *et al*. (2013) studied cost-benefit analyses in the context of EU rulemaking, breaking down costs and benefits into six "areas," depicted graphically as follows:

Source: Renda *et al*. (2013), p. 21

(a) Quantifying Costs.

Renda's approach divides costs and benefits into "direct" and "indirect."

(i) Direct costs consist of:

- Direct compliance costs incurred by the regulated firms, including fees or levies, one-off costs, recurrent costs, additional administrative burdens caused by the regulation.
- Hassle or irritation costs, ie. costs created by additional regulation that are difficult to quantify and therefore are not included in the first category of costs.
- Enforcement costs.

A word about enforcements costs is in order: the costs of enforcing a legal rule are a key consideration in any cost benefit analysis. A rule that costs 10 to enforce while yielding a benefit of 5 does not increase social welfare. Enforcement costs include both public and private costs. The costs and delay associated with pursuing a private lawsuit are a form of enforcement cost. Renda *et al*. (2013) divide enforcement costs into five categories:

- One-off adaptation costs, such as those associated with training personnel about a new legal rule;
- Information costs and administrative burdens, which include the cost of collecting information relevant for enforcement.
- Costs of monitoring compliance. Monitoring costs will be lower when the obligation consists of a detailed rules as opposed to a general standard.
- Pure enforcement costs, such as the costs of handling complaints.
- Adjudication/litigation costs, including the cost of lawsuits.

(ii) Indirect costs consist of:

- Indirect compliance costs, eg. costs that result from increased prices charged by the regulated firms.
- Other indirect costs, such as:
    - Substitution effects on consumption. One example of substitution effects would be consumers' use of alternative streaming technology in response to a regulation designed to detect and punish peer-to-peer online copyright infringement.
    - Transaction costs: where a regulation increases the cost of identifying counter-parties and negotiating with them, the increase in transaction costs must be taken into account.
    - Reduced competition and inefficient resource allocation. These costs would occur where a regulation makes it more difficult for competitors to enter the market, or

prevents firms from competing aggressively, or favors collusion. Standards can sometimes have this effect (Breyer, 1982).

- Reduced market access: if a regulation reduces market access opportunities for a certain class of producer, this will reduce consumer choice and create costs.
- Reduced investment and innovation: regulation can reduce the incentive to invest in new infrastructure or innovative products. For example, a regulation that requires a firm to provide competitors with access to the firm's infrastructure at cost-oriented prices can reduce the expected return on investment for new projects, and thereby reduce the firm's incentive to invest and/or innovate. A regulation that reduces the open, end-to-end character, of the internet, may reduce innovation by edge providers by increasing uncertainty as to the application's ability to reach consumers around the world.
- Uncertainty and investment: uncertainty as to the future regulatory environment can also reduce the expected return on investment and thereby have an adverse effect on investment.

Renda *et al*. (2013) omit a category of indirect costs linked to impairment of a fundamental right. Such costs will be difficult to quantify, but should be included as a separate category of indirect costs caused by a regulatory intervention. For example, a regulation that protects the so-called "right to be forgotten" will enhance the right to data protection, but will restrict freedom of expression. The promotion of data protection is counted as a benefit; the impairment of freedom of expression should be counted as a cost, and both must be counted.

Renda *et al*. describe the total cost of a proposed regulation as the sum of direct costs (DC), indirect costs (IC) and enforcement costs (EC), *ie*. total cost of regulation = DC + IC + EC

(b) Quantifying benefits.

On the benefits side of the equation, Renda *et al*. (2013) distinguish again between direct and indirect benefits. In the category of direct benefits, Renda speaks first of improvements to individual wellbeing. These improvements may include enhanced life expectancy, a better environment, or improved political rights. A second category of direct benefits consists of improved market efficiency. For Renda, this category includes the objective of correcting market failures: externalities, insufficient supply of public goods, missing or weak competition, missing or incomplete markets or information failures. When speaking of market efficiency, Renda distinguishes between productive efficiency, allocative efficiency, and dynamic efficiency. Renda's distinction between individual wellbeing and market efficiency can of course lead to a double counting. A regulation that is intended to reduce air pollution targets an increase in wellbeing, i.e. the value that individuals attribute to a clean environment, as well as a market failure, i.e. the negative externalities created by diesel-powered automobiles, for example.

Renda then describes indirect benefits flowing from a regulatory proposal. Those indirect, or spillover, benefits include benefits deriving from third party compliance with legal rules. For example, regulations that increase market efficiency and productivity can lead to lower prices which in turn benefit consumers. Another category of indirect benefits is wider macroeconomic benefits that flow from the proposed regulation.

(c) Distributional effects

Renda's methodology then calls for an analysis of how the various costs and benefits impact different categories of stakeholders. The categories of stakeholders may include consumers, businesses, governments or non-EU countries. Some impacts of regulation may affect citizens more broadly, and not just consumers.

5.5 Areas requiring further study

Existing methodologies for cost benefit analysis generally treat fundamental rights as a separate stand-alone question. Aside from Robert Alexy (2012), the approach for quantifying the impact on fundamental rights, either positive or negative, has not been studied. Attempts to integrate fundamental rights into the cost benefit analysis have so far lacked analytical rigor. Renda's thorough study on cost-benefit analyse devotes very little attention to fundamental rights.

The other area that requires more study is how to evaluate impacts, positive or negative, to the internet ecosystem. The term internet ecosystem refers to the existing technical, governance and regulatory approaches that have permitted unprecedented innovation, particularly at the applications level. A regulatory policy that changes one of the elements in the current internet ecosystem may disrupt the ecosystem and have an impact on innovation. I have not seen any attempt to factor these impacts into a regulatory cost-benefit analysis.

6. IMPACTS ON INNOVATION

The sections below attempt to capture how some authors view the link between regulation and innovation. Because the impact of regulation is not the key theme of this thesis, the summary below is necessarily incomplete and superficial.

6.1 Why internet firms innovate

Viscusi *et al*. (2005) indicate that regulation can have an effect on innovation in several ways. First, when regulation leads to prices being set above costs, the profits generated by the regulated firm can be reinvested in research and development. Second, above-cost prices caused by regulation will encourage new market entry which in turn will fuel innovation as the firms entering the market compete on price. Where regulated prices are low, firms will not compete on price but on product differentiation.

A number of internet-based businesses are based at least in part on free services for the end-user. High prices are therefore not a factor in encouraging market entry. Indeed most internet-based businesses earn no profits for a significant time after their creation. The search for short term profit will therefore not generally be a factor in market entry and innovation for internet businesses. However, successful internet businesses can scale quickly, reaching hundreds of millions of users in a few short years. The ability to reach users around the world rapidly and with relatively low capital expenditure attracts early-stage investors. The rapid scalability of internet-based businesses will lead investors to give high valuations to internet start-ups that have a promising new technology or business model. Venture capitalists invest with the hope that the start-up will go public through an initial public offering, or will be sold in an industrial sale. Venture capital investment permits innovators in the internet field to become multi-millionaires in a very short time. For internet entrepreneurs, the key motivation for innovation will be to enhance parameters that create the highest valuation for the business in the eyes of venture capitalists. Currently, those parameters do not include whether the business can earn a profit in the short term. Typical parameters include the rate of progression of individual users of the service, the ease with which the service can be replicated by another competitor, and the likelihood of the business becoming the first to reach a global scale. If all these parameters are favorable, the internet entrepreneur's business may have a valuation of many millions of dollars even though the service has relatively few users, and no immediate likelihood of earning a profit.

For more established companies such as Google, Facebook, and Apple, the principal motivation for innovation comes from the threat that their existing technologies and business models could be rendered obsolete by new entrants. It is the contestability of internet markets (competition "for the market") that pushes innovation even within companies that have reached the top of the food chain in a particular internet business (Shelanski, 2013).

If we take these factors for innovation into account, then any regulation that hinders the rapid scalability of a new internet business, including its ability to reach a global market, will hurt innovation, because it is this characteristic that drives valuation of internet businesses, as well as the contestability of existing internet players.

6.2 Knut Blind explains link between regulation and innovation

Blind (2012) surveys economic literature on how regulation can affect innovation, either in a positive or a negative way. Not surprisingly, the literature shows that the effect of regulation on innovation varies depending on the type of regulation, the industry sector, and the institutional environment. The size of the company is also a factor in the company's ability to adapt to new regulation and continue to innovate in spite of new compliance costs. There is no "one size fits all" correlation between regulation and

innovation. Blind points out that new regulatory obligations can spur innovation for compliance, or innovation for avoidance. Innovation for compliance is when a new regulation that has a broad scope, such as fuel efficiency requirements for motor vehicles, will spur innovation among companies to try to comply with the regulatory obligation in the most efficient way possible. Innovation for avoidance refers to the situation where a regulatory obligation has a relatively narrow scope of application, and the company's innovation consists of finding ways to avoid application of the regulation. An example of "innovation for avoidance" would be regulation on providers of electronic communications services. In light of the regulatory burdens associated with providing electronic communications services to the public under European law, companies may innovate to seek ways to provide a comparable service that does not fall within the regulatory definition of electronic communications service.

Blind's survey of literature shows that the effects of regulation on innovation cannot be reduced to a single formula, but must be evaluated on a case by case basis. Blind emphasizes, however, that the effect on innovation must be introduced as part of regulatory impact assessments when regulations are created. This is consistent with the proposed approach in Chapter 6, where the negative effect on innovation must be considered as part of the "costs" created by a regulatory alternative. Blind's conclusions can be summarized as follows:

- Strengthen the focus on innovation and regulatory policy. This means, among other things, that regulators should consider innovation as a means to achieve policy objectives, and that regulators and stakeholders should develop an innovation culture and sensitivity.

- Increase the quality of the regulatory framework regarding innovation. This means, for example, that regulatory tools should wherever possible be technology neutral and outcome-focused. Regulators should implement regulatory foresight exercises in cooperation with the science and technology community.

- Improve the implementation of regulations to foster innovation. This is linked to the effectiveness of regulatory bodies. Regulators should have staff equipped with innovation-related know-how and strategies.

- Include innovation in *ex ante* and *ex post* regulatory impact assessments. Impact assessments should systematically take into account the potential effect, good or bad, that a regulatory proposal may have on innovation. The initial impact assessment should then be tested after-the-fact with periodic reviews to measure the actual effect on innovation.

- Move innovation into the center of public policies in general and instill a general culture of innovation in regulatory bodies in particular. Blind points out here that in the field of environmental regulation, the use of regulation as a catalyst for innovation has been considered extensively. However, outside the environmental field, policy makers have not sufficiently considered the interaction between regulation and innovation.

- Integrate regulation into research on innovation systems. Blind's recommendation is to make sure that regulatory policy is an integral part of the research stream on innovation systems.

7. ADAPTIVE OR EXPERIMENTAL REGULATION

One of the keys to better regulation is to accept the fact that legislators and regulators can make mistakes. Errors can occur because regulators initially had insufficient information to make perfect decisions, because they were unduly influenced by interest groups, or because their decisions became obsolete due to technological or market developments. To address this inevitable risk of error, the EU better regulation guidelines require that EU legislation be regularly reviewed to ensure fitness for purpose. Whitt (2009) proposes the concept of "adaptive regulation". Whitt argues that for fast-moving digital environments, regulators need to move through small incremental steps, and be able to adapt their policies based on experience.

Ranchordas (2013) uses the term "experimental legislation". According to Ranchordas, experimental legislation implies introducing a new legislative solution on a small scale and reviewing the results before broadening its application. Katz (2000) and Greenstone (2009) also urge experimentation as a means to foster regulatory learning. Experimental regulation in France was made possible by an amendment to the French constitution. In spite of the amendment, the French Conseil d'Etat (2016) notes that little experimentation has been done to date.

Listokin (2008) also argues for legislative experimentation in which different regulatory solutions are tried and the best ones are retained after an experimental period. According to Ranchordas (2015) adaptive regulation is one of the keys to a regulatory policy that fosters innovation.

One way to ensure that adaptive regulation is applied in practice is to insert sunset clauses into new legislation or regulation dealing with digital environments. Sunset clauses require that the legislator or the regulator affirmatively renew the provision in order for it to remain valid. Typically the renewal is done only after an assessment of the measure's effectiveness.

The European framework for the regulation of electronic communications services (ECS) attempts to apply the principles of adaptive regulation. Under the framework for ECS, economic regulation is permitted only on certain predetermined markets which satisfy a three-criteria test. First, the market must be one where there are significant barriers to entry. Second, technological and market evolutions are not likely to change the situation. Third, competition law alone is not

sufficient to treat the problem. The European Commission periodically draws up a list of markets in the electronic communications sector that are deemed to satisfy the three criteria. If regulators want to enact a new regulation in a market that is not on the Commission's list, the regulators must make a particularly strong case for regulation, with the European Commission holding a veto power in case of disagreement. The Commission is required to review the list periodically to ensure that the relevant markets included on the list still satisfy the three-criteria test. Over a period of 10 years, the Commission reduced the number of markets on the list from 18 to 5 on the ground that market conditions had evolved and permitted the emergence of competition on some of the relevant markets. The list of markets for which *ex ante* regulation can be applied decreases over time. Regulations are thus removed as soon as competitors obtain a foothold to enter the market and/or technological or market conditions evolve.

The periodic review, and where appropriate removal, of regulatory measures is a key aspect of the ECS regulatory framework that should be replicated in any methodology for assessing regulatory measures targeting undesirable content on the internet.

Unfortunately, adaptive "evidence-based" regulation is often politically unattractive, because it conveys the message that the regulator is not sure whether the measure is in fact the best solution to the problem. Conveying uncertainty may harm the regulator's institutional power.

Moreover, legislation and regulation are costly to create, and the creators of the regulation may not want the legislation to be too easy to modify or repeal by the regulator's successors.

8. CRITICISMS OF COST-BENEFIT ANALYSES IN REGULATORY DECISIONS

Several authors (Baldwin, 2010; Radaelli and De Francesco, 2010; Hahn and Tetlock, 2008) have examined whether cost-benefit analyses of the kind described in this chapter really work in practice. Most authors agree that cost-benefit analyses are useful because they force policy makers to define the output that the regulation is intended to achieve, and to more closely analyze the options for achieving the desired output. However, cost-benefit analyses are not a panacea:

- Rigorous cost-benefit analyses are costly to produce, and may generate few benefits for their authors.

- Politicians generally know in advance what regulatory solution they want. It will be the solution that maximizes the short-term political benefits for the authors of the proposal. This solution may not coincide with the solution that maximizes welfare for society.

- Where regulators produce their own cost-benefit analysis, the analysis will necessarily be flawed by an inherent conflict of interest on the part of the study's authors. The regulator will naturally be biased in favor of a solution that maximizes the regulator's own role and resources.

- A comprehensive cost-benefit analysis requires the comparison of different solutions, some of which may fall outside the power of regulators, and some of which may be impossible to implement politically. The range of options that are politically possible may be limited. A cost-benefit analysis that compares possible solutions with impossible ones serves no purpose, even if the impossible solutions would yield a higher net benefit.

- EU regulatory impact assessments are more qualitative than United States cost-benefit analyses conducted under United States "better regulation" procedure.

- Independent peer review is essential for any cost-benefit analysis.

These points are examined in more details in the following paragraphs.

8.1 Robert Baldwin asserts that impact assessments are ill-adapted to political realities

While praising the theoretical benefits of cost-benefit analyses, Baldwin (2010) explains why regulatory impact assessments are often not well adapted to the realities of political processes. In an ideal situation, the regulatory impact assessment will take into account a wide variety of variables, including variables that are outside of the control of any one agency or regulatory authority. A regulatory impact assessment should compare different solutions to the same problem, and choose the one that is the most effective and creates the fewest costs. However, in many cases, the ideal solution may involve a combination of tax incentives, self-regulatory measures, government imposed regulation, and intelligent enforcement strategies. For the persons conducting the regulatory impact assessment, government-imposed regulation may be the only variable that they can control. Consequently, it would be futile to put on the table solutions that are outside the reach of what is politically feasible. Similarly, Baldwin points out that most legislation is a result of political negotiations and trade-offs. Out of the range of 10 possible solutions to a problem, perhaps only one or two of the solutions are politically feasible:

> *"To compare this proposal with an array of alternatives via the RIA procedure may be to compare a live horse with a number of dead non-runners."* (Baldwin, 2010, p. 271)

As a result of these difficulties, regulatory impact assessments are helpful in theory but less so in practice. According to Baldwin, many regulatory impact assessments limit themselves to relatively narrow issues, such as evaluating the costs for the administrative agency of implementing two or three different regulatory options. The idea of using a regulatory impact assessment as a tool to think "outside the box" is not feasible in practice for many government institutions because those institutions do not have a holistic vision of the problem, or keys to the full range of solutions.

Baldwin also points out that regulatory impact assessments may be viewed by lawmakers as interfering with the political process. The UK House of Lords expressed the concern

that *"considerations about the impact of legislation or regulation on personal liberties and freedoms should be regarded as part of the political process rather than as a matter for formal risk assessment procedures"*. (Baldwin, 2010, p. 270)

Another shortcoming of regulatory impact assessments is that they occur only at one time, and typically do not adequately take into account factors linked to the deployment of enforcement strategies over time. Under risk-based regulation, enforcement should be targeted on areas that will have the greatest impact. However, to develop a risk-based enforcement strategy, regulators must have access to considerable information about the market. To acquire this information, regulators may need to impose information-reporting requirements on the regulated firms. This in turn creates a significant cost for businesses that needs to be taken into account in any regulatory impact assessment. In reality, however, it is difficult for persons conducting a regulatory impact assessment to factor in various enforcement strategies by the regulatory agency and the costs associated with those respective strategies.

8.2 Radaelli and De Francesco compare U.S. and E.U. approaches

Radaelli and De Francesco (2010) examine how regulatory impact assessments are implemented in the United States and Europe. They explain that regulatory impact assessments are frequently not implemented in a serious fashion, even though most politicians say that they are in favor of such assessments. The reason is quite simple:

> *"For a politician, adopting a general provision on how regulatory proposals should be empirically assessed has low cost and high political benefits – in terms of signals sent to international organizations and the business community. To go beyond it and write guidelines, create oversight structures, and implement the guidelines across departments and agencies is politically and economically expensive. Given that the benefits of a well implemented RIA program emerge only in the medium and long-term, that is after the next elections, there is an incentive to opt for symbolic adoption."* (Radaelli and De Francesco, 2010, p. 292)

Radaelli and De Francesco also ask the question of whether regulatory impact assessments are themselves cost effective:

> *"A dollar invested in RIA cannot be invested in ex post policy evaluation – hence the opportunity cost of ex ante analysis is given by the money that is not invested in ex post evaluation or in any type of assessment taking place after regulation decisions have been made."* (id., p. 294)

8.3 Robert Hahn and Paul Tetlock evaluate the costs of regulatory impact assessments in the U.S.

Hahn and Tetlock (2008) studied the shortcomings of regulatory impact assessments in the United States:

> *"Clearly, the use of economic analysis in improving regulations has hardly been an overwhelming success. There is no evidence it has had a significant general impact, the economic analysis supporting it is frequently done poorly (if at all), and there is only anecdotal evidence to suggest that it has made a difference."* (Hahn and Tetlock, 2008, p. 78)

Hahn and Tetlock point out that the average economic analysis of a major regulation in the United States costs about $700,000. The cost of reviewing the analysis within the OIRA is about $20,000. This translates into a total costs of about $72 million annually, because there are approximately 100 regulatory impact assessments done per year. The authors believe that the process of analysis and evaluation leads many regulatory proposals to increase their net benefits by $1 billion annually. This applies, for example, to the regulations requiring removal of lead from gasoline and the market-based approach for cutting sulfur dioxide emissions. Hahn and Tetlock suggest that economic analysis of proposed regulations be subject to peer review. They also suggest using prediction markets as a proxy to estimate the overall impact that a regulation will have. A prediction market means that the government would issue a contract that would pay an amount proportional to net benefits if the particular legislative measure were implemented, and a second contract that paid an amount proportional to net benefits if the measure were not implemented. The difference between the prices of the two contracts could capture the overall impact of the regulation as measured by the change in net benefits from the regulation. The authors suggest that the legislative branch should also have a body devoted to regulatory analysis in order to create healthy competition between agencies.

8.4 Ackerman and Heinzerling criticize CBAs that attempt to "price the priceless"

Ackerman and Heinzerling (2002) challenged the very concept of trying to put a price on social benefits and harms for which no market exists. Ackerman and Heinzerling focus on environmental and health and safety cost-benefit analyses and point out the absurdity of certain valuations. For example, studies in the field of environmental protection conclude that the average American household is willing to pay $257 to prevent the extinction of bald eagles, $280 to protect humped-back whales and $80 to protect grey wolves. The loss of one IQ point due to lead poisoning is valued at $9,000 according to one study, £1,100 according to another. Saving a life is "worth" $6.3 million. Ackerman and Heinzerling's main point is that economists' efforts to determine the willingness to pay for certain social benefits are measuring the wrong thing. This is because people's preferences as citizens and voters may be different from their choices as buyers and

sellers of goods and services. To illustrate this point, Ackerman and Heinzerling give the example of a student who as a citizen votes in favor of a measure that would prohibit any commercial development in a given wilderness area. At the same time, that same student will willingly purchase a ski-pass in order to ski at a development built in the relevant wilderness area. According to Ackerman and Heinzerling, there is nothing contradictory about the student's two choices. When the student expresses his choice to purchase a ski-pass, he or she is maximizing his or her individual wellbeing without taking into account the effects of collective actions. When voting on a measure to preserve the wilderness area (which would destroy the student's ability to ski in the area), the student takes into account the voting behavior of others and the possibility that his or her individual choice, in combination with others, could make a lasting social change. Ackerman and Heinzerling use this example to show that contrived methods used to determine willingness to pay for broad social values are likely to be misleading.

Ackerman and Heinzerling also challenge the use of discount rates to discount harms that occur in the future. Using a discount rate reflects the view that most human beings, as individuals, prefer being harmed sometime in the future as opposed to being harmed now. By using a discount rate, a catastrophic harm occurring in 100 years would have almost no value today. Ackerman and Heinzerling point out, however, that this use of a discount rate is again based on the false assumption that social choices should be based on the same willingness to pay approach as those used when an individual makes a choice about buying a computer, or lighting up a cigarette. When an individual makes a choice to maximize his or her own wellbeing, he or she will attach very little value to what happens in 100 years. By contrast, as a citizen and a voter, the same individual may, when taking into account the effects of collective political action, decide to vote for matters that preserve future generations against catastrophic loss. He or she may make these voting decisions even if they result in an individual cost for him or her.

In summary:

> *"Cost-benefit analysis turns public citizens into selfish consumers and interconnected communities into atomized individuals. In this way, it distorts the question it sets out the answer – how much do we, as a society, value health and the environment?"* (Ackerman and Heinzerling, 2002, p. 1567)

Ackerman and Heinzerling's criticism on valuing environmental harms would also apply to fundamental rights, which explains why many individuals would vote in favor of privacy-enhancing regulations, while at the same time engaging in privacy-harming behavior on the internet. Even if Ackerman and Heinzerling's criticism is valid, it is not a reason to abandon cost-benefit analyses that involve fundamental rights. The criticism means that valuing fundamental rights must be approached with care and used as a tool to compare alternative approaches, and not as a stand-alone decision rule.

8.5 Greenstone: cost-benefit analyses require experimentation

Greenstone (2009) argues that reliable cost-benefit analyses require experimentation, which is rarely done for regulatory proposals. Without conducting a randomized trial, it is impossible to reliably build a counterfactual and compare the costs and benefits with various regulatory alternatives. Without a randomized study, the costs and benefits associated with the counterfactual scenario, and with the regulatory proposals, are little more than guesses. While experimentation is not always possible before regulations are adopted, Greenstone argues that systematic *ex post* evaluation of regulatory performance should be mandatory, and conducted under the supervision of an independent regulatory board. This echoes the French Conseil d'Etat's recent recommendations (Conseil d'Etat, 2016).

9. WHY CONDUCT A COST-BENEFIT ANALYSIS?

Conducting regulatory impact assessments, including cost-benefit analyses, has become a key element of "good regulation" approaches in the United States and Europe, and forms the basis for OECD guidelines. The United States has had the longest experience in applying cost-benefit analyses to proposed federal regulations. The United States' system includes a robust peer review process through the OIRA.

Experience in the EU is more recent, although the European Commission's May 2015 toolbox and the 2013 Renda study show that EU practices in cost-benefit analyses should converge in theory with those of the United States. A number of authors express scepticism regarding the practical utility of cost-benefit analyses because they seem out of sync with political realities. Their utility may be greater for technical regulations, where political debate is less intense.

In the field of internet regulation, there exists almost no track record for regulatory impact assessments. In the United States, regulatory impact assessments apply only to measures proposed by agencies of the executive branch of the government. Measures proposed by independent regulatory authorities, such as the FCC's open internet order, escape federal "better regulation" scrutiny. In Europe, regulatory impact assessments generally limit their analysis to enforcement costs for the administration and direct compliance costs for businesses. The assessments do not attempt to quantify effects on innovation or fundamental rights.

internet regulation involves hard-to-measure parameters such as the regulation's impact on innovation and fundamental rights. This might lead some to conclude that detailed cost-benefit analyses are useless in the context of regulatory measures designed to limit access to harmful content on the internet. The exercise is time-consuming and costly, and the outcome contestable.

Nevertheless, the same criticisms were made for regulations designed to preserve wildlife, or increase the quality of air. Early proponents of "better regulation" in the United States were quick to point out that the purpose of cost-benefit analyses is not to put a monetary value on clean air or on a human life, but to help make rational choices between alternatives when government

resources are limited. If a regulator must choose between two measures having equivalent cost, one parameter of the regulator's decision would be to know which of the two measures has the highest positive effect on the regulator's desired outcome.

Another response to critics is that the process of conducting cost-benefit analyses brings significant benefits, by requiring regulators to:

- define precisely the outcome that the regulator seeks to achieve, including a realistic definition of what "success" looks like;
- conduct a careful analysis of the baseline scenario of doing nothing;
- prepare a list of adverse effects associated with different regulatory alternatives, comparing the relative impacts of each alternative;
- respond to a rigorous peer review process.

The process helps regulators avoid mistakes, by slowing down the process and requiring consideration of several alternatives (Sunstein, 2014). Posner (2000) emphasizes that cost-benefit analyses have limitations, and therefore should be used as input to decisions, rather than as strict decision rules. Posner nevertheless defends cost-benefit analyses as improving the quality of regulatory decisions by helping to reveal anomalies and making choices more explicit.

CHAPTER 6 – CREATING A METHODOLOGY FOR ASSESSING REGULATORY OPTIONS

1. BRINGING IT ALL TOGETHER

I will attempt now to bring together the lessons learned from each of the previous chapters in order to propose a methodology for assessing regulatory options to advance content policies on the internet. As discussed in Chapter 2, the range of content policies is diverse: They may target child pornography, racism, anti-Semitism, promotion of terrorism, copyright infringement, illegal gambling, the right to be forgotten or even the promotion of national culture or language. The range of internet intermediaries, and the possible actions they can take, is also varied. Internet access providers, search engines, payment providers, advertising intermediaries, and social media platforms could potentially be called on to help implement a content policy, and the range of actions they could take is potentially vast

Chapter 3 explored impacts on fundamental rights. The proportionality test requires a listing of all the fundamental rights potentially affected by each regulatory measure, and an attempt to identify the relative impact of each of the regulatory options on each of those rights. Proportionality then involves evaluating the relative benefit of the proposed measures in terms of promoting certain fundamental rights such as privacy or the right to property, and then choosing the regulatory alternative that gets the job done while causing the least adverse impact on other fundamental rights. In most cases, 100% enforcement of a content policy on the internet will not be possible or even desirable, because the cost of approaching 100% enforcement would be disproportionally high in terms of harming other fundamental rights.

Chapter 4 presented the range of possible institutional and legal frameworks. They include self-regulation, co-regulation, liability and property rules, and full-fledged administrative regulation with a dedicated regulatory authority set up to oversee enforcement. The choice of institutional framework will affect how flexible the regulatory regime is, and how susceptible the regime is to industry capture or regulatory creep.

Chapter 5 examined the principles of better regulation in the United States and Europe. I identified aspects of better regulation that are particularly important for the internet, focusing on the 2011 OECD recommendations for internet policy making. Chapter 5 also presented some of the limitations of cost-benefit analysis, and in particular their incompatibility with the realities of the political process.

In this chapter, I will try to weave these strands into a single methodology that can be used by policy makers to help evaluate regulatory options and fulfill their duties under better regulation principles.

(a) A regulatory impact assessment that incorporate a cost-benefit analysis

When using the term "regulatory impact assessment", I mean the entire methodology proposed in this chapter, which includes several steps, including a questionnaire, a cost-benefit analysis, a public consultation and peer review. The cost-benefit analysis is therefore one part of the overall regulatory impact assessment. The two terms, "regulatory impact assessment" and "cost-benefit analysis", are not synonymous.

(b) Who would use the regulatory impact assessment?

The regulatory impact assessment would be applied in two possible institutional contexts. In the first, a national government would conduct the assessment before submitting a legislative proposal to parliament. This is currently how impact assessments are conducted in France. The impact assessment is prepared by the government before legislative proposals are presented to parliament. But the impact assessments currently conducted by the French government fall short of the analysis called for in this thesis. Among other things, the impact assessments do not attempt to measure indirect costs.

The second institutional context would involve a regulatory authority, who would conduct the impact assessment before adopting a regulatory solution for limiting access to harmful content. This is currently what happens when regulatory authorities in Europe propose measures affecting the electronic communications market. Regulatory authorities must conduct a market analysis and justify the proposed measure based on a methodology imposed by the European Commission.

Regardless of whether the regulatory impact assessment is conducted by the government or by a regulatory authority, the impact assessment would have to be reviewed by an independent institution in order to ensure that the impact assessment is conducted rigorously. This is the peer review procedure I describe in Section 6 below.

(b) Why would the regulatory impact assessment increase regulatory quality?

As explained in Chapter 1, the regulatory impact assessment will force the sponsors of regulation to define better the objective they hope to achieve and ways to measure success. The impact assessment will require a better analysis of alternative scenarios, including the alternative of doing nothing. The cost-benefit analysis will require consideration of indirect costs, which are generally ignored today. The process will also foster regulatory improvement by allowing comparisons and learning between different countries and regulatory approaches. Finally, the regulatory impact assessment will permit a clear demarcation between regulatory measures adopted by democratic countries that uphold free expression and net neutrality, and similar measures adopted by less democratic countries.

2. ELEMENTS OF THE METHODOLOGY

To analyse proposed measures limiting access to content on the internet, I propose a five step methodology:

Step 1: A questionnaire requiring policymakers to identify the relevant variables in the policy equation, *ie*:

- the underlying content policy that needs to be enforced, its relative importance compared to other content policies and fundamental rights, and how "success" in applying the content policy can be measured;
- the range of internet intermediaries and actions that could help enforce the content policy, ranging from the least intrusive to the most intrusive;
- international practices, if any, used to address the problem;
- the institutional alternatives that can be considered, including liability and property laws, self-regulation, co-regulation, and/or administrative regulation;
- the fundamental rights affected by each proposed measure, and how each proposed measure ranks in a proportionality test;
- other indirect costs such as harm to the internet ecosystem.

Step 2: After completing the questionnaire, policy makers should apply a cost-benefit analysis to the proposals, comparing the alternatives to a baseline scenario. The cost-benefit analysis requires policymakers to:

- build the baseline scenario (or "counterfactual") consisting of no regulatory intervention, taking into account dynamic factors such as possible evolutions of internet technology and markets, anticipated enforcement of existing laws and self-regulatory policies;
- evaluate the level of benefits flowing from each regulatory proposal, compared to the baseline;
- evaluate the level of direct costs resulting from each proposal compared to the baseline, including direct costs for internet intermediaries, their customers, and taxpayers;
- evaluate the level of indirect costs resulting from each proposal compared to the baseline, including impacts on fundamental rights, on the internet ecosystem and innovation;

- select the one or two proposals that are likely to yield the highest net benefits;
- confront the proposals with the list of constraints, and eliminate any alternatives that do not satisfy the constraints. The constraints would permit certain ethical considerations to be included in the cost-benefit analysis.

Step 3: Conduct a public consultation based on the initial questionnaires and cost-benefit analysis.

Step 4: Submit the questionnaire and cost-benefit analysis to institutional peer review, permitting an independent authority to verify that the proposed measure delivers the highest net benefit and takes into account the constraints.

Step 5: Organize a periodic *ex post* review mechanism to ensure that regulatory measures are modified or removed as soon as they are no longer necessary.

Each of these five steps is presented below.

3. THE QUESTIONNAIRE

The first step in the impact assessment is a qualitative questionnaire. The questionnaire will force policy makers to identify precisely the objective they hope to achieve, and to list all the alternative mechanisms – technical and institutional -- available to achieve the objective. The questionnaire will also force policy makers to identify, from a qualitative standpoint, costs associated with each measure, and provide a first guess at their magnitude. The questionnaire will also require policy makers to identify international best practices.

The questionnaire is designed to put all the variables on the table, before narrowing down the choice of alternatives and applying a full cost-benefit analysis to those alternatives.

The questionnaire would look something like this:

3.1 Analysis of the underlying content policy that needs to be enforced

QUESTION: Please describe the kind of content that is targeted by the proposed measure:

Content category	*Describe the specific content targeted by the proposed policy*
Malware or other threats to the network or to user data	
Spam, phishing	
Cookies, tracking software	
"Right to be forgotten" content	

Content category	*Describe the specific content targeted by the proposed policy*
Online gambling	
Cigarettes, alcohol	
Illegal drugs, counterfeit drugs	
Other counterfeit articles	
Copyright infringement	
Defamation, protection of privacy	
Racial, religious hatred	
Protection of culture, language and cinema	
Advertising laws	
Protecting minors against violent or pornographic content	
Child pornography	
Terrorism	
Other (please describe)	

Qualifying the intensity of the harm.

QUESTIONS: Describe the provisions (if any) of the criminal code that apply to this content, including applicable sanctions, if any. Is the content illegal in all circumstances, or only when accessed by certain classes of persons (e.g. minors), or using certain search terms (e.g. the right to be forgotten)?

Does the content in question create a risk of physical harm for citizens (*eg*. sexual exploitation of children, slavery, and terrorism)? If so, please describe the kind of harm, and its extent (*e.g.* number of cases per year). Where access to the content does not create a risk of physical harm, describe the nature of the harm: harm to a fundamental right, to mental development of minors, to culture? Please describe the extent of the harm: how many persons affected and the range of intensity of the harm for each individual.

The prevention of these harms, as compared to the baseline scenario, will constitute the benefits flowing from each alternative proposal.

How to measure the benefits of the content policy.

QUESTIONS: How would the benefits associated with the content policy be measured? If the content policy is successfully applied, how would "success" be measured? Are there proxies that can be used to measure success?

Developing measurement tools to evaluate success of a content policy is one of the most challenging aspects of the impact assessment. I examine this problem in Section 4.3 below.

International acceptance of the content policy.

QUESTIONS: Is the content in question illegal or restricted everywhere in the European Union? In most countries in the world? Are there international treaties dealing with this form of harmful content?

3.2 The range of internet intermediaries and actions they could take to help enforce the content policy, ranging from the least intrusive to the most intrusive

QUESTIONS: List the internet intermediaries that could assist in enforcing the relevant content policy, and the action they could take. In the third column, rate the level of intrusiveness of the relevant measure, *ie*. how much would the measure interfere with fundamental rights or the proper functioning of the internet.

Category of internet intermediaries	*Describe internet intermediary (ies) that are potential candidates to enforce the content policy, and the potential actions they could take.*	*Level of intrusiveness of the measure (low, medium or high)*
Search engines		
Hosting providers		
Social media platforms		
Internet access providers		
Domain name registrars		
Payment service providers		
Advertising service providers		

Category of internet intermediaries	*Describe internet intermediary (ies) that are potential candidates to enforce the content policy, and the potential actions they could take.*	*Level of intrusiveness of the measure (low, medium or high)*
Application stores		
Content delivery networks		
Internet backbone providers		
End-user applications, browsers, antivirus software, parental control software		
Set-top box or modems		
Device operating systems		
Other (please describe)		

QUESTIONS ON TECHNICAL OPTIONS:

Least intrusive measures: Among the internet intermediaries on your list, which ones could apply the most "light touch" measures, *ie*. the measures that would have little or no impact on the functioning of the internet or on fundamental rights. An example of a "light touch" measure is one that educates internet users on how to protect themselves against the relevant content, by adjusting browser settings, for example.

Most intrusive measures: Among your list of internet intermediaries and the potential actions they could take, which actions are the most intrusive, i.e. those that would have the greatest effect on the normal functioning of the internet and/or on fundamental rights? Examples of intrusive measures include blocking internet content based on deep packet inspection technology and/or requiring that all internet traffic flow through a central gateway that can detect illegal content. Another example of intrusive measures would be those that have extraterritorial effects.

Intermediate measures: List actions that could be taken by the internet intermediaries on your list that are in a middle range, i.e. neither the most intrusive nor the least intrusive.

Territorial enforcement: Among the internet intermediaries on your list, which ones are subject to the jurisdiction of courts and regulatory authorities in your country? If some of the intermediaries potentially considered for regulation are subject to the jurisdiction of your country and other intermediaries of the same category are not, how effective would the proposed measure be? Would the proposed measure create a competitive distortion between intermediaries within your jurisdiction who apply the measure, and intermediaries outside your jurisdiction who do not?

3.3 Remedies used in other countries

QUESTIONS: How do other countries deal with this kind of content? What are the advantages and disadvantages of the approaches used in other countries? Are there any international instruments (treaties, recommendations, charters) addressing remedies for this content issue?

Would any of the measures envisaged have extraterritorial effects? If so, are the measures consistent with the laws of the foreign countries affected? What is the likely response of other countries if the proposed measure has effects in those countries? Katz (2000) refers to these issues as "jurisdictional externalities."

How easy is it for the relevant internet intermediaries to limit the effect of the measure to your country?

Are the proposed approaches consistent with the OECD Recommendations on internet Policy Making, and if not, which aspects diverge from the OECD Recommendations?

3.4 The institutional alternatives, including liability and property rules, self-regulation, co-regulation, and/or full-fledged administrative regulation

QUESTIONS ON INSTITUTIONAL ALTERNATIVES:

Criminal law enforcement: How do prosecutors and police currently deal with the problem? What is the current volume of criminal prosecutions and convictions relating to this content policy? How effective is cross-border police cooperation in this field? Will the development of more effective cross-border police cooperation make a difference?

Administrative regulation: Are there any regulatory agencies or independent regulatory authorities that currently investigate and enforce the relevant content policy? What measures do these regulatory authorities currently take to enforce the content policy?

Liability and property laws: What role do liability and property laws, and their enforcement before civil courts play, if any? What existing laws, civil and criminal, are used to address the problem? Are there ways in which the enforcement of existing legal provisions can be improved (OECD, 2009)?

Unilateral self-regulation: Do internet intermediaries attempt to regulate this problem through their own terms of use and internal procedures? Do the relevant internet intermediaries apply a notice and takedown procedure, and if so how effective is it? What problems, if any, have been reported in connection with these internal procedures? How might they be improved?

Multilateral self-regulation: Are there any existing codes of conduct or other forms of multilateral self-regulation that address the problem? How effective are those measures?

Administrative regulation: If a regulatory authority were to become involved in enforcing the relevant content policy, what exactly would the regulatory authority do? How would the role of a regulatory authority differ from that of a judge?

Taxes: Is the matter one that could be treated through public subsidies and/or tax incentives (*eg.* subsidies to promote culture)?

Territorial level of regulation: What is the best territorial level of regulation: individual country? European Union? International agreement? OECD recommendation?

3.5 The fundamental rights affected by each proposed measure

QUESTIONS ON FUNDAMENTAL RIGHTS:

Describe the impact, positive or negative, that potential actions by internet intermediaries could have on fundamental rights, including the following:

Category of fundamental right	*Describe persons affected, nature of the effect, and extent (number of persons affected)*
Freedom of expression, including freedom to access information	
Protection of personal data and privacy	
Protection of property, including intellectual property	
Freedom to conduct a business	
Protection of security and/or health	
Right to a fair trial, presumption of innocence	
Other	

3.6 Internet ecosystem

QUESTIONS ON THE INTERNET ECOSYSTEM:

List the other potential harms generated by each proposal, such as negative impacts on:

- Net neutrality and the end-to-end architecture of the internet;
- Innovation;
- Competition.

For each harm caused by a measure, describe its intensity (low, medium, high, extremely high).

For each measure, describe whether it respects the principle of technology neutrality, and if not, describe the technological approach that is taken, and the potential risks associated with the absence of neutrality (eg. technological obsolescence or harm to innovation).

3.7 Behavorial economics and "nudges"

QUESTIONS ON BEHAVIORAL ASPECTS:

List changes in default settings or user interfaces that might help achieve the desired policy objective.

List possible actions that could be taken to change user behavior without recourse to internet intermediaries, *e.g.* advertising campaigns, educational programs.

Describe possible changes in user behavior that may result from regulatory action and that would be counter-productive, *e.g.* increased use of VPNs and encryption, use of intermediaries outside the country's jurisdiction.

Can taxation be used to influence behavior?

3.8 Adaptive and experimental regulation

QUESTIONS ON ADAPTIVE REGULATION:

For each proposal, the questionnaire should ask whether the effectiveness of the approach has been tested through experimentation. If no experimentation has been conducted, the sponsor of the proposal should explain how effectiveness can be measured through *ex post* reviews, and whether the approach can be modified or removed as a function of its observed effectiveness. The questionnaire should ask whether the suggested approach is "highly flexible", "flexible", or "inflexible."

4. A COST-BENEFIT ANALYSIS UNDER CONSTRAINT

The questionnaire will permit policy makers to eliminate a number of alternatives, either because they are too intrusive, or because the relevant intermediaries are beyond the territorial reach of the regulation. Ideally, the questionnaire will help policy makers narrow down the options to a manageable number. The questionnaire will also help identify the variables that need to be captured in the cost-benefit analysis.

The next step is the cost-benefit analysis itself. The analysis will require:

- preparation of a baseline scenario or counterfactual;
- an estimate of the net benefits (benefits less costs) generated by each regulatory alternative;
- the application of constraints, which may lead to the elimination of certain proposals.

4.1 How to deal with hard-to-quantify benefits and costs?

As we saw in Chapter 5, transforming certain benefits and costs into measurable units is challenging. Impact assessments dealing with environmental protection or safety measures must deal with this problem on the benefits side. For example, measures designed to protect the environment must deal with questions such as how to measure the social value of a pristine meadow, or a certain kind of wildflower. Health measures must deal with the question of how to measure the value of a human life. As we saw in Chapter 5, Ackerman and Heinzerling (2002) challenge the very idea of "pricing the priceless". Nevertheless, most cost-benefit analyses involving environmental, health or safety regulations at least attempt to attribute values to the benefits flowing from the regulation. (I emphasize again that the measurement of these values is not intended to suggest that they can be bought and sold, but rather to help choose among alternatives when government resources are limited.)

Measures designed to limit access to harmful content are even more complicated than these environmental and health examples. Blocking content on the internet is generally aimed at protecting values, such as human dignity, that are hard to quantify. In this respect the exercise is just like an environmental or health regulation. Instead of protecting wildflowers or human life, the policy protects privacy or the right to dignity. However, unlike most environmental or health measures, measures to block internet content will create costs that are equally hard to quantify: limitation to freedom to access information, limitation to privacy rights, harms to the internet ecosystem. Thus we have a problem where hard-to-quantify elements exist both on the benefits and cost sides.

Before examining the various steps in the cost-benefit analysis, this section describes ways to quantify, and if possible transform into monetary units, these benefits and costs.

(a) Contingent valuation or stated preferences.

One technique for valuing hard-to-measure elements is called contingent valuation (also referred to as the "stated preferences" method) (Viscusi et al., 2005). Under the contingent valuation approach, researchers develop survey questions that attempt to determine individuals' willingness to pay for certain hard-to-quantify benefits, such as reducing the risk of an oil spill that would spoil the Alaska coastline. The survey questions must be drafted so as to present individuals with concrete choices in hopes of eliciting responses that objectively measure how much individuals would be willing to pay -- for example in additional annual taxes -- in order to reduce the risk of an oil spill similar to the Exxon Valdez catastrophe. This approach is the same as the "stated preferences" approach described in Chapter 5 in connection with the United States Government Circular A4.

(b) Cost effectiveness analysis.

The second technique consists of not trying to convert the benefit into dollar or euro amounts at all, but into some other unit of measurement. For example, a regulation designed to increase the safety of swimming pools might be measured by the number of infant deaths avoided. A regulation designed to protect the environment might be measured by number of hectares of wetlands preserved from development. The unit of measurement (infant deaths avoided, hectares of wetlands) would then be used to compare different regulatory options in order to compare the cost-effectiveness of each option. For example, if one regulatory measure permits an increase in swimming pool safety at a cost of 1,000 euros per avoided infant death, and another proposal increases safety at a cost of 1,000,000 euros per avoided infant death, the first lower-cost proposal would be implemented in priority, all other things being equal. Viscusi (2005) calls this a cost-effectiveness sensitivity analysis. Circular A4 calls this a "CEA", a cost effectiveness analysis.

As we will see below, this technique for measuring benefits can be used for content policies. The persons preparing the impact assessment would have to define units by which to measure the success of different regulatory proposals. For example, a policy designed to protect the so-called "right to be forgotten" might be evaluated based on the time it takes an average person to see the information that is supposed to be hidden on the search engine. A policy designed to fight online copyright infringement might be evaluated based on the number of persons who subscribe to legal streaming services. One or more proxies are used to measure the benefit flowing from a given content policy, and these proxies are not converted into money.

(c) Benefit transfer.

A third approach is to try to convert the benefits or harms into monetary units by comparing them to other benefits or harms for which monetary valuations are available. This is the "benefit transfer" method described in United States Government Circular A4 (*see*, Chapter 5, §4.6). In the field of fundamental rights, this might be done by comparing the harm to fundamental rights to the statistical value of a human life. Economists have developed monetary values associated with saving a human life, or extending a human life by a given number of years. Restricting a fundamental right such as freedom of expression or privacy diminishes the quality of human life, but in an amount that is presumably less than losing life entirely. Starting from this assumption, it may be possible to develop approaches that attribute values to different levels of intrusions into fundamental rights. For example, a severe restriction of freedom of expression might be deemed the equivalent, in monetary terms, to the loss of one, or two, or ten, years of life. The right not to be tortured may have a value equivalent to, or even greater than, the statistical value of a human life. Saving a child from sexual abuse may also have a value equal to, or greater than, the statistical value of a human life. Preserving an individual's privacy against government intrusion would have a value less than the statistical value of a human life, although how much less would depend on the level of the intrusion. As an extreme example, if individuals lived in an Orwellian world where they had no fundamental rights at all, some might say that the quality of life has been impaired in an amount that approaches the statistical value of a human life. In other words, a total deprivation of the fundamental human rights might be the equivalent of death. Based on that assumption, it may be possible to work backwards and develop values for different incremental intrusions of fundamental rights. By doing this, it might be possible to convert harms to fundamental rights into dollar or euro figures. I mention this as a possible field of future research in Chapter 7.

Many would cringe at attributing a monetary value to a fundamental right, arguing that rights cannot be reduced to money. However, the same objections would apply to human life. Yet regulatory impact assessments, at least in the United States, have nevertheless developed a statistical value for a year of human life saved. The sole utility of the valuation is to compare the efficiency of different regulatory alternatives.

(d) Hedonic pricing.

A fourth method used in environmental impact assessments is hedonic pricing. Under this approach, one takes prices of a good for which there exists a market, eg. the price of a house, and compares the prices in low-pollution areas and high-pollution areas. The difference in price represents, at least in part, the value of living in a pollution-free

environment. Similarly, in health and safety regulation, the higher salary given to persons who do dangerous jobs may reflect the market value of the increased risk to health.

I have not found a way to apply hedonic pricing to benefits and costs relating to blocking internet content. But there may exist approaches I have not thought of.

(e) Qualitative scoring.

The fifth method is to develop a qualitative scoring system. In the field of fundamental rights, Robert Alexy has proposed a scoring system that permits different outcomes to be compared. For example, a measure that yields a fundamental rights score of +4 would be better than a measure that yields a fundamental rights score of -2. Scoring can work when comparing elements with similar unitary values. But when comparing elements whose unitary values differ, scoring can run into an "apples and oranges" comparison problem. For example, courts generally agree that privacy and freedom of expression have equal normative value. A "unit" of freedom of expression is roughly equal to a "unit" of privacy. In that case, it would be theoretically possible to balance units of freedom of expression against units of privacy. A regulatory measure that promotes privacy by +4 but harms freedom of expression by -1 compared to the baseline scenario would yield a net fundamental rights improvement of +3.

This kind of trade-off is possible, but has limits. First, a fundamental right can never be reduced to zero, even if there is a strong countervailing benefit for another fundamental right. The essence of the right must always be preserved. This is why Alexy's formula incorporates an exponential progression, so that "severe" restrictions of a fundamental right have an exponentially higher value than "medium" or "high" restrictions. This is also why I propose a step in the cost-benefit analysis that eliminates any proposal that causes a "severe" or "extremely high" negative impact on a fundamental right (*see*, §4.7 of this chapter).

Second, fundamental rights cannot generally be traded against other values on a one-to-one basis. One unit of harm to privacy would not have the same value as one unit of harm to innovation. Except for freedom of expression and privacy, where there is a rough correspondence in unit values, fundamental rights cannot be traded off against each other on a one-to-one basis.

(f) Qualitative labels.

A last approach consists of attributing qualitative labels for values that are hard to quantify, without trying to add them up through a scoring system. For example, some of the costs associated with a regulatory proposal may be characterized by qualitative labels such as "severe intrusion", "medium intrusion", "light intrusion," "no intrusion." This

technique may permit certain proposals to be eliminated without having to convert the relevant costs into fungible units. For example, in the three proposals below, proposals A and C can be eliminated based solely on a comparison of the qualitative labels:

	Proposal A	Proposal B	Proposal C
Quantifiable benefits	+200	+250	+250
Quantifiable costs:	-100	-100	-100
Net quantifiable benefits:	+100	+150	+150
Non-quantifiable costs:			
Harm to privacy	Light intrusion	Light intrusion	Severe intrusion
Harm to freedom of expression	No intrusion	No intrusion	No intrusion
Harm to innovation	Light intrusion	Light intrusion	Light intrusion

In this example, proposal B emerges as the preferred outcome. Proposals A and C necessarily present lower net benefits than proposal B. It is not necessary to add up the non-quantifiable costs to privacy, freedom of expression and innovate to reach this conclusion.

(g) Conclusion

In summary, the six methods for measuring hard-to-quantify benefits or costs are:

- Contingent valuation or stated preferences (*ie.* using questionnaires);
- Using non-monetary units to measure the level of the benefit or cost (*eg.* number of lives saved);
- Benefit transfer method (*eg*. finding a correlation between fundamental rights and the statistical value of a human life);
- Hedonic pricing (finding differences in the pricing in some good that reflect the different elements we're trying to measure);

- Fundamental rights scoring (used by Robert Alexy to compare measures impacting fundamental rights);

- Qualitative labels (*ie.* using labels like "extremely high" to denote the level of cost).

4.2 **Prepare a baseline scenario of no regulatory intervention, taking into account dynamic aspects such as possible evolutions of internet technology and markets, and application of existing laws and self-regulatory policies**

We can now turn to the steps involved in the cost-benefit analysis. The first step is to create a baseline scenario, or counterfactual. As noted in Chapter 5, preparation of a baseline scenario is one of the most important elements of a regulatory impact assessment, and also one of the most widely misunderstood. The baseline scenario is not the *status quo*, but an attempt to project how the *status quo* will evolve in the absence of regulatory intervention.

Anticipate technological and market changes. The baseline scenario must try to anticipate technological or market developments that may intervene in the following years, as well as increased use of existing laws and self-regulatory initiatives. For example, a baseline scenario involving a proposed regulatory framework to deal with online copyright infringement should take account of:

- future use of civil lawsuits, including notice and takedown, and requests for injunctive relief against internet intermediaries;
- future market changes in how music and films are consumed online;
- cross-border criminal actions;
- any existing self-regulatory regimes and their likely development over time.

In the fast-moving internet ecosystem, market or technological developments can make regulation obsolete. It is important that the baseline scenario attempt to characterize these developments and their dynamic effect on the problem. The baseline scenario should attempt to anticipate whether the identified problem is likely to get better or worse over time based on different assumptions, such as increased resources devoted to law enforcement, or increased adherence to voluntary codes of conduct. A sensitivity analysis should be done to measure the effect of changes of assumptions on the outcome.

Defining "success". If possible, the baseline scenario should identify the level of intensity of the problem at different time periods, 12, 24 and 36 months, should be quantified. Measuring the intensity of the problem will depend on the nature of the problem and the definition of "success" in achieving the relevant content policy.

Defining how success is measured is one of the most challenging aspects of the exercise. I discuss in Section 4.3 below ways of breaking down benefits into different categories, analysing each category of benefits in terms of their importance to society, and measuring how the level of benefits varies over time. It may be necessary to measure benefits through proxies. For example, success in fighting online copyright infringement might be measured through various proxies, such as:

- an increase in the number of prosecutions or fines for copyright infringement;
- an increase in revenues for legal online music and film distribution platforms;
- a decrease in detected illegal downloads;
- an increase in box office or live concert sales.

Success in fighting online child pornography might be measured through:

- an increase in the number of arrests and confiscations of images;
- a decrease in the number of visits by internet users to prohibited sites (if that can be measured);
- the amount of time and effort required for an average person to obtain access to a prohibited site (if that can be measured);
- the ease with which one can locate a child pornography site using various search engines.

Success in promoting French film production might be measured through:

- an increase in the number of French films produced annually;
- an increase in aggregate production budgets;
- an increase in the number of French films viewed on digital distribution platforms;
- an increase in the number of French films viewed in cinemas;
- an increase in the number of French films receiving international awards.

Whatever the content policy is, a crucial step is to define a way to measure its achievement. And the first place this comes into play in the cost-benefit analysis is in the baseline scenario, *ie.* what is likely to happen in the absence of regulatory intervention? The exercise will reveal the sometimes tenuous link between the objective being pursued and the corrective measure being proposed.

The problem of measuring success also raises the important question of whether a regulatory action creating costs that we know exist, such as an impact on fundamental rights and direct costs on internet intermediaries, should be implemented when there is no way to know for sure if the measure is effective in achieving the relevant content policy.

To provide an example, France is considering measures that would obligate certain internet intermediaries to provide a preference for French content in recommendation algorithms. The objective is to promote French culture, language and content production. But how exactly would the impact on French culture, language and content production be measured to determine whether the regulatory measure is effective in achieving the desired objective? The baseline scenario will require the drafters of the cost-benefit analysis to attempt to project what the relevant success parameter would look like in the absence of regulatory intervention. This baseline result would then be compared with the result flowing from various regulatory alternatives. Would a policy be considered successful if every recommendation contains at least one French-produced picture? Does it matter in this context if users actually click on the recommendation that is proposed? Does it matter what the search terms were?

4.3 Measuring benefits compared to the baseline scenario

After building the baseline scenario, the drafters of the cost-benefit analysis must examine each of the regulatory alternatives and attempt to measure the benefits that those alternatives generate compared to the baseline.

(a) Choice of non-monetary units to measure benefits.

If the drafters of the cost-benefit analysis choose to measure benefits using an alternative non-monetary unit such as number of lives saved, or number of French films produced (the second approach mentioned in Section 4.1 above), the same metrics should be used when measuring the likely achievement of the content policy in the various alternative scenarios. The nature of the success metrics will naturally affect the intensity of the total benefits flowing from the measure. A success metric based on projected increases in revenues for online music platforms would have a different absolute value in terms of benefits for society than a success metric based on number of lives saved from decreased sales of counterfeit drugs. Recognizing the difference in the absolute value of the success metrics is important to be able to compare the overall benefits to the overall costs, particularly in situations where benefits will require trade-offs against fundamental rights. To illustrate the point, 1000 saved lives will justify a higher level of costs, including interferences with fundamental rights, than 1000 saved record sales. This is why using monetary units to measure benefits is always better, whenever possible.

(b) Breaking benefits into different categories.

Certain content policies will yield multiple related benefits. To measure benefits, the drafters of the cost-benefit analysis should unpack the different categories of benefits and measure them separately. For example, for measures to block access to images of child pornography, the set of benefits may include:

(i) a reduction in the number of children subject to sexual abuse,

(ii) a reduction in the number of children or young adults who are psychologically harmed by being exposed to child-abuse images on the internet,

(iii) increased used of the internet flowing from the fact that the internet is a safer place, and

(iv) the symbolic value of showing that society does not tolerate serious violations of human rights on the internet.

In this example, there are four separate benefits with different qualitative characteristics. Some of the benefits may correspond to saved lives, some of the benefits may correspond to increased usage of internet, and some of the benefits may relate to the affirmation of important societal values.

The drafters of the cost-benefit analysis should determine which of the categories of benefits are quantifiable, and which are not. Saving a child's life may have a quantifiable benefit, if the number of saved children can be estimated. The saved lives may also be translated into monetary values, using the statistical values of human lives published in connection with United States health and safety regulations.

Affirming the symbolic value of not tolerating human rights violations on the internet may be impossible to quantify in monetary terms, whereas the benefit flowing from increased usage of the internet might be quantifiable, albeit hard to measure in practice.

The purpose of this exercise is to highlight the likely impact of the regulatory measure on each category of benefit. For a measure designed to block access to child pornography, the different categories of benefits might look like this:

Category of benefit	Quantifiable? Value of the benefit to society
Reduction in number of molested children	Quantifiable: estimate number of saved children compared to baseline. Monetary units: perhaps possible to convert to monetary units using US statistical values. Value of each unit of benefit (life of a child): extremely high.
Reduction in young or vulnerable individuals exposed to shocking images	Quantifiable: estimate reduction in number of persons exposed to images compared to baseline. Monetary units: difficult to convert to monetary values. Value of each unit of benefit: high

Category of benefit	Quantifiable? Value of the benefit to society
Increased use of internet due to making the internet safer	Quantifiable and possible to convert to monetary values.
Affirming society's refusal to tolerate serious human rights violations on the internet	Non-quantifiable: high symbolic value.

Where benefits cannot be translated into monetary values, they should be given qualitative labels or scores, using one of the methods examined in Section 4.1.

(c) The causal link between the regulatory measure and the benefit.

Once the benefits have been broken down into categories, the drafters of the cost-benefit analysis should then determine the strength of the causal link between the proposed regulatory measure and the achievement of the relevant category of benefit. For example, the linkage between the blocking of access to child porn images and the reduction in the number of abused children may be difficult to establish. The link would be indirect at best. The most direct way to reduce the number of abused children is to arrest child molesters. Fewer criminals would result in fewer victims. A regulatory measure limiting access to child porn images could potentially reduce demand for child porn images and therefore potentially lead to a reduction in supply, and therefore a reduction in the number of sexually abused children. But this is not the only possible outcome. An enforcement measure that achieves 100% blocking might make the task of finding and arresting child molesters more difficult for law enforcement authorities because the criminals would use more hidden ways to exchange images. This could paradoxically increase the number of victims. Thus the causal link between the hypothetical "perfect" blocking measure and the category of benefits related to saved children is likely to be indirect, and may (depending on the views of law enforcement authorities) even be counter-productive.

The link between the enforcement measure and the creation of a safer internet may be more direct. There, too, however, it would still be necessary to show that the safer internet in fact increases internet usage.

The most direct causal link would relate to achieving the symbolic benefit of showing zero tolerance for serious violations of human right on the internet. A new regulatory measure would in most cases have a direct causal link to achieving this benefit.

Category of benefit	Value of the benefit to society	Causation link with the blocking measure
Reduction in number of	Quantifiable	Weak

Category of benefit	Value of the benefit to society	Causation link with the blocking measure
molested children		
Reduction in young or vulnerable individuals exposed to shocking images	Quantifiable	Strong
Increased use of internet due to making the internet safer	Quantifiable	Medium
Affirming society's refusal to tolerate serious human rights violations on the internet	Non-quantifiable: high	Strong

(d) Practical measurement of success.

As a last step, the drafters of the cost-benefit analysis should try to determine the practical measurability of "success" for each category of benefits. What would one count in order to determine if the benefit has increased, decreased or remained the same, and is the counting practical? In our example, the number of sexually abused children in a year is probably easy for regulators to count based on police records. For the second category, it would be hard to measure directly the number of persons exposed to shocking child-porn images. Indirect measurement may be possible through questionnaires, or by developing a test to determine the time it takes an average internet user to find shocking images. Presumably the more time it takes to find child-porn images, the less likely it is that young or vulnerable people will find them by accident. There may be an indirect correlation between the time it takes to find a child-porn image and the number of persons exposed in a given year.

The third category would be difficult to measure without experiments between two populations, one in which a child-porn blocking measure has been imposed by regulation, and another where no such regulation has been applied. One would then measure the difference in usage levels of the internet.

The last category, which consists of affirming an important normative value in society, might be measured by surveys asking people if they are aware of the regulatory enforcement measures designed to block access to child porn images on the internet and the sanctions that accompany any effort to circumvent those measures. Success would be measured through the level of public awareness of the measure.

Category of benefit	Value of the benefit to society	Causation link with the blocking measure	How to measure success
Reduction in number of molested children	Quantifiable	Weak	Number of children sexually abused during a year
Reduction in young or vulnerable individuals exposed to shocking images	Quantifiable	Strong	Time it takes an average uninitiated adult or adolescent to find child-porn images on the internet
Increased use of internet due to making the internet safer	Quantifiable	Medium	Usage statistics, but requires experiment with control group
Affirming society's refusal to tolerate serious human rights violations on the internet	Non-quantifiable: high	Strong	Surveys to measure citizens' awareness of regulatory measure

(e) Identifying the maximum possible benefits

When developing success metrics for the regulatory alternatives, the drafters of the cost-benefit analysis should try to define first what "total success" would look like for each category of benefits, as compared to the baseline scenario. The difference between "total success" and the baseline scenario would represent the maximum benefits that the enforcement policy can possibly achieve. The "total success" scenario should correspond to 100% enforcement of the content policy on the internet, *ie*. 100% blocking of the harmful content, regardless of costs.

For example, for a measure designed to fight child pornography, the 100% enforcement scenario might correspond to the use of deep packet inspection and image recognition technology to block anything that looks like a child without clothes. This technology would probably block all child porn images, but would also block images from medical textbooks and artwork. The over-blocking would create significant costs. But the benefits would correspond to the maximum achievable, ie. the outer limit of what is possible.

This level of 100% enforcement, and the corresponding maximum potential level of benefits, will almost never be the optimal level, but will help define the maximum range of available benefits. The baseline scenario represents the lower limit of the range, and the 100% enforcement represents the upper limit of the range. The optimal level will be somewhere in between. The optimal level will correspond to the amount of enforcement at which the marginal cost of an additional unit of enforcement is equal to the marginal benefit gained by the extra unit of enforcement. Put another way, the level of enforcement should be situated at a point where the sum of the costs of harms related to the content policy and the costs of prevention is minimized.

In most cases, the marginal cost of enforcement increases as the level of enforcement approaches 100%. Achieving 99% enforcement may be hugely more costly than achieving 95% enforcement. The marginal benefit generally remains constant, or may even decrease. Thus optimal enforcement is usually less than 100%.

By first looking at an extreme enforcement scenario, it will be easier to apply a sensitivity analysis to see what benefits less-than-total enforcement would deliver. For example, the drafters of the cost-benefit analysis may conclude that 100% blocking of child porn images is not likely to reduce the number of sexually abused children, or that the connection between blocking and the reduction in the number of victims is too tenuous to support projections. By contrast, total blocking may reduce by "*x*" the number of vulnerable people who, in a given year, accidentally find child porn images and are influenced by them. "x" is the maximum benefits in this category that could possibly be achieved. The sensitivity analysis would seek to determine by how much "*x*" is reduced for various regulatory options that consist blocking of less than 100% of all images.

For the category of benefits associated with affirming society's refusal to tolerate exploitation of children on the internet, the total enforcement scenario might yield a public awareness factor that is 100% higher than the baseline scenario. The drafters of the CBA may find, however, that an enforcement scenario of 85% (as opposed to 100%) also yields a 100% increase in awareness compared to the baseline scenario. The sensitivity analysis would show that a lower level of enforcement still yields a high level of benefits for this category.

(f) For each regulatory proposal, estimate the level of benefits between the maximum and minimum.

Once benefits have been broken down into categories, and the minimum (corresponding to the baseline scenario) and maximum (corresponding to 100% enforcement) for each category have been identified, the drafters of the CBA should determine where benefits lie for each of the regulatory proposals. Drafters should use the same methodology as they applied to the baseline scenario and to the 100% scenario. For each technical option

(search engine, DNS blocking, self-regulatory initiatives), the drafters would have to determine if the option yields benefits that are close to the baseline, close to the 100% scenario, or halfway in between. It may be possible to position each option according to its level of achievement of the maximum. For example, a DNS blocking measure may attain 100% of the maximum benefit for the category of affirming society's refusal to tolerate child porn images, and 85% of the maximum for category corresponding to preventing young or vulnerable people from being exposed to shocking images.

4.4 The direct costs resulting from each proposal, including direct costs for internet intermediaries, their customers, and taxpayers

After analysing benefits, the next step in the cost-benefit analysis involves examining the direct costs generated by each proposal compared to the baseline.

Calculating the level of direct cost is relatively straightforward. This is what most regulators already do when they prepare a cost-benefit analysis. If the proposal involves setting up a new regulatory authority, the cost-benefit analysis will include a calculation of the setup costs and annual operating expenses of the new authority. The impact assessment then generally attempts to calculate the level of compliance costs for businesses. If the proposal involves new reporting requirements for businesses, the cost-benefit analysis will attempt to calculate the number of businesses affected and the annual cost per business of completing the new paperwork.

Direct costs would also include capital expenditures and operating expenses for internet intermediaries that would not have been incurred but for the new regulatory measure. An example of this kind of expense is the cost of installing and operating filtering equipment at various points in an ISP's network. Another example is the annual cost of processing "right to be forgotten" requests by a search engine, including the costs of hiring new staff to evaluate delisting requests. After the *Costeja* judgment of the European Court of Justice, operators of search engine created online processes to handle delisting requests made by European individuals. The search engine operators had to hire new employees to handle the hundreds of thousands of delisting requests filed using the online tool. Search engine operators also had to deal with new legal claims before courts and data protection authorities, giving rise to legal costs. The one-time costs of setting up the process and the annual costs of administering the process would be included in the category of direct costs created as a result of the regulatory measure.

Direct costs can generally be estimated in monetary terms. In the case of delisting requests under the European "right to be forgotten", it should be fairly easy to calculate the amount of the direct costs associated with each delisting request. It would suffice to calculate the sum of (i) the additional costs incurred by regulatory authorities and courts to deal with delisting requests and (ii) the total costs incurred by operators of search

engines, and then divide these aggregate costs by the number of delisting requests. This would yield the direct cost associated with enforcing the new right recognized by the European Court of Justice.

4.5 The indirect costs resulting from each proposal, including relative impacts on fundamental rights, on the internet ecosystem and innovation

Direct costs are only part of the story. Most actions taken by internet intermediaries to enforce content policies create indirect costs, and these are much harder to evaluate. They are generally ignored today in impact assessments. Some of these costs may be difficult or impossible to quantify in monetary terms, in which case one of the methods examined in Section 4.1 must be used.

If we use the example of measures to fight online copyright infringement, the following indirect costs may be generated:

(a) Harms to innovation and competition.

The imposition of obligations on technical intermediaries might discourage market entry, or encourage market exit by smaller players, thereby decreasing competition and innovation (Haber, 2010; Breyer, 1982). Technical measures might be proportionally less costly for large players to implement than for smaller players or new market entrants, thereby reinforcing the market power of large existing players. If these costs for smaller intermediaries are not reimbursed, they could create barriers to entry, thereby making markets less contestable and competitive. Technical intermediaries might also increase their prices to reflect the cost of the technical measure, which could cause certain internet users to reduce their activity (Lichtman, 2005). Imposing obligations on technical intermediaries may also damage innovation and growth by altering the open and neutral architecture of the internet. This might decrease innovation, competition and growth, not to mention affect fundamental rights.

In addition to the cost burden associated with implementing a given technical measure, its imposition may also skew competition because the measures reflect a particular technology or approach promoted by one actor that disadvantages its competitors. To minimize this potential cost, regulators should endeavor to impose technologically neutral remedies, performance standards as opposed to technologically specific “design” standards (Breyer, 1982). Regulators should make sure that measures are subject to public consultation and stakeholder comments, so as to identify any hidden competitive distortions (Hancher, Larouche and Lavrijssen, 2003).

(b) Harms to fundamental rights.

A measure designed to limit access to harmful content will in most cases affect freedom of expression and privacy. Those indirect costs are hard to quantify, so one of the techniques mentioned in Section 4.1 will have to be used. Freedom of expression and access to information does not justify unrestricted access to all content. Nevertheless, most technical measures will be over-broad, blocking some content that is legitimate. Any overspill will be considered as an interference with freedom to access information.

While freedom of expression and access to information is probably the most important right affected by technical measures, the right to privacy will also likely be affected. Measures intended to limit access to harmful content will often have a potential adverse effect on privacy. For example, a system that tracks online behavior to detect copyright infringement carries inherent risks because the system, or the data it collects, can potentially be misused. Like the collection of geolocation information, the collection of IP addresses for purposes of limiting copyright infringement must be surrounded by safeguards to avoid possible abuse. A system that does not permit the identification of individual downloaders will create lower privacy costs than a system that permits such identification.

(c) Dividing indirect costs into categories.

For each category of indirect cost, the drafters of the impact assessment should determine whether the costs are quantifiable, and if so whether quantification is possible in monetary terms. For those costs that are not quantifiable in monetary terms, the drafters of the impact assessment should use one of the techniques described in Section 4.1 to measure the intensity of the relevant cost. Scoring systems, such as the one proposed by Robert Alexy for fundamental rights, might be used. Using qualitative labels such as "extremely high", "high", "medium", and "low"', may still permit certain proposals to be eliminated without it being necessary to add up the qualitative scores in a column in order to arrive at an aggregate score of non-quantifiable costs. A proposal may be eliminated because we know that its net benefits are necessarily lower than those of another competing proposal. For example, as between two proposals with equal benefits and equal quantifiable costs, the proposal that creates a "high" level of harm to freedom of expression and to innovation would necessarily yield lower net benefits than the proposal that creates a "medium" level of harm to freedom of expression and to innovation.

Another way to eliminate certain proposals based on the qualitative labels is to impose a constraint in the cost benefit analysis, such as: "any proposal with a harm to freedom of expression exceeding the 'medium' level shall be eliminated." Constraints will be discussed in Section 4.7 below.

To illustrate how non-quantifiable costs are treated, let us examine three proposals designed to reduce online copyright infringement. Proposal A involves deep packet inspection, proposal B involves DNS blocking, and proposal C involves graduated response.

	Proposal A Deep packet inspection	Proposal B DNS blocking	Proposal C Graduated response
Quantifiable benefits per annum compared to the baseline scenario	500M€	500M€	400M€
Direct costs per annum compared to the baseline scenario (quantifiable)	400M€	100M€	300M€
Net quantifiable benefits	100M€	400M€	100M€
Indirect costs per annum compared to the baseline scenario			
Harms to freedom to access information (non-quantifiable)	Low	Medium	Low
Privacy harms (non-quantifiable)	Extremely High	Low	Medium to high
Harm to net neutrality and the proper functioning of the internet (non-quantifiable)	High	High	None

Table 3: Illustration of labeling non-quantifiable costs.

In this example, proposal A consists of deep packet inspection permitting the ISP and right holders to determine with a high degree of accuracy the content that should be blocked because of a violation of copyright. The impact on freedom to access legitimate information will be low because there will be few, if any, false positives. However people

may reduce their activity because they feel they're being watched. (Reduction of activity would indirectly reduce freedom to access information.)

The negative impact on privacy will be extremely high because deep packet inspection can easily be used to spy on individual opinions. Some countries use this technology to do precisely that. The negative impact on the internet's end-to-end architecture will be high because network equipment will be used not just to route packets but to apply content policies. This would be viewed by net neutrality advocates as a dangerous disrespect for the layered character of internet transmissions. Net neutrality dictates that except for measures needed to assure good network management, routing and transmission equipment should not become involved in the content of packets. Content policies should be implemented whenever possible at the edges of the network, using software on terminal equipment.

Proposal B consists of blocking access to certain websites through DNS blocking. DNS blocking consists of substituting a wrong IP address for the right one in the central directory that permits websites to be identified and found. The potential harm to freedom to access information is medium because there may be over-blocking. DNS blocking can block perfectly legal content in addition to the targeted illegal content. The negative impact on privacy is low because the technology is less capable of tracking individual behavior. Unlike deep packet inspection, DNS blocking does not keep track of individual attempts to access the content. The negative impact on internet architecture and net neutrality is high because DNS blocking amounts to inserting false addresses in the local version of the DNS registry, thereby tricking routing equipment to deliver packets to the wrong destination.

Proposal C consists of issuing administrative fines against persons who have been detected as illegally downloading copyrighted works. No blocking occurs, but individuals may reduce their activity because they are afraid of being watched, leading to some restriction on freedom to access information. This yields a "low" harm to freedom of expression. The negative effect on privacy is medium to high, because the mechanism tracks individual usage, and results in network operators and public authorities translating IP addresses into names of individual subscribers. Mechanisms like this could potentially be misused to spy on individuals, even though most graduated response mechanisms include strict controls over the use of individual IP addresses.

Proposal C respects net neutrality because the system does not interfere with routing functions on the internet. The internet continues to function as it should. There is no harm to the internet architecture. The IP addresses of potential infringers are identified by agents of rightholders who introduce themselves into peer-to-peer networks and make note of users who offer copyright-protected content. Outside agents watch what is

happening, but do not interfere with the functioning of the internet. The benefits of graduated response are lower than for DNS blocking and deep packet inspection because graduated response only affects peer-to-peer file exchanges.[62]

4.6 How to rank proposals

Going through this exercise already permits us to conclude that proposal C is superior to proposal A. Both have a positive quantifiable net benefit of 100M€, but proposal A scores less well than proposal C with regard to harms to privacy and to net neutrality. However, we are not able to determine whether proposal B is superior to C, or vice versa. Proposal B has a much higher net quantifiable benefit (400M€ versus 100M€) than C, but B scores worse than proposal C on freedom of expression and net neutrality, while better than proposal C on privacy. As between proposals B and C, the trade-off is therefore whether the 300M€ difference in quantifiable net benefits, plus the better protection of privacy under proposal B more than offsets the marginal harm to freedom of expression and net neutrality caused under proposal B compared to proposal C.

If we assume that the harms to freedom of expression and privacy are roughly equivalent (which is not an unreasonable assumption given European case law), we are left with a more explicit trade-off: is the DNS blocking system's harm to net neutrality worth more than 300M€ per year?

We see in this simplified example that even where certain costs are not quantifiable, the process of comparing costs and benefits can nevertheless permit some proposals to be eliminated, and for the remaining proposals, the process can make trade-offs more explicit.

4.7 Applying additional constraints

The list of benefits and costs in the cost-benefit analysis may not capture the full range of parameters identified in the questionnaire. Where this is the case, the additional parameters can be applied to the outcome of the cost-benefit assessment in order to help rank the proposals. For example, if two or three proposals emerge from the cost-benefit analysis as requiring trade-offs based on non-quantifiable costs or benefits, additional rules may help eliminate certain proposals, or give added weight to others.

Fundamental rights: Where qualitative labelling is used to characterize costs to fundamental rights, a rule could be created to eliminate any proposal that contains an "extremely high" harm to any fundamental right. Similarly, a proposal that contains more than one "high" interference with a fundamental right could be eliminated. This constraint would permit the application of an ethical filter after the initial cost-benefit analysis, such as that proposed by Nussbaum (2002).

---

[62] The assumptions I present here are for illustration purposes. Actual proposals may have different characteristics.

International legitimacy: If international effects have not been incorporated into the indirect costs of the cost-benefit analysis, an additional rule could be created to give added weight to a proposal that has been used in other democratic countries, versus a proposal that has not been used in another democratic country. Similarly, added weight could be given to a proposal that is consistent with the OECD recommendations on internet policy making.

Technology neutrality: If technology neutrality has not been incorporated into the indirect costs of the cost-benefit analysis, an additional rule could be created to give added weight to a proposal that is technologically neutral versus one that is not.

Adaptive regulation: If "flexibility" has not been incorporated into the benefits or costs of the cost-benefit analysis, a rule could be created to give added weight to a proposal that is flexible, and can be easily modified or withdrawn, as compared to a proposal for which the modification costs are high.

4.8 Conclusion on how to rank proposals

Cost-benefit analyses will fall into one of four categories:

Category 1: All benefits and costs can be converted into monetary amounts. This case is the most straightforward, but will be unusual for measures designed to limit access to harmful content.

Category 2: Benefits and costs will both include a combination of quantifiable (in monetary terms) and non-quantifiable elements. This will be the most frequent scenario, to which we will return below.

Category 3: Benefits are quantifiable in monetary terms, and costs consist of both quantifiable (in monetary terms) and non-quantifiable (in monetary terms) elements.

Category 4: the mirror image of category 3: All costs are quantifiable in monetary terms, and benefits consist of both quantifiable (in monetary terms) and non-quantifiable (in monetary terms) elements.

The simplified example in Section 4.5 above (proposals A, B and C to fight copyright infringement) falls into category 3: All benefits are quantifiable in monetary terms. This example helped show how the use of qualitative labels on the costs side can still help eliminate certain proposals, and make choices more explicit.

Environmental, or health and safety measures often fall into category 4. Benefits include difficult-to-quantify elements such as saving a species of frog or wildflower, whereas costs are generally quantifiable in a monetary sense. To deal with category 4, United States regulators advise using a "cost effectiveness analysis" (CEA), which consists of

calculating the monetary cost of achieving a given unit of benefit, the unit being a non-monetary measurement such as a year of life saved, or the preservation of a hectare of wilderness. The proposal that delivers a unit of benefit at the lowest monetary cost would be preferred over other competing proposals.

Let us examine category 2, which will be the most frequent for regulatory measures designed to restrict access to internet content. Non-quantifiable elements will appear on both the benefits and cost sides, which makes the ranking process complicated. Here is a way it could be done.

Step 1: calculate net monetary benefits. As with our category 3 example examined in Section 4.5, a useful first step is to calculate the net quantifiable monetary benefits corresponding to each proposal.

Step 2: check if any proposals can be eliminated based on the constraints mentioned in Section 4.7. For example, a proposal with an "extremely high" impact on privacy or freedom of expression would be eliminated.

Step 3: check that the success parameters have been carefully defined and applied on the benefits side of each proposal. Eliminate false success parameters. In Section 4.3 I proposed a way of doing this. The important point is to break benefits into different categories, determine ways to measure success compared to the baseline scenario for each category ("success metrics"), and then estimate how the success metrics will vary for each proposal compared to the baseline, taking into account the uncertainties of causation. As illustrated in the child pornography example in Section 4.3, causation may be so tenuous for certain categories of benefits that the relevant categories should be eliminated entirely from the equation.

It may be possible to convert the relevant the success metric into a score. The European Commission's SURVEILLE project on police surveillance measures (examined in Chapter 7) attempts to do this by attributing a score for effectiveness of the surveillance measure in fighting crime. However, where there are different categories of benefits -- as will often be the case for measures limiting access to harmful content -- attributing a single aggregate score for multiple benefit categories can be problematic.

Step 4: for difficult-to-quantify costs, choose between using a scoring mechanism such as Alexy's, or using qualitative labels such as "high", or "extremely high". Because European courts have held that the right to privacy and the right to freedom of expression have equal normative value, a scoring mechanism relating to these two rights would work. A score of +1 for privacy could offset a score of -1 for freedom of expression. As Alexy's system recognizes, severe restrictions on either of these rights are not permitted, so the set-off rule only works for light or moderate restrictions. One simplifying measure

therefore would be to use scoring for privacy and freedom of expression rights, both on the costs and on the benefits side.

However, even this is tricky. Let us take the example of measures designed to protect the so-called "right to be forgotten" (RTBF). The benefits would consist in protecting privacy, and costs would involve limitation to freedom to access information. Theoretically, these could be set-off. Various technical measures used to achieve the right to be forgotten would carry different levels of benefits for privacy, and different levels of impacts on freedom of expression. Scoring these different levels is not straightforward, in large part because the right to be forgotten benefit is not intended to be total. Its objective is to make access to certain content less likely, but not impossible. Attributing a score to the benefit corresponding to each technical measure could be difficult.

Example:

RTBF Proposal A: Delisting on local domain results covers 98% of search requests in the territory being covered.

RTBF Proposal B: Delisting on all domains for users within the territory using IP restrict covers close to 100% of search requests in the territory.

Proposal A results in a very large difference compared to the baseline (from 0% to 98% of coverage). Proposal B results in a small incremental benefit (+2%) compared to proposal A. It is unclear how Alexy's system would score the small incremental increase in benefit between proposals A and B.

Considerable work is needed before relying on a scoring mechanism, particularly where incremental differences in effects on fundamental rights are small.

It is difficult to conduct a cost-benefit analysis with hard-to-quantify benefits and costs. I have touched in Section 4.1 on methods that can be used. The ideal solution is to transform all costs and benefits into monetary values. Standardized values have been created relating to the value of a human life. Once a standard value has been fixed for the statistical value of one year of life saved, this statistical value can be used to measure the benefits associated with regulatory proposals to limit air pollution, for example. If a monetary value can be associated with a year of human life, it is not absurd to think that a monetary value could be attributed to the protection of privacy or freedom of expression.

Other methods consist of choosing non-monetary units to count benefits or costs, such as the number of films produced annually, or the time it takes for an average person to find pornographic images on the internet. Scoring or qualitative labels are also possible. Before the cost-benefit analysis I describe can become operational, it would be necessary

to refine and possibly standardize these approaches. The methodology would lose much of its value if regulators used different approaches.

5. PUBLIC CONSULTATION

The questionnaire and cost-benefit analysis should then be subject to public consultation. If we refer again to regulatory proposals in the European system for regulating electronic communications, public consultation is a critical part of the process. The regulator prepares its justifications for the regulatory measure based on the market analysis and the requirements of the European Framework Directive 2002/21/EC. The analysis and proposal are then submitted to public consultation. The comments received from the public consultation are analysed by the regulator. The regulator must show in its final proposal, which is sent to the European Commission's Article 7 Task Force, that it has taken due account of the various comments received as a result of the public consultation. The peer review conducted by the European Commission will verify whether the comments of stakeholders have been taken into account.

In the system I propose here, the questionnaire and cost-benefit analysis would be published for public consultation before being sent to peer review. After receiving public comments, the drafters of the impact assessment would summarize the main inputs from the consultation process, and revise the conclusions of the cost-benefit analysis and questionnaire accordingly.

Public consultation contributes to transparency, which enhances the legitimacy of the proposed action and the likelihood of compliance by affected stakeholders (Hancher, Larouche and Lavrijssen, 2003). Public consultation is part of "better regulation" (OECD, 2012).

6. INSTITUTIONAL PEER REVIEW

The literature on better regulation shows that regulatory impact assessments are of limited utility if they are not reviewed by an independent institution (OECD, 2012; Conseil d'Etat, 2016). The initiators of regulatory proposals generally act in response to political needs to take action with regard to a perceived market or regulatory failure. The proponents of regulation will often have a conflict of interest because their superiors have made a political decision that a given regulatory solution is needed. The drafters of the impact assessment will tend to reverse engineer the impact assessment in order to support the proposal that meets the political needs of their management. The persons completing the impact assessment will often have no interest in examining indirect costs of the measure, or the risk of regulatory error. Those costs and risks will materialize only much later, well beyond the relevant political horizon. The drafters' priority will be to complete the impact assessment as quickly as possible and for the document to contain enough evidence to support the proposal that political decision-makers want.

This is why independent review is critical. As noted above, the European Commission's "Article 7" reviews in the electronic communications sector provide a useful example. The peer review is conducted by individuals from the European Commission who are independent from the

institutions proposing the regulatory measure. The peer review team is supervised by officials at the European Commission whose only objective is to ensure that the principles set forth in the European Directives are applied properly. Their goal is good regulation rather than satisfying political demands for action. Proponents of regulatory measures must plead their case before the peer review panel, in some cases asking for exceptions from the strict rules imposed by the directives.

The Article 7 Task Force also has the advantage of reviewing similar regulatory proposals from throughout Europe. The panel gains accumulated knowledge and perspective that may not be available to regulators in a single member state.

In Europe, the best peer review panel for regulatory proposals relating to internet content would be the European Commission, because of its relative independence from political pressure at the member state level. However, this would require the adoption of a European directive or regulation giving the European Commission power in the field of internet regulation. As is the case for peer review in the electronic communications sector, the European Commission could potentially have the right to open phase II proceedings where the rationale given by member states for their regulatory proposals is insufficient. In some cases, the European Commission would have the right to veto measures if they diverge too much from regulatory best practices. A peer review system could also be established at the national level (Conseil d'Etat, 2016).

A peer review system is currently used in the United States for any federal regulatory proposal. Each agency must submit its cost-benefit analysis to the OIRA (see Chapter 5, *supra*). The OIRA scrutinizes the cost-benefit analysis to ensure that it complies with the methodology imposed under Circular A4. OIRA can request revisions to the cost-benefit analysis, or even veto the measure. This power explains why the director of OIRA is referred to as the United States's "regulatory czar."[i63]

Currently, OIRA does not review proposed legislation that is to be submitted to Congress, or proposed regulation from independent regulatory authorities such as the FCC. Thus most regulatory or legislative proposals involving internet regulation escape OIRA's scrutiny. United States law would have to be modified if OIRA were to have power to review regulatory proposals involving internet content. However, OIRA seems to be a good example of effective peer review.

After receiving comments from the peer review institution, the drafters of the impact assessment would modify the proposal to take the peer review comments into account. Once this is done, the proposal, including the questionnaire and cost-benefit analysis, would be submitted to the relevant decision-making authority for final adoption. If the measure is legislative, the relevant decision-making authority would be the legislature. If the measure is regulatory, the relevant decision-making authority would be regulatory authority or government agency.

---

63 R. Rampton and J. Mason, "Obama nominates antitrust expert Shelanski as new regulatory czar", Reuters.com, April 25, 2013.

7. PERIODIC REVIEW OF THE MEASURE

The last element of the methodology is to ensure that regulatory measures are reviewed *ex post* to ensure that they are still fit for purpose. Measures that are not delivering the expected level of benefits, or that are creating unanticipated costs, should be modified or eliminated. In the field of electronic communications, regulators must conduct periodic market analyses to identify technological and market trends that have occurred during the last 36 months, and evaluate the impact of those trends on competition in the market. Where a particular regulatory measure is no longer necessary to ensure effective competition, the measure must be removed. The European Commission's Article 7 Task Force panel for electronic communications will examine the market analysis and ensure that the regulatory authority has considered the option of removing regulatory provisions where they are no longer necessary.

Given the fast rate of change of internet technology and markets, the risk of regulatory error is high (Shelanski, 2013). The impact assessment and peer review are designed to reduce the risk of error upfront. Periodic *ex post* review is designed to detect and correct errors that become visible later. As examined in Chapter 5, "adaptive regulation" (Whitt, 2009) requires that regulatory measures be tested regularly to determine whether they are still fit for purpose. *Ex post* review is advanced by the Conseil d'Etat (2016) as a key element of good law making.

8. CONCLUSION

The entire system is summarised in the following flowchart:

CHAPTER 7 – STRENGTHS AND WEAKNESSES OF THE PROPOSED METHODOLOGY AND AREAS OF FUTURE RESEARCH

1. STRENGTHS OF THE METHODOLOGY

I have attempted to present a better system for reviewing regulatory proposals designed to limit access to harmful content on the internet. My purpose is to bring more analytical rigor to the preparation of proposals. The impact assessment (questionnaire, cost-benefit analysis and accompanying steps) will require systematic consideration of:

(i) what is likely to happen in the absence of regulatory intervention (the "baseline scenario" or "counterfactual");

(ii) the benefits that the proposals seek to achieve, and how to measure them compared to the baseline ("success metrics");

(iii) the direct and indirect costs that the regulatory proposals may generate, including those that are difficult or impossible to quantify in monetary terms; and

(iv) alternative approaches, both technical and institutional.

I explore whether the methodological rigor used for regulation of electronic communications in Europe could be used as a starting point for internet regulation. I also look at the principles used in regulatory impact assessments in the United States -- and increasingly in Europe -- to internet content regulation. United States "better regulation" principles require that agencies

> *"assess both the costs and the benefits of the intended regulation and, recognizing that some costs and benefits are difficult to quantify, propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs."*[64]

As pointed out by the office within the White House in charge of reviewing impact assessments,

> *"regulatory analysis … provides a formal way of organizing the evidence on the key effects -good and bad - of the various alternatives that should be considered in developing regulations. The motivation is to (1) learn if the benefits of an action are likely to justify the costs or (2) discover which of various possible alternatives would be the most cost-effective."*[65]

A more rigorous impact assessment would require the proponents of regulation to identify a clear market failure that cannot be addressed by existing legislation, and to define objective success metrics. This would act as a healthy counterweight to politicians' normal tendency to create new regulations to deal with new perceived problems emerging from digital markets (Sunstein,1996; Shelanski, 2013).

---

64 Executive Order 12866.

65 The White House, Office of Information and Regulatory Affairs (OIRA), Q&As, https://www.whitehouse.gov/omb/OIRA_QsandAs, accessed February 28, 2016.

The uniform methodology and peer review system I propose here would permit knowledge to be shared, and best practices to emerge. Over time, best practices would emerge for each type of internet content problem (copyright infringement, privacy, child pornography, protection of minors) and any new regulatory proposal would be measured against those best practices.

Finally, the methodology would help distinguish measures adopted in democratic countries like France from measures adopted in totalitarian regimes to censor content. Without a robust benchmark against which to measure proposals, it is difficult to criticize other countries for adopting blocking measures when the country doing the criticizing also applies blocking measures for its own content policies.

2. WEAKNESSES OF THE METHODOLOGY, AND POSSIBLE RESPONSES

There are a number of reasons why the system proposed here may not work as expected. Some of these reasons have already been mentioned in Chapter 5 in connection with criticisms of better regulation methodology.

(a) Criticism 1: Interference with democratic debate.

The first objection is that the rigors of a well-done impact assessment are incompatible with the sometimes messy trade-offs in the political process. Measures taken to limit access to harmful content involve fundamental rights and societal values that require political debate in the legislature. Debate on these issues cannot be reduced to a formula. The framework for regulating electronic communications, which deals with economic and technical questions of limited political impact, may not be transposable to questions involving fundamental rights and societal values. For measures involving the fight against terrorism or child pornography, the trade-offs involve public fears and moral values that are not always compatible with rational regulatory analysis.

The response to this criticism is that rigorous analysis of regulatory options does not preclude emotional political debate (Hahn, 2004). On the contrary, a conscientiously-drafted impact assessment can become an important element of the debate, helping avoid costly errors and making political choices more explicit. The impact assessment is merely an input to the decision, not a rule that dictates a particular outcome (Posner, 2000). The impact assessment would not replace a legislative compromise on an emotional issue such as the fight against terrorism, but would provide an objective reference point against which to measure legislative proposals. For example, a national legislature may still decide to grant broad powers to the government to block websites without judicial oversight, but the impact assessment would show that the measure is not in line with best practices. The impact assessment would potentially be used in judicial review of the measure's constitutionality.

What's clear however is that political decision makers would have little or no interest in buying in to a system that constrains their own decision making authorities. Why would they? The political

process is already sufficiently complex without adding another constraint linked to a cost-benefit analysis. Governments and parliaments are elected based on their political visions and principles, which are generally incompatible with the dry calculations of a cost-benefit analysis. As mentioned by Radaelli and De Francesco (2010), politicians will all support the idea of evidence-based laws and regulations as long as this remains an abstract concept. However, when it comes to actually implementing a rigorous cost-benefit analysis system, politicians will see only a downside. The only exception to this would be where a regulatory impact assessment is mandated for independent regulatory authorities. Here, law makers will see the impact assessment as a useful constraint on an independent regulator's powers. Law makers sometimes see the delegation of powers to independent regulatory authorities with suspicion since those authorities are not directly accountable to the government, the parliament or to citizens. It is therefore no coincidence that the rigors of market analysis and impact assessments are seen most frequently in the field of telecommunication regulation, where independent regulatory authorities have significant discretion. It is also no coincidence that the OECD sees many countries adopting the principles of better regulation, but failing to actually implement them in practice.

(b) Criticism 2: Conflicts of interest.

The impact assessment methodology described in Chapter 6 will run into conflict of interest problems, as do all regulatory impact assessments. The drafters of the regulatory impact assessment may report to a minister or a president who has already made a political decision to implement a certain measure. The drafters will not want to undermine their boss's proposal, and so will have a natural tendency to reverse engineer the impact assessment to fit a given outcome. It is not reasonable to expect the government to prepare an impact assessment that would go against a political decision made by the president. A peer review system can help this problem, but it will not cure it entirely.

The OECD recommends that governments create a separate office to conduct impact assessments (OECD 2012), but even a separate office will not be immune from conflicts of interest if the president or prime minister has publicly supported a particular outcome.

For this reason, impact assessments of the kind I describe here may work best where the legislature has delegated to an independent regulatory authority the task of finding the optimal solution to a problem such as limiting pollution or access to harmful content on the internet. The regulatory authority's mission would be to apply a cost-benefit analysis when developing measures to protect citizens against harmful internet content. However, this implies that the government and legislature are comfortable delegating to a regulatory authority the responsibility for making these choices.

(c) Criticism 3: Impact assessments are too expensive and complicated.

Impact assessments are complicated and costly to prepare. If there is anything that this thesis has shown, it is that a comprehensive cost-benefit analysis would be extraordinarily complex, involving many variables that are difficult or impossible to quantify, such as the impact of a measure on the internet ecosystem or on fundamental rights. Because many of the estimates of costs or benefits rely on subjective factors on which reasonable people can disagree, the results of the cost-benefit analysis could easily be challenged. If the cost-benefit analysis is costly and time-consuming to prepare, and the results are contestable, what good is it?

Here, too, the European regulatory framework for electronic communications provides some guidance. The framework for electronic communications is also difficult to apply. It is based on principles such as the "three criteria test", pursuant to which electronic communications markets should not be subject to *ex ante* regulation unless they show durable barriers to market entry, no signs of evolving toward effective competition, and competition law is inadequate to address market failures. The relevant markets themselves are to be defined using standard competition law tools, and dominance assessed within those markets using competition law methodology. If national regulators were left alone to apply these principles, they would have conducted costly studies, and likely reached different outcomes. The criticism: "Too complicated and too expensive" would apply there, too. To address this problem, the European Commission issued recommendations and guidelines that indicate which relevant markets pass the three-criteria test, and how dominance should be assessed on these markets. National regulators were given an initial instruction manual to guide their decisions. The instruction manual included a number of simplifying assumptions that national regulators could feel safe applying. Regulators could challenge the Commission's simplifying assumptions if they had strong reasons to do so, but the easiest approach for most regulators was to use the simplifying assumptions contained in the European Commission's guidelines.

A similar approach could be used here. The European Commission (or another authority) could provide a list of benefits and costs to be considered in every impact assessment, and issue guidelines one how to measure certain costs. For example, the Commission could indicate that measures involving deep packet inspection (DPI) would normally create "high" or "extremely high" costs for privacy, because of the danger that DPI could be misused to spy on individuals. National authorities would be free to disagree with the Commission's conclusions, but would have to explain why. The Commission's guidelines could be developed in cooperation with the European Union Agency for Fundamental Rights.

Consequently, one useful simplification measure for my methodology would be for a central authority – presumably the one that would conduct peer reviews – to provide initial guidance on how various measures might be scored in the CBA. This would provide a non-binding starting point for the drafters of the regulatory impact assessments. The guidelines may not avoid qualitative trade-offs of the kind: "Is a 300M€ per year increase in net benefit worth a 'high' impact on net neutrality?" But if regulators apply a consistent approach to valuation -- via scoring,

qualitative labels, or other techniques -- the overall quality of decisions will increase because it will be possible to compare results across different subject matters and jurisdictions.

The second lesson from the EU framework for electronic communications is that the first years of impact assessments will be difficult, but that the task then gets easier. In the system proposed in this chapter, the drafters of impact assessments will be conducting impact assessments on internet content measures for the first time, and there will be few examples available from other countries to rely on. Each impact assessment will be new and complex, even with simplifying assumptions issued by a central authority such as the European Commission. The peer review team will also be learning as they go. The peer reviewers will be trying to develop a consistent approach in assessing proposals, and may make mistakes along the way. However, once the initial round of impact assessments and peer reviews has been completed, things will get easier. The second round will be easier than the first, and the third easier than the second. The peer review panel will share best practices from other countries, and publish criticisms and veto decisions relating to other countries. Over time, it will become clear what regulatory measures are within the realm of acceptable, and what regulatory measures are off limits. The shared blackboard of best practices would begin to emerge. This will lead national regulators to avoid wasting time on measures that clearly have no chance of succeeding, and concentrating on measures, and variants thereof, that have worked in other countries. The development of international best practices and shared knowledge about what measures work, and what measures don't, are key benefits flowing from the methodology.

(d) Criticism 4: Do not try to quantify the unquantifiable

Effects on fundamental rights cannot be reduced to a simple formula or scoring mechanism. As we have seen in Chapters 3 and 6, converting effects on fundamental rights into measurable units is fraught with difficulty. This is true, but the problem is not insoluble. A recent research project funded by the European Commission attempts to attribute a score to fundamental rights intrusions showing that a scoring mechanism is not completely crazy. The SURVEILLE project, which involves nine research institutions in Europe, resulted in the creation of a standard methodology against which police surveillance techniques can be assessed (Scheinen and Sorell, 2015). The project is similar to the approach I propose here in that it seeks to develop a rational method for comparing different regulatory measures in light of their effect on fundamental rights. The project is different because it only considers police surveillance measures. Also, the SURVEILLE project does not incorporate into the equation factors such as institutional alternatives and the effects on the internet ecosystem.

The SURVEILLE project's deliverables include a scoring methodology that relies heavily on the work of Robert Alexy, described in Chapter 3. The methodology used in the SURVEILLE project first involves attributing a technology assessment usability score from 1 to 10 to the relevant surveillance technology. This assessment score includes the risk of error created by the

technology, the level of privacy protection already built into the technology and its cost. The technology assessment score also takes into account the efficiency of the surveillance technology in achieving the desired policy objective (which is to catch criminals and prevent crime). The project then proposes for each type of surveillance technology a fundamental rights intrusion score from 1 to 16 that assesses the degree of intrusion into fundamental rights. These two scores are then compared to provide an initial indication of whether the surveillance technology presents an acceptable benefit compared to the level of intrusion into fundamental rights. This initial assessment would then be evaluated based on a qualitative ethical valuation yielding a green light, a yellow light, or a red light depending on the level of acceptability of the measure. A green light would mean that the measure is acceptable, a yellow light means that additional work is needed in order to make the technology more acceptable for its proposed surveillance purpose, and a red light means that the form of surveillance is unacceptable and must be rejected.

Figure 6: Summary of the European Commission's "SURVEILLE" project (Source: Surveille website surveille.eui.eu

The SURVEILLE methodology has shortcomings (for example, it does not incorporate institutional alternatives), but using a standard methodology, even imperfect, is better than having no standard methodology at all. A methodology (even imperfect) provides an objective measurement tool against which proposals can be assessed. The SURVEILLE project shows that the European Commission is interested in developing evaluation tools for regulatory measures that affect fundamental rights. The project also shows the need to simplify methodologies in order to make them operational. The SURVEILLE project does a good job doing this. The methodology proposed in my thesis currently is too complex to be easily implemented by government agencies. Additional work is needed to simplify the methodology and make it more user-friendly.

The SURVEILLE project does not attempt to make any connection between its methodology and the regulatory impact assessments that governments are supposed to conduct before adopting new regulatory measures. The SURVEILLE research team did not appear to consider "better regulation" methodology in their work, which is unfortunate. As Chapter 5 of this thesis demonstrated, better regulation methodology applies to all proposed government measures, and police surveillance measures would fall within this scope.

The SURVEILLE project also did not take into account the institutional options that may accompany police surveillance technology. A surveillance measure that is ordered by police authorities themselves would have a different impact on fundamental rights than a surveillance measure ordered by an independent court. The duration of the surveillance measure, and mechanisms to ensure that the measure is lifted as soon as it is longer necessary, are also relevant in assessing the level of impact on fundamental rights. Also, the SURVEILLE methodology does not call for a peer review mechanism to ensure that the methodology is applied correctly, and that the effects of conflicts of interest are minimized.

3. QUANTIFYING THE UNQUANTIFIABLE

Applying a regulatory impact assessment, including a cost-benefit analysis, will lead to an improvement in how regulations on internet content are adopted and applied. However, further work is needed in coming to grips with "quantifying the unquantifiable". A cost-benefit analysis works best when all costs and benefits can be transformed into monetary equivalents. In the United States, drafters of cost-benefit analyses have developed ways to transform risks to human lives into monetary equivalents, as well as risks (and benefits) to the environment. If the benefit or cost associated with modifying the risk of death can be quantified, there would seem to be no reason why changes in the enjoyment of other fundamental rights cannot also be quantified. To date, research has focused on the monetary value of various privacy rights (Acquisti 2010, Thierer 2013). However, I am not aware of similar research focusing on the monetary value of freedom to access information.

One approach that has not yet been used to my knowledge would be to take the statistical values of human lives developed in the course of impact assessments in the United States, and attempt

to extrapolate how an interference with a fundamental right such as privacy would compare with the statistical value of a human life. Viscusi and Aldy (2003) estimate the value of a statistical life in the United States at $7 million. The European Commission recommends a value of €1 million (OECD, 2009). It may be possible for researchers to approach this question by looking first at fundamental rights that come close to the value of life itself, such as the right not to be tortured, or the right not to be imprisoned. Four years in prison might have a value roughly equivalent to four years of loss of life. Torture might have a value close to that of the loss of an entire life (or perhaps more?). Researchers would then try to work backwards to address other fundamental rights such as freedom of expression and privacy, each of which would presumably have a lower relative value. At the end, it may be possible to convert losses of certain fundamental rights into a number of life years lost, which in turn would allow us to have a rough monetary value for various fundamental right restrictions.

The monetized value of fundamental rights would be used solely in the cost-benefit analysis to help identify regulatory solutions that are optimal in an economic sense. The outcome of the cost-benefit analysis would still be subject to constraints such as those described in Chapter 6, Section 4.7. For example, even if a cost-benefit analysis were to show a given proposal as optimal, the relevant proposal could be rejected if its effect on privacy or freedom of expression was "extremely high." These constraints would ensure that cost-benefit analyses remain subject to an ethical filter (Nussbaum, 2000). Likewise, the monetized value of fundamental rights would never replace the role of courts, whose job it is to ensure that measures adopted by regulators do not unduly restrict fundamental rights. Courts would naturally not be bound by the statistical value of a fundamental right used in the cost-benefit analysis. The sole utility of the monetized value would be to help analyze regulatory options in a uniform manner.

Another direction for research would be to draw parallels with the evaluation of environmental costs and benefits. Environmental impact assessments have been conducted for decades, and considerable effort has gone into quantifying environmental costs and benefits. If we consider the internet ecosystem as similar to an environmental ecosystem, the study of environmental impact assessments might help determine how indirect impacts on the internet ecosystem or other hard-to-quantify costs should be measured. Scholars have examined how difficult-to-quantify factors such as the beauty of landscape might be measured in the context of environmental impact assessments (DEFRA, 2007). Some scholars have proposed mathematical tools, including "fuzzy logic," to help better take account of uncertainty and hard-to-quantify impacts (Shepard, 2005). Some of these methods may be transposable to the evaluation of harms to fundamental rights and/or the internet ecosystem.

REFERENCES

Ackerman, F. and L Heinzerling (2002), "Pricing the Priceless: Cost-Benefit Analysis of Environmental Protection", *150 U. of Penn. L. Rev. 1553.*

Acquisti, A. (2010), "The Economics of Personal Data and the Economics of Privacy," *OECD Background Paper n° 3, Joint WPISP-WPIE Roundtable.*

Acquisti, A., L. John and G. Loewenstein (2009), "What is Privacy Worth", *Workshop on Information Systems and Economics (WISE).*

Ahlert, C., C. Marsden and C. Yung (2004), "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation" *http:/pcmlp.socleg.ox.ac.uk/text/liberty.pdf.*

Akerlof, G. (1970), "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism", *84 Quarterly J. of Econ. 488.*

Alexandre, D., Ph. Coen, J.-M. Dreyfus (2016), "Pour en finir avec Mein Kampf – Et combattre la haine sur Internet", *Le Bord de l'Eau***.**

Alexy, R. (2014), "Constitutional Rights and Proportionality", *22 Revus [Online].*

Ambrose, M. L. (2013), "Speaking of Forgetting: Analysis of Possible Non-EU Responses to the Right to Be Forgotten and Speech Exception", *TPRC Conferences, TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy. Available at SSRN: http://ssrn.com/abstract=2238602 or http://dx.doi.org/10.2139/ssrn.2238602.*

APEC (Asia-Pacific Economic Cooperation) (2013), "Promoting cooperation on data transfer systems between Europe and the Asia-Pacific" *http://www.apec.org/Press/News-Releases/2013/0306_data.aspx*

ARCEP (2012), "Report to Parliament and the Government on Net Neutrality", *http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutrality-sept2012-ENG.pdf.*

Autorité de la Concurrence and Competition and Markets Authority (2014), "The Economics of Open and Closed Ecosystems," 16 December;

Baker, E.C. (2002), "Media, Markets and Democracy", *Cambridge University Press.*

Baldwin, R. (2010), "Better Regulation: the Search and the Struggle", *in R. Baldwin, M. Cave and M. Lodge (ed.) Oxford Handbook of Regulation, p. 270.*

Balleisen, E. and M. Eisner (2009), "The Promise and Pitfalls of Co-Regulation: How Governments Can Draw on Private Governance for Public Purpose", *in D. Mass and J. Cisternino (ed.), "New Perspectives on Regulation", The Tobin Project, p. 129.*

Bamberger, K. (2006), "Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State", *56 Duke L. J. 377.*

Bamberger, K. and D. Mulligan (2011), "Privacy on the Books and on the Ground," *63 Stan. L. Rev. 247.*

Barron, A. (2011), "Graduated response à l'anglaise : online copyright infringement and the Digital Economy Act 2010", *3 J. of Media L. 305.*

Barzel, Y. (1989), "Economic Analysis of Property Rights", *Cambridge U. Press.*

Beales, H. (2003), "The FTC's Use of Unfairness Authority: its Rise, Fall, and Resurrection," *Federal Trade Commission Marketing and Public Policy Conference, 30 May, available at* http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection

Beales, H. and T. Muris (2008), "Choice or Consequences: Protecting Privacy in Commercial Information", *75 U. of Chicago L. Rev. 109.*

Benkler, Y. (1999), "Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain", *74 N.Y.U. L. Rev. 354.*

Benkler, Y. (2006), "The Wealth of Networks", *Yale University Press.*

Bernstein, L. (1992), "Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry", *21 J. of Legal Studies 115.*

Blind, K. (2012), "The Impact of Regulation on Innovation", *Nesta Working Paper No. 12/02.*

Bomsel, O. and H. Ranaivoson (2009), "Decreasing copyright enforcement costs: the scope of a graduated response", *6 R. of Econ. Research on Copyright Issues 3*.

Borgesius F. Z. (2013), "Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics?", *Institute for Information Law Research Paper 2013-02.*

Boyer, M. (2012), "The Economics of Fair Use/Dealing: Copyright Protection in a Fair and Efficient Way", *9 Rev. of Econ. Research on Copyright Issues 3.*

Bracha, O. and F. Pasquale (2008), "Federal Search Commission? Access, Fairness, and Accountability on the Law of Search", *93 Cornell L. Rev. 1149.*

Brandimante, L., A. Acquisiti and G. Loewenstein (2012), "Misplaced Confidences: Privacy and the Control Paradox", *4 Social, Psychological and Personality Science 340*.

Breton, A. and R. Wintrobe (1992), "Freedom of speech vs. efficient regulation in markets for ideas", *17 J. of Econ. Behavior and Organization 217.*

Breyer, S. (1970), "The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs", *84 Harvard L. Rev. 281.*

Breyer, S. (1982), "Regulation and its Reform", *Harvard University Press.*

Bridy, A. (2010), "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement", *89 Oregon L. Rev. 81.*

Bridy, A. (2011), "Is Online Copyright Enforcement Scalable?", *13 Vanderbilt J. of Entertainment and Tech. L. 695.*

Brousseau, E. (2006), "Multi-level governance of the digital space: does a "second rank" institutional framework exist?", *in E. Brousseau and N. Curien (ed.), "Internet and Digital Economics", Cambridge University Press.*

Callanan, C., M. Gercke, E. De Marco and H. Driez-Ziekenheiner (2009), "Internet Blocking – Balancing Cybercrime Responses in Democratic Societies", *http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf*

Carroll, M. (2007), "Fixing Fair Use", *85 North Carolina L. Rev. 1087.*

Cecot, C., R. Hahn, A. Renda, L. Schrefler (2007), "An Evaluation of the Quality of Impact Assessment in the European Union with Lessons for the U.S. and the EU", *Working Paper, AEI-Brookings Joint Center for Regulatory Studies, December.*

CJEU (2011), "Scarlet Extended v SABAM", *C-70/10*

Coase, R.H. (1959), "The Federal Communications Commission", *2 J. of L. and Econ. 1.*

Coase, R.H. (1960), "The Problem of Social Cost", *3 J. of L. and Econ. 1.*

Coase, R.H. (1974), "The Market for Goods and the Market for Ideas", *64 American Econ. Rev. 384.*

Coase, R.H. (1977), "Advertising and Free Speech", *6 J. of Leg. Studies 1.*

Collin, P. and N. Colin (2013), "Task Force on Taxation of the Digital Economy", *Report to the Minister for the Economy and Finance, the Minister for Industrial Recovery, the Minister Delgate for the Budget and the Minister Delegate for Small and Medium-sized Enterprises, Innovation and the Digital Economy.*

Conseil d'Etat (2016), "Etude Annuelle: Simplification et qualité du droit", *La Documentation française, 26 septembre 2016.*

Crawford, S. (2005), "Shortness of Vision: Regulatory Ambition in the Digital Age", *Benjamin N. Cardozo School of Law, Jacob Burns Institute for Advanced Legal Studies, Working Paper n° 102.*

Croley, S. (1998), "Theories of Regulation: Incorporating the Administrative Process", *98 Columbia L. Rev. 1.*

Curien, N. (2011), "Innovation and Regulation serving the digital Revolution," *The Journal of Regulation, I-1.32, pp. 572-578.*

Curien, N. and W. Maxwell (2010), "Net Neutrality in Europe: An Economic and Legal Analysis", *Concurrences, Review of competition laws, N°4.*

Curien, N. and W. Maxwell (2011), "La neutralité d'Internet", *Editions La Découverte.*

DeMarzo, P., M. Fishman and K. Hagerty (2005), "Self Regulation and Government Oversight", *72 Rev. of Econ. Studies 687.*

De Vries, S. (2013), "Balancing of Fundamental Rights with Economic Freedoms According to the European Court of Justice", *9 Utrecht L. Rev. 169.*

DEFRA Department for Environment, Food and Rural Affairs – United Kingdom (2007), "An introductory guide to valuing ecosystem services," *Defra Publications.*

Dixit, A. (2009), "Governance, Institutions and Economic Activity", *99 American Econ. Rev. 5.*

Ehrlich, I. and R. Posner (1974), "An Economic Analysis of Legal Rulemaking", *3 J. of Leg. Studies 257.*

Electronic Frontier Foundation (2013), "Unintended Consequences: Fifteen Years under the DMCA", *EFF White Paper.*

Elkin-Koren, N. (2005), "Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic", *9 Legislation and Public Policy 15.*

European Advertising Standards Alliance-EASA website *http://www.easa-alliance.org/page.aspx/166 (accessed April 24, 2016).*

European Commission (2010), "Smart Regulation in the European Union, Communication from the Commision", *COM(2010) 543 final, Oct. 8.*

European Commission (2011), "Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments", ***Commission Staff Working Paper, SEC(2011) 567 final, May 6.***

European Commission (2015), "Better Regulation Guidelines", *Commission Staff Working Paper, SWD(2015) 111 final, May 19.*

European Network and Information Security Agency (ENISA) (2012), "Study on monetizing privacy – an economic model for pricing personal information," *27 February.*

European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe (2014), "*Handbook on European data protection legislation," Publications Office of the European Union.*

Farano, B.M. (2012), "Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches", *Transatlantic Technology Law Forum (TTLF) Working Paper n° 14.*

Federal Trade Commission (FTC) (1980), "FTC Policy Statement on Unfairness," *17 December, available at* http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

Fowler, M.S. and D.L. Brenner (1982), "A Marketplace Approach to Broadcast Regulation", *60 Tex. L. Rev. 207.*

Foxman, A. and C. Wolf (2013), "Viral Hate – Containing its Spread on the Internet", *Palgrave Macmillan.*

Fraas, A. and R. Lutter (2011), "On the Economic Analysis of Regulations at Independent Regulatory Commissions", *Resources for the Future Discussion Paper 11-16*.

Garfield, A. (1998), "Promises of Silence: Contract Law and Freedom of Speech", *83 Cornell L. Rev. 261*.

Geisfeld, M. (2009), "Efficiency, Fairness, and the Economic Analysis of Tort Law," *N.Y.U. School of Law, Law & Economics Research Paper n° 09-21.*

Goldfarb, A. and C. Tucker (2011), "Privacy and Innovation," *National Bureau of Economic Research Working Paper 17124, June.*

Graham, J.D. (2008), "Saving Lives through Administrative Law and Economics", *157 U. Penn. L. Rev. 395.*

Grazia Porcedda, M. (2013), "SURVEILLE Deliverable 2.4 – Paper establishing a classification of technologies on the basis of their intrusiveness into fundamental rights", *European Commission Seventh Framework Programme FP7–SEC-2011-284725*.

Greenstone, M. (2009), "Toward a Culture of Persistent Regulatory Experimentation and Evaluation", *in D. Moss and J. Cisterino (ed.), "New Perspectives on Regulation", The Tobin Project, p. 113.*

Haber, E. (2010), "The French Revolution 2.0: Copyright and the Three Strikes Policy", *2 J. of Sports & Entertainment L. 297.*

Hahn, R.W. (2004), "The Economic Analysis of Regulation: A response to the Critics", *71 U. of Chicago L. Rev. 1021.*

Hahn, R., J. Burnett, Y-H Chan, E. Mader, P. Moyle (2000), "Assessing the Quality of Regulatory Impact Analyses", *Working Paper 00-01, AEI-Brookings Joint Center for Regulatory Studies, January*.

Hahn, R.W. and R.E. Litan (2005), "Counting Regulatory Benefits and Costs: Lessons for the U.S. and Europe", *8 J. of International Econ. L. 473.*

Hahn, R. W. and C.R. Sunstein (2002), "A New Executive Order for Improving Federal Regulation? Deeper and Wider Cost-Benefit Analysis", *U Chicago Law & Economics, Olin Working Paper No. 150.*

Hahn, R.W. and P.C. Tetlock (2008), "Has Economic Analysis Improved Regulatory Decisions?", *22 J. of Economic Perspectives 67.*

Halftech, G. (2008), "Legislative Threats", *61 Stanford L. Rev. 629.*

Hamdani, A. (2003), "Gatekeeper Liability", *77 Southern Cal. L. Rev. 53.*

Hancher, L., P. Larouche and S. Lavrijssen (2003), "Principles of Good Market Governance", *4 J. of Network Industries 355.*

Hatzis, A. N. (2008) "An Offer You Cannot Negotiate: Some Thoughts on the Economics of Standard Form Consumer Contracts", *in Hugh Collins (ed.) "Standard Contract Terms in Europe: A Basis for and a Challenge to European Contract Law" (Kluwer 2008).*

Helm, D. (2006), "Regulatory Reform, Capture, and the Regulatory Burden", *22 Oxford Rev. of Econ. Policy 169.*

Hickman, T. (2008), "The Substance and Structure of Proportionality", *Public Law 694.*

Holmes, S. and C.R. Sunstein (2013), "The Cost of Rights – Why Liberty Depends on Taxes", *W.W. Norton & Company.*

Hugenholtz, B. and M. Senftleben (2011), "Fair Use in Europe: In search of flexibilities", *IVR Working Paper, Universiteit Amsterdam.*

Impact Assessment Board (IAB) (2014), "2014 Activity Assessment", *http://ec.europa.eu/smart-regulation/impact/key_docs/docs/iab_stats_2014_en.pdf* .

Johnson, D.R. and D. Post (1996), "Law and Borders – The Rise of Law in Cyberspace", *48 Stan. L. Rev. 1367.*

Kahneman, D. (2003), "Maps of bounded rationality: psychology for behavioral economics", *93 American Econ. Rev. 1449.*

Kaplow, L. (1992), "Rules versus Standards: An Economic Analysis," *42 Duke L. J. 557.*

Kaplow, L. and S. Shavell (2006), "Fairness versus Welfare," *Harvard University Press.*

Katz, M. (2000), "Regulation: The Next 100 Years", *in "Six Degrees of Competition: Correlating Regulation with the Telecommunications Marketplace", The Aspen Institute.*

Kreimer, S. (2006), "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link", *155 Penn. L. Rev. 11.*

Landes, W. and R. Posner (1987), "The Economic Structure of Tort Law", *Harvard University Press.*

Larusson, H.K. (2009), "Uncertainty in the Scope of Copyright", *European Intellectual Property Rev. 124.*

Laudon, K. (1996), "Markets and Privacy", *39 Communications of the ACM 92, Association for Computing Machinery, September.*

Lemley, M.A. and A. Reese (2004), "Reducing Digital Copyright Infringement Without Restricting Innovation", *56 Stanford L. Rev. 1345.*

Lemley, M.A. and E. Volokh (1998), "Freedom of Speech and Injunctions in Intellectual Property Cases", *48 Duke L. J. 147.*

Lerner, A.V. (2014), "The Role of Big Data in Online Platform Competition," *Working Paper 26 August, SSRN Abstract 2482780;*

Lescure, P. (2013), "Mission Acte II de l'exception culturelle", *French Ministry of Culture.*

Lessig, L. (1999), "Code and Other Laws of Cyberspace", *New York, Basic Books*.

Lessig, L. and P. Resnick (1999), "Zoning Speech on the Internet: A Legal and Technical Model", *Harvard Law School, Berkman Center for Internet and Society, Research Publication no. 1999-06.*

Lichtman, D. and W. Landes (2003), "Indirect Liability for Copyright Infringement: An Economic Perspective", *16 Harvard J. of L. & Technology 395.*

Lichtman, D. and E. Posner (2006), "Holding Internet Service Providers Accountable", *14 S. Ct. Econ. Rev. 221.*

Liebowitz, S. (2011), "Is Efficient Copyright a Reasonable Goal?", *79 George Wash. L. Rev.*

Listokin, Y. (2008), "Learning Through Policy Variation", *Faculty Scholarship Series, Paper 557, http://digitalcommons.law.yale.edu/fss_papers/557.*

Liu, J. (2004), "Regulatory Copyright", *83 North Carolina L. Rev. 87.*

MacCarthy, M. (2010), "What Payment Intermediaries Are Doing About Online Liability and Why It Matters", *25 Berkeley Tech. L. J. 1039.*

Mann, R. and S. Belzley (2005), "The Promise of Internet Intermediary Liability", *47 Wm & Mary L. Rev. 239.*

Marsden, C. (2011), "Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace", *Cambridge University Press.*

Maxwell, W. (2014), "Global Privacy Governance: A Comparison of Regulatory Models in the US and Europe, and the Emergence of Accountability as a Global Norm," *in C. Dartiguepeyrou (ed.), "The Futures of Privacy," Fondation Telecom.*

Maxwell, W. and C. Coslin (2014), "L'efficacité à l'étranger des décisions françaises en matière de communication : le cas des Etats -Unis et du Premier Amendement" *Légicom n° 52.*

Maxwell, W. (2015), "Principles-based regulation of personal data: the case of 'fair processing'", *5 Int'l Data Privacy L. 205.*

Mazzone, J. (2009), "Administering Fair Use", *5 Wm. & Mary L. Rev.395.*

Mialon, H. and S. Mialon (2008), "The Effects of the Fourth Amendment: An Economic Analysis", *24 J. of L., Econ., and Organization 22.*

Mialon, H. and P. H. Rubin (2007), "The Economics of the Bill of Rights", *Emory Law and Economics Research Paper No. 07-15.*

Monaghan, H.P. (1970), "First Amendment 'Due Process'", *83 Harvard L. Rev. 518.*

Mooney, P., S. Samanta and A. Zadeh (2010), "Napster and its Effects on the Music Industry: An Empirical Analysis", *6 J. of Social Sciences 303.*

Morrall, J.F. III (1986), "A Review of the Record", *10 Regulation 25*.

Nissenbaum H. (2004), "Privacy as Contextual Integrity", *79 Wash. L. Rev. 101.*

Noam, E.M. (2006), "TV Regulation Will Become Telecom Regulation", *Financial Times,* October 24.

North, D. (1990), "Institutions, Institutional Change and Economic Performance", *Cambridge U. Press*.

NTIA (National Telecommunications & Information Administration) (2013), "Privacy Multistakeholder Process: Mobile Application Transparency", *http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency*

Nussbaum, M. (2000), "The Costs of Tragedy: Some Moral Limits of Cost-Benefit Analysis", *29 J. of L. Studies 1005*.

Oberholzer-Gee, F. and K. Strumpf (2007), "The Effect of File Sharing on Record Sales: An Empirical Analysis", *115 J. of Political Economy 1.*

OECD (2004), "Regulatory Performance: Ex-Post Evaluation of Regulatory Tools and Institutions" *GOV/PGC/REG(2004)6, 15 October.*

OECD (2009), "Regulatory Impact Analysis, A Tool for Policy Coherence", *OECD Publishing.*

OECD (2010), "The Economic and Social Role of Internet Intermediaries", *OECD Publishing.*

OECD (2011a), "The Role of Internet Intermediaries in Advancing Public Policy Objectives", *OECD Publishing.*

OECD (2011b), "Recommendation of the OECD Council on Principles for Internet Policy Making", *OECD Publishing, December.*

OECD (2012), "Recommendation of the Council on Regulatory Policy and Governance", *OECD Publishing, March.*

OECD (2016), "The Economic and Social Benefits of Internet Openness", *OECD, DSTI/ICCP(2015)17/Final, June 2, 2016.*

Ogus, A. (1998), "Corrective Taxes and Financial Impositions as Regulatory Instruments", *61 Modern L. Rev. 767.*

Parchomowsky, G. and P. Weiser (2011), "Beyond Fair Use", *96 Cornell L. Rev. 91.*

Peltzman, S. (1976), "Toward a More General Theory of Regulation", *19 J. of L. and Econ. 211.*

Pelkmans, J. and A. Renda (2014), "Does EU regulation hinder or stimulate innovation?", *CEPS Special Report n° 96.*

Pildes, R.H. and C.R. Sunstein (1995), "Reinventing the Regulatory State", *62 U. of Chicago L. Rev. 1.*

Portuese, A. (2013), "Principle of Proportionality as Principle of Economic Efficiency", *19 European L. J. 612.*

Posner, R.A. (1978), "An Economic Theory of Privacy", *Regulation, May/June.*

Posner, R.A. (1981), "The Economics of Privacy", *75 The American Econ. Rev. 405.*

Posner, R.A. (2000), "Cost-Benefit Analysis: Definition, Justification, and Comment on Conference Papers", *29 J. of Legal Studies 1153.*

Posner, E. (2002), "Using Net Benefit Accounts to Discipline Agencies: A Thought Experiment" *150 U. of Penn. L. Rev. 1473.*

Posner, R.A. (2005), "Intellectual Property: The Law and Economics Approach", *19 J. of Econ. Perspectives 57.*

Posner, R.A. (2005), "Intellectual Property: The Law and Economics Approach", *19 J. of Econ. Perspectives 57.*

Posner, R.A. (2008), "Privacy, Surveillance, and Law", *75 U. of Chicago L. R. 245.*

Posner, R.A. (2011), "Economic Analysis of Law", *Aspen Casebook Series, 8th Edition*.

Post, R.C. (1996), "Subsidized Speech", *106 Yale L. J. 151.*

Radaelli, C.M. and F de Francesco (2010), "Regulatory Impact Assessment", *in R. Baldwin, M. Cave and M. Lodge (ed.) "The Oxford Handbook of Regulation", p. 279, Oxford.*

Ranchordas, S. (2013), "The Whys and Woes of Experimental Legislation", *1 Theory and Practice of Legislation 415-440.*

Ranchordas, S. (2015a), "Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation" *55 Jurimetrics, Vol. 55, No. 2, Available at SSRN: http://ssrn.com/abstract=2544291*

Ranchordas, S. (2015b), "Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy", *16 Minn. J. L. Sci. & Tech. 1.*

Reidenberg, J.R. (1998), "Lex Informatica: The Formulation of Information Policy Rules through Technology", *76 Texas L. Rev. 553.*

Renda, A., L. Schrefler, G. Luchetta, and R. Zavatta (2013), "Assessing the Costs and Benefits of Regulation", *Study for the European Commission, Secretariat General, Final Report, December.*

Rivers, J. (2006), "Proportionality and Variable Intensity of Review", *64 Cambridge L. J. 174.*

Rosen, J. (2012), "The Right to be Forgotten", *64 Stan. L. Rev. Online 88.*

Rosen, J. (2013), "The Delete Squad", *The New Republic, 29 April.*

Sauter, W. (2013), "Proportionality in EU law: a balancing act?", *TILEC Discussion Paper DP 2013-0003.*

Scheinin M. and T. Sorell (2015), "SURVEILLE Deliverable D4.10 – Synthesis report from WP4 merging the ethics and law analysis and discussing their outcomes", *European Commission, Seventh Framework Programme FP7– SEC 2011 284725.*

Schroeder, C.H. (1986), "Rights Against Risks", *86 Columbia L. Rev. 495.*

Schruers, M. (2002), "The History and Economics of ISP Liability for Third Party Content", *88 Va. L. Rev. 205.*

Schultz, T. (2008), "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", *19 European J. of Int'l L. 799.*

Ségur, Ph. (2012), "La Dimension Historique des Libertés et Droits Fondamentaux", *in R. Cabrillac, M.-A. Frson-Roche & Th. Revet, "Libertés et Droits Fondamentaux", Dalloz, 18th edition.*

Seltzer, W. (2010), "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment", *24 Harvard J. L. & Technology 171.*

Shavell, S. (1984), "Liability for Harm versus Regulation of Safety", *13 J. of Legal Studies 357.*

Shavell, S. (1993), "The Optimal Structure of Law Enforcement", *36 J. of L. and Econ. 255.*

Shavell, S. (2004), "Foundations of Economic Analysis of Law", *The Belknap Press of Harvard University Press.*

Shelanski, H. (2013), "Information, Innovation, and Competition Policy for the Internet", *161 U. Penn L. Rev. 1663.*

Shepard, R. B. (2005), "Quantifying Environnmental Impact Assessments Using Fuzzy Logic", *Springer.*

Siebens, C. (2011), "Divergent Approaches to File-Sharing Enforcement in the United States and Japan", *52 Virginia J. of Int. L. 155.*

Singh, A. (2011), "Agency Regulation in Copyright Law: Rulemaking under the DMCA and its broader implications", *26 Berkeley Technology L. J. 527.*

Sieradzki D.L. and W. Maxwell (2008), "The FCC's network neutrality ruling in the Comcast case: towards a consensus with Europe?", *Communications & Strategies, N° 72, p. 73*.

Slawson, D.W. (1971), "Standard Form Contracts and Democratic Control of Lawmaking Power", *84 Harvard L. Rev. 529.*

Solove, D. and W. Hartzog (2014), "The FTC and the New Common Law of Privacy," *114 Col. L. Rev. 583.*

Stigler, G.J. (1971), "The theory of economic regulation", *2 Bell J. of Economics and Management Science 3.*

Stigler, G.J. (1980), "An Introduction to Privacy in Economics and Politics", *9 J. of Legal Studies 623.*

Sunstein, C.R. (1990), "Paradoxes of the Regulatory State", *57 U. of Chicago L. Rev. 407.*

Sunstein, C.R. (1996), "Congress, Constitutional Moments, and the Cost-Benefit State", *48 Stanford L. Rev. 247.*

Sunstein, C.R. (1996), "On the Expressive Function of Law", *144 U. of Penn. L. Rev. 2021.*

Sunstein, C.R. (2000), "Cognition and Cost-Benefit Analysis", *29 J. of Legal Studies 1059.*

Sunstein, C.R. (2002), "Risk and Reason: Safety, Law and the Environment," *Cambridge University Press.*

Sunstein, C.R. (2014), "Simpler – The Future of Government", *Simon & Schuster.*

Tene, O. and J. Polonetsky (2013), "A Theory of Creepy: Technology, Privacy and Shifting Social Norms", *16 Yale J. L. & Tech. 59.*

Thaler, R. and C.R. Sunstein (2008), "Nudge – Improving Decisions about Health, Wealth and Happiness", *Yale University Press.*

Thierer, A. (2013), "A Framework for Benefit-Cost Analysis in Digital Privacy Debates," *20 Geo. Mason L. Rev. 1055.*

Tranberg, C.B. (2011), "Proportionality and data protection in the case law of the European Court of Justice", *1 Inter. Data Privacy L. 239.*

United Nations (2011), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", *Human Rights Council, Frank La Rue, May 16, A/HRC/17/27.*

Van Eijk, N. and T. van Engers (2011), "Duties of care on the Internet", *Paper presented at the Telecommunications Policy research Conference (TPRC), September 23-24, 2011.*

Varian, H. (1996), "Economic Aspects of Personal Privacy", *U. of Cal. Berkeley Research Paper, December 6.*

Varian, H. R. (2010), "Intermediate Microeconomics, A Modern Approach", *W.W. Norton & Co., New York.*

Viscusi, W.K. and J. Aldy (2003), "The Value of a Statistical Life: a Critical Review of Market Estimates Throughout the World", *AEI-Brookings research Paper 03-2.*

Viscusi, K. W., J. Harrington Jr., and J. M. Vernon (2005), "Economics of regulation and Antitrust", 4th Edition, *The MIT Press.*

Waldron, J. (2012), "The Harm in Hate Speech", *Harvard U. Press.*

Wan, C.W. (2010), "Three strikes law: a least cost solution to rampant online piracy", *5 J. of Intellectual Prop. L. & Practice 232.*

Warren, S. and W. Brandeis (1890), "The Right to Privacy", *4 Harv. L. Rev. 193.*

Waz, J. and P. J. Weiser (2012), "Internet Governance: the Role of Multistakeholder Organizations", *10 J. on Telecom & High Tech. L.*

Weiser, P.J. (2009), "The Future of Internet Regulation", *43 U. of Cal. Davis L. Rev. 529.*

White House (2003), Office of Management and Budget Circular A-4 on Regulatory Analysis, *September 17.*

White House (2012), "Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy," *https://www.whitehouse.gov/sites/default/files/privacy-final.pdf*

White House (2013), "Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies", *http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.*

Whitt, R.S. (2009), "Adaptive Policy-Making: Evolving and Applying Emergent Solutions for U.S. Communications Policy", *61 Federal Communications L. J. 483***.**

Whitman, J.Q. (2004), "The Two Western Cultures of Privacy: Dignity Versus Liberty", *113 Yale L. J. 1151.*

Wiener, J.B. (2006), "Better Regulation in Europe", *59 Current Legal Problems 447.*

WIK Consult, YouGov, Deloitte (2015), "The Value of Net Neutrality to European Customers", *Report commissioned by the Body of European Regulators of Electronic Communications, April 2015.*

Wu, T. (2003), "Network neutrality, broadband discrimination", *J. of Telecomm. and High Tech. L. 141.*

Wu, Tim (2012), "When Censorship Makes Sense: How YouTube Should Police Hate Speech", *New Republic, September 18, 2012. (proposes community panels to judge cases of takedown for hate speech – like Wikipedia)*

Yoo, C.S. (2005), "Beyond network neutrality", *19 Harvard J. of L. & Tech. 1.*

Yoo, C.S. (2013), "Modularity Theory and Internet Policy", University of Pennsylvania Law School, *Institute for Law and Economics, ILE Research Paper n° 13-15.*

Yu, P.K. (2010), "The Graduated Response", *62 Florida L. Rev. 1373.*

Zittrain, J. (2003), "Internet Points of Control", *43 Boston College L. Rev. 1.*

Zittrain, J. (2008), "The Future of the Internet, and How to Stop It," *Yale University Press, New Haven.*

Le condensé du manuscrit en français

Chapitre 1 - Introduction

La thèse examine les problèmes économiques liés à la régulation des contenus illicites sur Internet. La thèse propose d'appliquer une analyse coûts/bénéfices à chaque fois que l'on veut imposer à un intermédiaire technique une mesure destinée à lutter contre des contenus illicites. Dans certains cas, imposer une mesure de filtrage peut se révéler nécessaire. Mais la mesure peut se révéler inefficace car les moyens de contournement sont nombreux. La mesure peut également générer des coûts qui n'étaient pas pris en compte lors de l'élaboration de la mesure. Ces coûts cachés peuvent comprendre des impacts préjudiciables sur la liberté d'expression ou sur d'autres droits fondamentaux, ainsi que des impacts préjudiciables sur l'écosystème de l'Internet.

Dans d'autres domaines, l'utilisation d'études d'impact et d'analyses coûts/bénéfices est fréquente. Les Etats-Unis, l'OCDE et la Commission Européenne sont unanimes sur la nécessité d'effectuer systématiquement des études d'impact qui prennent en considération l'ensemble des coûts et des bénéfices générés par la mesure de régulation envisagée. Cependant, pour des mesures visant à limiter l'accès à des contenus illicites sur Internet, les études d'impact prennent rarement en considération les coûts indirects générés par la mesure, y compris l'impact sur les droits fondamentaux. Il en résulte une cacophonie de mesures destinées à traiter différents types de contenu sur Internet, sans que l'on puisse dégager une ligne conductrice.

L'idée de cette thèse découle de mes travaux en matière de régulation des communications électroniques en Europe. Dans ce domaine, les régulateurs sont contraints de conduire une analyse de marché, identifier les défaillances du marché nécessitant une intervention réglementaire, examiner plusieurs options pour traiter les défaillances du marché et de peser les coûts et bénéfices de chaque option. Ensuite, l'analyse du régulateur est revue par un comité créé au sein de la Commission Européenne pour s'assurer de la qualité de l'analyse. Les régulateurs sont également obligés de revoir périodiquement les mesures réglementaires en vigueur et révoquer les mesures qui ne sont plus utiles. Cette approche dans le domaine des communications électroniques est parfaitement cohérente avec les principes de "bonne régulation" issus des recommandations de l'OCDE et de la Commission Européenne. Ce type de rigueur n'est pas appliqué, cependant, aux mesures de régulation visant les intermédiaires techniques de l'Internet.

La régulation des contenus illicites sur Internet est autrement plus complexe que la régulation des réseaux de communications électroniques. La régulation des communications électroniques vise

à augmenter la concurrence ainsi qu'à favoriser l'investissement dans les nouveaux réseaux fixes et mobiles. La régulation des contenus sur Internet vise à limiter les effets dommageables de certains types de contenus qui deviennent facilement accessibles grâce à l'Internet. Mais les effets dommageables d'un certain type de contenus sont difficiles à mesurer de manière quantitative. Bien souvent, ces politiques de contenu reflètent des valeurs sociétales qui peuvent difficilement être insérées dans une analyse coûts/bénéfices classique. Même si tout le monde est d'accord sur la nécessité de bloquer certains types de contenus nuisibles, il peut exister une grande divergence de points de vue sur la signification du terme "bloquer". L'Internet est conçu pour éviter des points de blocage. Ainsi des mesures destinées à limiter l'accès à certains contenus peuvent souvent être contournées. Un blocage vraiment efficace pourrait nécessiter la mise en place d'un filtrage systématique de tout le trafic entrant et sortant d'un pays, ce qui reviendrait à détruire le caractère ouvert et international de l'Internet et créerait des menaces pour la protection de la vie privée. Ainsi un blocage total et incontournable ne serait pas la bonne solution. Des mesures moins intruses seraient appropriées, mais lesquelles ? La thèse dresse une feuille de route qui aidera le législateur ou le régulateur à trouver le "bon" niveau d'intervention tenant compte à la fois de la nature du contenu nuisible en jeu, le choix des actions possibles par des intermédiaires techniques, et leur relative efficacité par rapport aux coûts. La "bonne" mesure est celle qui maximise le bien-être social, à savoir la totalité des bénéfices découlant de la mesure d'intervention moins la somme des coûts engendrés par la mesure. Les coûts à prendre en compte comprennent évidemment les coûts directs pour l'administration et pour les intermédiaires techniques liés à la mise en œuvre de la mesure, mais également les coûts indirects pour la société. Ces coûts indirects peuvent comprendre l'effet dommageable sur la liberté d'expression, sur la protection de la vie privée, ou sur la protection du caractère ouvert de l'Internet. En théorie, une bonne prise en compte des coûts et bénéfices pour la société de telle ou telle mesure conduira à une approche optimale pour traiter chaque problème de contenu sur Internet. En réalité, la méthode servira uniquement à identifier plusieurs approches pour lesquelles les bénéfices nets paraissent élevés. Il reviendra ensuite aux décideurs politiques, législateurs ou régulateurs, à choisir la meilleure approche qui teindra compte non seulement de l'étude d'impact, mais aussi d'aspects liés à la faisabilité politique de certaines mesures. Ainsi, l'étude d'impact sera un outil pour éclairer la décision politique, non pas une règle pour s'y substituer.

Chapitre 2 – Les quatre variables de l’équation.

Le chapitre 2 de la thèse présente les différentes variables qui doivent entrer en ligne de compte pour trouver l'approche optimale pour limiter l'accès à des contenus nuisibles. Ces variables sont au nombre de quatre :

- Le type de contenu nuisible en jeu,

- Le type d'intermédiaire technique et la forme d'action que cet intermédiaire technique pourrait prendre,
- Les options institutionnelles disponibles,
- Les dommages potentiels causés aux droits fondamentaux et à l'écosystème de l'Internet.

Chacune de ces variables est expliquée dans les prochains paragraphes.

Première variable: le type de contenus.

Les contenus nuisibles sur Internet regroupent un très grand nombre de cas. Le concept de contenu nuisible sur Internet reflète différentes priorités de politique publique destinées à protéger des valeurs sociétales ou économiques. Chaque type de contenu nuisible soulève des enjeux différents pour la société qui peuvent justifier des mesures de prévention et de sanction plus ou moins fortes. A titre d'exemple, les ressources que la société est disposée à investir dans la lutte contre la pédopornographie seront vraisemblablement plus élevées que les ressources que la société est disposée à investir contre les paris en ligne non autorisés. Il en est de même pour la lutte contre le terrorisme comparée à la lutte contre les téléchargements illicites d'œuvres protégées par le droit d'auteur. Le prix que la société est disposée à payer pour ces mesures de prévention et de sanction dépendra donc du type de contenu en jeu. Quand j'utilise le terme "prix à payer", je vise non seulement l'argent que l'administration et les entreprises vont dépenser pour mettre en œuvre des mesures de prévention et de sanction, mais également les coûts que les citoyens sont prêts à assumer en termes d'interférences avec leurs droits fondamentaux. Par exemple, une mesure visant à limiter l'accès à des sites d'incitation au terrorisme pourrait donner lieu à un "prix" plus élevé en termes d'interférence avec la protection de la vie privée qu'une mesure destinée à limiter l'accès à des sites proposant le téléchargement non autorisé de films.

Cela ne veut pas dire que certaines politiques de contenu sont plus légitimes que d'autres. L'ensemble des politiques de contenu adoptées dans une société démocratique ont leur légitimité et méritent donc un certain niveau de ressources pour leur mise en œuvre. Mais dans un contexte où les ressources sont limitées, une priorisation entre les différentes politiques de contenus sera inévitable et cette priorisation tiendra compte bien évidemment des dommages sociétaux que la politique de contenu est destinée à prévenir. Pour simplifier, si l'on dispose de 100 euros pour mettre en œuvre des mesures de prévention, on allouera ces 100 euros à différentes mesures de prévention en tenant compte du résultat visé par chaque mesure : prévention d'attaques terroristes, prévention de l'exploitation sexuelle d'enfants, prévention de téléchargements illicites. Comme nous le verrons dans le chapitre 6, bien définir le résultat que l'on cherche à atteindre par une politique de blocage est la première démarche à entreprendre dans une étude d'impact. La définition de ce résultat, et le lien de causalité entre la mesure

réglementaire et l'atteinte de ce résultat, seront déterminants pour mesurer les bénéfices escomptés de telle ou telle mesure de régulation.

Les politiques de contenu correspondent généralement à des défaillances du marché de différents types. L'envoi de spams et de codes malveillants créent des externalités négatives car la personne qui envoie ces messages et son fournisseur d'accès Internet (FAI) ne supportent pas l'intégralité des coûts associés à l'envoi. Dans ce domaine, les fournisseurs de services e-mail et les FAIs déploient eux-mêmes des outils anti-spams et anti-codes malveillants sans que ces actions soient ordonnées par un tribunal. Il est communément admis que le blocage de contenus malveillants de ce type peut être effectué par les opérateurs de réseaux afin d'assurer la sécurité de leurs réseaux et de leurs utilisateurs. Il s'agit d'une dérogation aux principes de la neutralité de l'Internet qui est admise à la fois dans la législation américaine et européenne. Même si les intermédiaires techniques internalisent une grande partie des coûts liés à des attaques de cybersécurité, certains aspects de la lutte contre la cybersécurité revêtent des caractéristiques de biens publics. Par exemple, la communication au gouvernement par l'ensemble des entreprises des caractéristiques d'attaques de cybersécurité peuvent contribuer à des défenses plus efficaces car coordonnées entre les entreprises et le gouvernement. Cependant cet aspect de la lutte contre la cybersécurité ressemble à l'effort de défense nationale. En tant que bien public, cet aspect de la lutte contre la cybersécurité ne sera pas produit par le marché en quantité suffisante en l'absence d'une obligation réglementaire. Cela explique pourquoi cet aspect de la cybersécurité fait l'objet d'une réglementation, notamment en Europe.

Une autre forme de contenu potentiellement nuisible est l'utilisation de cookies et d'autres logiciels pour pister l'activité des internautes. Contrairement aux codes malveillants, les cookies remplissent généralement une fonction légitime. Ils permettent une navigation plus aisée sur les sites web et permettent le développement d'un marché efficace pour la publicité. Cependant l'utilisation de cookies soulève un problème d'asymétrie d'information, ce qui empêche les utilisateurs d'effectuer des choix en connaissance de cause. Par conséquent, le but de la régulation est de renforcer des obligations d'information qui pèsent sur les éditeurs de sites web et sur les fournisseurs de cookies. Ces mesures de régulation doivent être mises en balance avec les bénéfices sociaux qui découlent de l'utilisation de ces cookies.

Le droit à l'oubli est une forme particulière de politique de contenus. Ce droit découle de la Directive 95/46 de l'Union Européenne, qui permet à une personne de demander le déréférencement de certains résultats de recherche sur les moteurs de recherche à la suite d'une recherche effectuée à partir de son nom. Ce droit au déréférencement est tout à fait particulier parce que l'objectif de la régulation n'est pas de rendre le contenu lui-même inaccessible. Le contenu lui-même, par exemple un article de journal, est parfaitement licite. L'objectif est seulement de rendre ce contenu plus difficile à trouver par le biais d'un moteur de recherche lorsque la recherche est effectuée à partir du nom d'une personne. L'exemple type d'une

demande de déréférencement serait une personne qui a fait l'objet d'un article de presse défavorable il y a de nombreuses années et qui ne souhaite plus que cet article de presse apparaisse sur les résultats de recherches effectuées à partir de son nom. S'il s'agit d'une personnalité publique, la demande de déréférencement sera généralement rejetée car l'accès à cette information est important pour le débat public et le journalisme. En revanche s'il s'agit d'une personne sans aucun rôle dans la vie publique, une autorité de régulation pourra ordonner le déréférencement de ce site web dans la liste des résultats de recherches. Sur le plan économique, le résultat de recherches désagréable crée un dommage pour la personne concernée, et ce dommage n'est pas internalisé par les parties à la transaction, à savoir l'internaute effectuant la recherche et le moteur de recherche. Il s'agit donc d'une externalité. S'il n'existait aucun coût de transaction, on pourrait imaginer un marché pour le droit à l'oubli. La personne qui souhaiterait bloquer un résultat de recherche proposerait un prix pour que le résultat n'apparaisse pas. La personne effectuant la recherche, elle, proposerait un prix pour voir le résultat en question. Si le prix de l'internaute effectuant la recherche était plus élevé que le montant demandé par la personne demandant le déréférencement, une transaction pourrait être effectuée qui serait bénéfique pour tous. Ce qui rend la situation beaucoup plus complexe est le fait que l'information est un entrant indispensable pour le marché des idées et la liberté d'expression. Ainsi le déréférencement, qu'il soit ordonné par une autorité de régulation ou qu'il résulte d'une transaction, crée également des dommages pour la collectivité qui doivent être pris en considération. Richard Posner (1978) met en avant les dommages créés par la non-divulgation d'informations importantes mais véridiques à propos d'une personne. Cela crée des asymétries d'information qui conduisent à des transactions inefficaces. Par ailleurs, si les personnes effectuant une recherche sur Internet savent que les résultats sont tronqués soit par le biais d'une régulation soit par le biais de transactions non divulguées, les personnes vont partir du principe que chaque liste de résultats cache des résultats non flatteurs à propos d'un individu. Cela conduira chaque personne qui effectue une recherche à effectuer des dépenses supplémentaires afin de trouver des résultats exhaustifs. Ces dépenses supplémentaires peuvent aller jusqu'à payer un détective privé afin d'effectuer des enquêtes. On constaterait en plus un phénomène d'*adverse selection* puisque les demandeurs d'informations partiraient tous du principe que l'information fournie est incomplète et n'inclut pas des informations défavorables. Cela pénaliserait des personnes qui n'ont aucune information défavorable à cacher. Sur le marché de l'information, on réduirait la valeur de l'information présentée par une personne qui n'a rien à cacher.

L'existence de moteurs de recherche neutres et non filtrés (au moins en ce qui concerne les contenus légaux) génère des bénéfices pour les éditeurs de sites web. Si on imagine une recherche sur Internet comme une transaction entre l'internaute et le moteur de recherche, cette transaction génère des externalités positives pour les éditeurs de site web, parce que ceux-ci n'auront pas besoin de dépenser des montants importants en publicité afin d'être visibles sur Internet. Le droit à l'oubli peut éventuellement diminuer ces externalités positives en réduisant

l'accessibilité de certains contenus. Dans le chapitre 3, nous décrivons les caractéristiques particulières de la liberté d'expression et pourquoi les mesures réglementaires qui réduisent l'accessibilité à des informations sur Internet sont considérées avec beaucoup de circonspection par les tribunaux.

Les sites de paris en ligne non autorisés sont un autre type de contenu qui donne lieu à des mesures de blocage auprès des intermédiaires techniques. Les paris en ligne peuvent générer des dommages car les personnes peuvent se surendetter et devenir psychologiquement dépendantes aux jeux. Les paris en ligne sont susceptibles également de générer d'autres dommages pour la collectivité notamment en permettant le développement de filières mafieuses. Pour cette raison, ces activités sont réglementées dans la plupart des pays. En France il existe une autorité indépendante dénommée l'ARJEL qui accorde des autorisations pour les sites de paris en ligne et qui identifie des sites de paris en ligne non autorisés pour lesquels l'accès en France doit être bloqué. Après avoir identifié ces sites, l'ARJEL demande à un tribunal d'ordonner le blocage de ces sites auprès de l'ensemble des fournisseurs d'accès à Internet en France.

La vente en ligne de cigarettes et d'alcool sont également réglementées en particulier pour limiter la contrebande et le détournement de règles fiscales. Les sites vendant des médicaments contrefaits peuvent également faire l'objet de mesures de blocage en raison de leur menace pour la santé publique. Il en est de même pour les sites de vente de substances interdites.

La protection de la propriété intellectuelle est source de grand nombre de mesures visant le blocage de sites et autres services en ligne. La dématérialisation des œuvres permet la reproduction et la transmission à faible coût d'un très grand nombre d'exemplaires d'une œuvre protégée par le droit d'auteur. L'Internet facilite donc la violation du droit d'auteur à la fois par des internautes et par les acteurs du crime organisé. Les mesures de régulation visent en premier lieu l'hébergeur des contenus illicites. Celui-ci doit retirer rapidement tout contenu qui est en violation de droit d'auteur dès que l'hébergeur reçoit une notification de l'ayant-droit. En plus de ce dispositif visant les hébergeurs, il existe des mesures de régulation qui visent à décourager le téléchargement par les internautes. L'approche "réponse graduée" est utilisée en France notamment, où une autorité indépendante, l'HADOPI, envoie des avertissements aux internautes qui utilisent des réseaux pair à pair pour échanger des œuvres protégées par le droit d'auteur. Des mesures de blocage peuvent également être ordonnées par un tribunal afin de rendre inaccessibles des sites qui proposent un accès à des œuvres sans l'autorisation des ayant-droits. Ces mesures de blocage sont ensuite mises en œuvre par les fournisseurs d'accès à Internet. Outre le droit d'auteur, le droit des marques ou des brevets peuvent également justifier des mesures de blocage à l'égard de sites proposant des produits contrefaisants.

Le contenu de certains sites est diffamatoire ou viole la protection de la vie privée de l'individu. Certains sites peuvent également proposer des contenus haineux, avec incitation à la haine raciale, ethnique ou religieuse. Des sites de ce type font souvent l'objet de mesures de blocage,

car les éditeurs et les hébergeurs de ces sites sont généralement situés en dehors du territoire national.

Deuxième variable : les intermédiaires techniques.

Le deuxième variable à prendre en considération est le type d'intermédiaire technique, ainsi que le type d'action que cet intermédiaire serait susceptible de prendre. Les moteurs de recherche sont parfois appelés à appliquer des mesures pour limiter l'accès à certains types de contenus. Le moteur de recherche peut délister totalement certains sites illégaux, afin qu'ils n'apparaissent pas du tout sur la liste de résultats. Le moteur de recherche peut également déclasser certains résultats afin qu'ils paraissent plus bas dans la liste de résultats. Les mesures prises par les moteurs de recherche sont généralement mises en œuvre en fonction du pays à partir duquel l'internaute effectue la recherche.

Les hébergeurs sont un intermédiaire technique privilégié lorsqu'il s'agit de mesures visant à empêcher l'accès à des contenus illicites. L'Europe et les Etats-Unis ont adopté des dispositions visant à protéger les hébergeurs contre toute responsabilité pour les contenus hébergés par leur service à condition que l'hébergeur agisse promptement pour retirer un contenu illicite lorsque l'hébergeur reçoit une notification.

Outre les hébergeurs et les moteurs de recherche, les fournisseurs d'accès à internet (FAI) sont souvent visés par des mesures de régulation. Les FAI sont parfois tenu d'empêcher l'accès à certains sites. Ces mesures de blocage peuvent faire appel à plusieurs mécanismes techniques. La mesure la plus fréquente consiste à donner une fausse adresse au site en question, afin que la requête aboutisse sur un autre site, par exemple une page qui prévient que le site a été déclaré illégal. Une autre technique de filtrage consiste à bloquer toute demande vers une certaine adresse IP. Cette technique conduit souvent à des phénomènes de surblocage, car la même adresse IP peut être partagée par plusieurs sites. Enfin, une technique de "deep packet inspection" permet au FAI d'examiner finement le contenu qui passe sur son réseau et le bloquer. Mais cette technique soulève des risques pour la protection de la vie privée.

Les registres de noms de domaines peuvent parfois changer l'adresse d'un site afin de rendre tout accès à ce site impossible. Cette technique a été utilisée aux Etats-Unis pour bloquer l'accès au site Megaupload.

Les fournisseurs de services de paiement en ligne peuvent appliquer des mesures pour empêcher tout paiement vers certains sites. Cependant, ces mesures peuvent être contournées par l'utilisation de moyens de paiements décentralisés tels que Bitcoin.

Les prestataires de services de publicité peuvent s'engager à ne pas vendre des services de publicité à certains sites illicites, mais là encore, il est relativement facile pour d'autre prestataires moins vertueux de remplir le vide.

Les magasins d'applications peuvent également mettre en œuvre des mesures afin d'éliminer de leurs magasins toute application qui serait contraire aux lois.

Les opérateurs de télécommunications de gros, ainsi que les CDN (content delivery networks), pourraient en théorie mettre en œuvre des mesures de filtrage, mais de telles mesures ne sont presque jamais mises en application en raison du volume de trafic qui passe par ces réseaux.

Les logiciels installés dans les navigateurs peuvent également permettre certains mesures de filtrage, à l'instar des logiciels de contrôle parental. Les "box" des FAI contiennent également des logiciels permettant le blocage de certains contenus.

Ainsi, la liste des intermédiaires techniques, et les mesures qu'ils peuvent prendre, est longue.

Troisième variable: le cadre institutionnel.

Le troisième variable dans notre équation est le cadre institutionnel. Ce cadre fera l'objet d'une étude approfondie dans le chapitre 4. Le cadre institutionnel représente un spectre d'alternatives, allant des règles sur la propriété et la responsabilité jusqu'à des mesures de droit souple d'autorégulation. Pour chaque politique de contenus, il existe en théorie un mélange optimal d'approches institutionnelles pour sa mise en œuvre.

Quatrième variable: Les externalités négatives provoquées par les mesures de régulation.

Chaque mesure de régulation va générer des coûts directs: coûts de l'administration, coûts des tribunaux, et coûts des intermédiaires techniques. En plus de ces coûts directs, il existe des coûts indirects qui sont rarement pris en compte. Ces coûts indirects comprennent d'une part l'impact d'une mesure sur les droits fondamentaux et d'autre part l'impact d'une mesure sur l'écosystème de l'internet. Ces coûts sont difficiles à mesurer. Le chapitre 3 est consacré aux droits fondamentaux. Le chapitre 6 aborde différentes méthodes pour mesurer l'impact sur ces droits. L'impact sur l'écosystème de l'internet est également difficile à mesurer. L'écosystème de l'internet est un terreau favorisant l'innovation, la liberté d'entreprendre, la liberté d'expression et la croissance économique. La liberté d'expression et la liberté d'entreprendre sont des droits fondamentaux. L'impact sur ces droits est donc mesuré sous la rubrique "droits fondamentaux". L'innovation et la croissance sont des éléments de richesse économique. Mesurer l'impact d'une régulation sur l'innovation et sur la croissance est également très difficile.

Une mesure de régulation peut également provoquer des comportements inattendues de la part des internautes qui peuvent créer d'autres coûts pour la société. Par exemple, une mesure destinée à pister les internautes afin de détecter des téléchargements illicites peut encourager l'utilisation d'outils de chiffrage, ou des réseaux alternatifs ("*dark web*"), rendant plus difficile la tâche des forces de police dans les enquêtes concernant d'autres crimes.

En résumé, il existe huit éléments dans l'équation:

A: le type de contenus en cause et le niveau de dommage que ces contenus causent à la société;

B: le type d'intermédiaire technique;

C: l'action que cet intermédiaire technique peut prendre;

D: l'encadrement institutionnel;

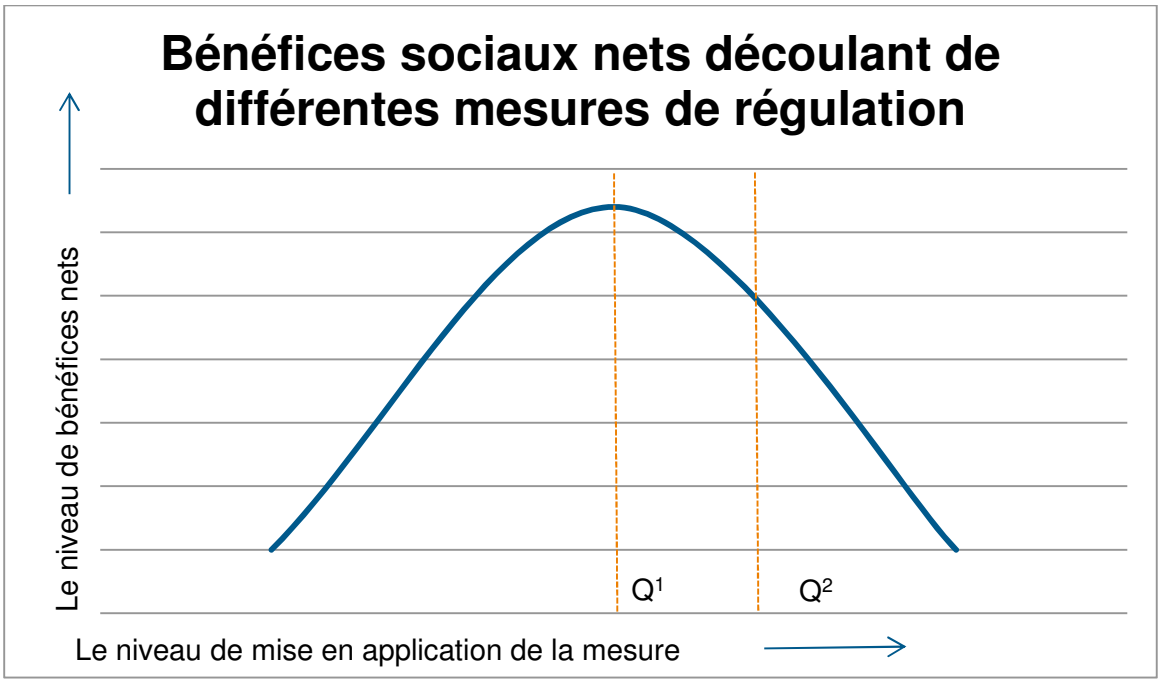
E: les coûts directs de la mesure envisagée;

F: les coûts indirects causés par la mesure sur la protection de droits fondamentaux;

G: les coûts indirects causés par la mesure sur l'écosystème de l'internet et l'innovation;

H: les coûts découlant de changements de comportement dommageables par les internautes.

Le problème à résoudre est de maximiser le bien-être social. Pour ce faire, il faut trouver la combinaison des éléments *B, C* et *D* qui maximise les bénéfices nets pour la société, à savoir les bénéfices découlant de la mise en œuvre de la politique de contenus *A* moins les coûts *E, F, G* et *H*. Résoudre ce problème est complexe car les éléments *A, F, G* et *H* sont difficilement quantifiables. Je propose une approche en chapitre 6.



Dans le diagramme ci-dessus, la mise en application de la mesure de régulation au niveau Q^1 maximise le bien-être social. Le niveau Q^2 représente une mesure plus stricte, qui permet un niveau de protection plus élevé contre le contenu dommageable. Cependant, en raison des coûts directs et indirects causés par la mesure Q^2, le bien-être social ne sera pas maximisé. Comme pour d'autre crimes et délits (Shavell 1993), le niveau optimal de mise en application

d'une mesure de prévention pour des contenus indésirables ne sera pas une mesure qui permet de prévenir le risque à 100%, car les coûts associés à une mesure prévenant le risque à 100% seraient très élevés.

Chapitre 3: les droits fondamentaux

Pour trouver la mesure qui maximise le bien-être social, il faut avoir une approche qui permet de comparer l'impact de différentes mesures sur les droits fondamentaux. Souvent, les droits fondamentaux doivent être mis en équilibre dans un test de proportionnalité. Les droits fondamentaux découlent de conventions internationales et de constitutions. Ils sont avant tout destinés à protéger les citoyens contre des abus commis par la majorité, à savoir des abus d'une majorité parlementaire et d'un gouvernement qui, une fois en place, serait tenté de mettre en place des mesures pour rester en pouvoir. Les droits fondamentaux sont des garde-fous de la démocratie. Un point souvent oublié est que les droits fondamentaux sont couteux pour la société. Même si ces droits existent sur le papier, les citoyens ne peuvent en bénéficier sans un système judiciaire efficace et indépendant, ainsi qu'une autorité de police non-corrompue. Les droits fondamentaux dépendent ainsi des impôts et des choix budgétaires du gouvernement et du parlement. Un droit à la protection des données personnelles bénéficiera peu aux citoyens sans une institution pour faire respecter le droit, et cette institution coûte de l'argent.

La communication via Internet implique plusieurs droits fondamentaux dont le droit à la protection de la vie privée et la liberté d'expression. Ces deux droits fondamentaux existent aussi bien aux Etats-Unis qu'en Europe, même si leurs contours précis diffèrent des deux côtés de l'Atlantique. Depuis l'affaire LICRA c/ Yahoo! en 2000[i] jusqu'à la décision du 13 mai 2014 de la Cour de Justice de l'Union Européenne (CJUE) dans l'affaire Google c/ AEPD[i], le Premier Amendement de la Constitution américaine[i] est souvent vu comme étant en divergence avec l'approche européenne.

La différence entre l'Internet et la télévision.

La décision américaine la plus importante en matière liberté d'expression sur Internet est *Reno c/ ACLU (1997)*.[i] Cette décision a examiné la constitutionalité d'une loi[i] qui punissait la mise à disposition de contenus indécents ou sexuellement explicites en ligne, lorsque l'éditeur du contenu savait que ce contenu serait susceptible d'être vu par des mineurs. La Ministre de la Justice de l'époque, Janet Reno, a soutenu que la loi était conforme au Premier Amendement, puisqu'elle ne visait pas la suppression des contenus, mais seulement l'aménagement d'espaces sur Internet où ces contenus seraient inaccessibles aux mineurs. Selon la Ministre, la loi était comparable à une règle d'urbanisme obligeant les cinémas pour adultes à s'installer dans

certains quartiers de la ville. Une loi qui crée seulement des limites à l'emplacement, à la durées ou à la manière de présenter des contenus (*time, place or manner restrictions*) est généralement compatible avec le Premier Amendement. La Ministre a également plaidé que la loi était justifiée parce qu'Internet était similaire à la radio ou à la télévision, et que Cour Suprême a toujours permis une régulation plus contraignante de la télévision et de la radio en raison du caractère invasif de ces médias.

La Cour Suprême n'a pas suivi les arguments de la Ministre. La Cour a commencé par souligner la puissance d'Internet comme moyen de communication, en comparant Internet à une tribune où chaque individu peut s'exprimer librement sur une place publique.[i] De plus, la Cour a estimé qu'Internet n'est pas comparable à la radio ou à la télévision, puisque chaque internaute cherche activement le contenu qu'il souhaite, comme lorsqu'il rentre dans une bibliothèque. Contrairement à une émission de radio où les personnes écoutent passivement et peuvent être surprises par un contenu choquant, l'internaute est à la recherche active d'information, et ne sera ni surpris ni choqué par le résultat de ses recherches.[i] L'autre raison pour laquelle Internet n'est pas comparable à la télévision est que l'Internet n'utilise pas le spectre radioélectrique. Contrairement aux chaînes de télévision dont le nombre est limité par la quantité de fréquences de diffusion disponibles, le nombre de sites web n'est pas limité par des contraintes techniques. Or c'est la rareté du spectre radioélectrique et l'influence exceptionnelle de la télévision qui justifient une régulation plus stricte de ce média.[i] Pour l'Internet, la Cour a donc écarté l'idée d'une régulation de type audiovisuel en préférant rester sur un mode de régulation légère et respectueuse de la liberté d'expression, similaire à celle applicable à la presse écrite.

Les "*chilling effects*" sur la liberté d'expression.

Le point le plus important de la décision *Reno vs. ACLU* concerne les "*chilling effects*", littéralement les "effets réfrigérants", que les tribunaux visent à limiter. Les effets réfrigérants comprennent deux phénomènes. Tout d'abord l'effet de débordement: si une mesure de régulation vise à limiter l'accès à un contenu nocif du type "A", la mesure risque-t-elle également d'avoir un impact sur l'accès aux contenus inoffensifs du type "B"? Dans l'affirmatif, il existe un effet de débordement dommageable à la liberté d'expression. Ensuite, les effets réfrigérants peuvent résulter de la suppression du contenu nocif lui-même: est-ce que la suppression de ce contenu conduira à un appauvrissement général des échanges sur le marché des idées?

Plus les effets réfrigérants seront importants, plus la mesure sera en contradiction avec le Premier Amendement. Dans le cas de la loi américaine contestée dans l'affaire *Reno c/ ACLU*, la Cour a identifié deux types d'effets réfrigérants. Premièrement, en visant l'accès à des contenus sexuellement explicites ou indécents, la loi pourrait restreindre l'accès non seulement à la pornographie – le cœur de cible de la mesure -- mais également à des informations sur la

contraception, sur les maladies sexuellement transmissibles, voire sur l'anatomie. La loi risquerait donc de dépasser sa cible et de freiner l'accès par des mineurs à des informations licites. Deuxièmement, la loi pourrait conduire les éditeurs de contenus réservés aux adultes à cesser leur activité ou à réduire leur présence sur Internet, par crainte d'être poursuivis pénalement au nom de la loi. Puisqu'il est difficile de vérifier l'âge d'un internaute, certains éditeurs préfèreront ne pas prendre le risque d'éditer des contenus pour adultes et cesseront de les rendre disponibles sur Internet. Ainsi les adultes auront accès à moins de contenus pornographiques sur Internet alors que ces contenus sont parfaitement licites pour les adultes. La loi provoquera un appauvrissement dans l'offre de contenus. Pris ensemble, ces deux effets réfrigérants ont rendu la loi non-compatible avec le Premier Amendement.

On retrouve le concept d'effet réfrigérant dans le test de proportionnalité appliqué par la CJUE et la CEDH.[i] Lorsqu'elle évalue des mesures prises pour limiter l'accès non-autorisé à des œuvres protégées par le droit d'auteur, la CJUE est attentive au moindre effet de débordement qui conduirait à bloquer l'accès à certains contenus non protégés par le droit d'auteur, ou à des contenus protégés par le droit d'auteur mais pour lesquels une exception au droit d'auteur s'appliquerait.[i] En présence d'un effet de débordement, la CJUE aura tendance à juger la mesure excessive par rapport à l'objectif recherché; la mesure ne passera pas le test de la proportionnalité.

Les effets réfrigérants se retrouvent également dans la littérature concernant la responsabilité des hébergeurs et autres intermédiaires techniques. Dans un régime où l'intermédiaire technique endosse une responsabilité pour le contenu qu'il héberge, Schruers (2002) démontre que l'intermédiaire technique optera pour la prudence: il choisira des contenus et des clients qui présentent des profils de risque faible, ce qui conduira à un appauvrissement général du type de contenus disponibles sur Internet.

Le régime spécial de responsabilité des hébergeurs est destiné à remédier à ce problème et à réduire ainsi les effets réfrigérants. Selon ce système, un hébergeur n'est pas responsable du contenu qu'il héberge à condition qu'il retire le contenu rapidement après avoir reçu un signalement. Mais même ce système, favorable aux hébergeurs, n'est pas à l'abri de critiques relatives à ses effets réfrigérants. Si un hébergeur retire un contenu automatiquement dès qu'il reçoit une notification, cela peut conduire à une suppression excessive. Cet effet de débordement a été démontré par Ahlert *et al.* (2004), qui ont adressé des notifications à plusieurs plateformes d'hébergement demandant le retrait du texte *De la Liberté* de John Stuart Mill, texte écrit en 1859 et appartenant manifestement au domaine public. Se plaignant d'une prétendue violation du droit d'auteur, la notification a été suivie d'effet par la plupart des hébergeurs situés en Europe, démontrant un "effet réfrigérant" même sous l'égide du régime de responsabilité aménagé. Selon Seltzer (2010) la loi américaine sur le droit d'auteur, le DMCA[i], provoque des effets similaires,

puisque les notifications de retrait fondées sur le droit d'auteur seront systématiquement suivies d'effet, même si le contenu relève d'un cas d'utilisation équitable (*fair use)*.

Les effets réfrigérants et le droit à l'oubli

Les effets réfrigérants seront particulièrement présents en matière de droit à l'oubli. Dans sa décision du 13 mai 2014 contre Google[i], la CJUE impose aux moteurs de recherche l'obligation de supprimer certains résultats de recherche à la demande d'une personne concernée, notamment si les informations paraissent anciennes et non pertinentes. Afin de réduire leur responsabilité éventuelle, les prestataires préfèreront donner suite à ces demandes de suppression même lorsqu'il existe un doute quant à leur caractère fondé. Le droit à l'oubli provoquera des effets réfrigérants puisque la mesure affectera non seulement des informations anciennes et non-pertinentes, c'est-à-dire celles visées directement par la CJUE, mais également des informations simplement gênantes pour la personne qui a envoyé la notification. En matière de mesures prises pour combattre le téléchargement illicite, la CJUE ne tolère pas d'effet de débordement de ce type.[i] En matière de droit à l'oubli, la Cour semble moins gênée par ces effets collatéraux.

En droit américain, un éventuel droit à l'oubli serait analysé à deux niveaux. Tout d'abord, le cœur de cible de la mesure est-il légitime du point de vue de la liberté d'expression? Une mesure qui vise le retrait de photos ou de vidéos jugées attentatoires à la vie privée serait probablement conforme au Premier Amendement. La liberté d'expression ne protège pas des informations jugées diffamatoires ou attentatoires aux droits d'autrui. En revanche, une mesure visant le déréférencement d'articles de presse qui ne sont pas diffamatoires serait manifestement contraire à la liberté d'expression aux Etats-Unis.

Deuxièmement, la Cour évaluerait d'éventuels effets de débordement découlant de l'application de la mesure. Si les modalités d'application de la mesure pouvaient conduire à la suppression de contenus en dehors du cœur de cible, la Cour Suprême américaine annulerait la mesure en raison de ses effets réfrigérants. Selon la jurisprudence de la CJUE et de la CEDH, le résultat devrait en principe être identique compte tenu du test de la proportionnalité. Cependant, la décision de la CJUE du 13 mai 2014 semble s'écarter du test de proportionnalité classique.

Pour Rosen (2012), le droit à l'oubli serait antinomique au Premier Amendement. Si on part du principe qu'un droit à l'oubli du type imposé par la CJUE est contraire au Premier Amendement, on peut s'interroger sur l'effet extraterritorial de la mesure européenne. Une décision de justice rendue en France en matière de droit à l'oubli pourrait-elle être exécutée aux Etats-Unis ? Cette question rappelle l'affaire LICRA c/ Yahoo! de 2000 dans laquelle le Tribunal de Grande Instance de Paris avait ordonné à la plateforme américaine de supprimer l'accès aux objets nazis d'une vente en ligne. Dans une première décision[i], un tribunal californien avait déclaré la décision française contraire au Premier Amendement. Mais la décision d'appel de 2006[i] avait été plus

nuancée. Il n'existe pas de convention sur l'exécution des décisions de justice entre la France et les Etats-Unis. L'exécution d'une décision étrangère est donc régie par des règles de procédure civile de chaque Etat. Contrairement aux idées reçues, la Cour d'Appel américaine n'a pas dit qu'elle n'exécuterait pas la décision française contre Yahoo! L'affaire a été rejetée pour d'autres raisons. La Cour a expliqué que même si la loi française en question était contraire au Premier Amendement de la Constitution, ce n'est pas pour autant qu'un tribunal américain refuserait son exécution sur le territoire américain lorsque l'application de la loi étrangère viserait à protéger des citoyens français.

Pour refuser l'exequatur, un tribunal américain doit conclure que l'application de la décision étrangère est "répugnante" par rapport aux valeurs constitutionnelles américaines.[i] Si les effets de la décision sont cantonnés à un territoire étranger comme la France, un tribunal américain ne refusera pas nécessairement l'exécution de la décision aux Etats-Unis.[i]

L'idéologie du "marché des idées"

La liberté d'expression aux Etats-Unis repose sur une foi quasi-absolue dans le bon fonctionnement du "marché des idées". Lorsque les propos en question s'éloignent du marché des idées, pour se rapprocher d'un acte illégal (par exemple, proférer une menace ou un propos diffamatoire), la liberté d'expression cède la place à la protection d'autres droits et libertés. Pour évaluer la compatibilité des mesures de régulation avec la liberté d'expression, les tribunaux appliquent un test de proportionnalité similaire à celui appliqué par la CJUE et la CJUE. D'un côté, on pèse le préjudice qui sera causé par les propos en question ainsi que la probabilité selon laquelle ce préjudice se réalisera. On tient compte également du caractère imminent du préjudice. De l'autre côté, on évalue le préjudice que la mesure de régulation est susceptible de provoquer elle-même, notamment en faussant le bon fonctionnement du "marché des idées". Si la mesure en question risque d'étouffer certains points de vue, notamment dans le débat politique, le préjudice causé au marché des idées sera considérable, et ne pourra être justifié qu'en présence d'un préjudice particulièrement important, probable et imminent de l'autre côté de l'équation.

Posner (2011)[i] résume l'équation comme suit: $B < P \times L/(1+i)^n$,

où:

B est le coût supporté par la société qui est lié à l'appauvrissement du marché des idées causé par la mesure de régulation proposée, en tenant compte notamment des effets réfrigérants;

L est le coût lié à l'événement nocif que la mesure de régulation vise à empêcher, par exemple la commission de crimes racistes ou une attaque terroriste;

P est la probabilité selon laquelle l'événement nocif se produira en l'absence de la mesure de régulation;

i est le taux d'actualisation;

n est le nombre d'années précédant la réalisation de l'événement nocif, en l'absence de la mesure de régulation.

En application de ce test, une mesure interdisant la publication d'informations sur la fabrication d'une bombe chimique artisanale serait justifiée compte tenu de l'ampleur de L. En revanche, une interdiction de propos préconisant le renversement du gouvernement américain ne serait pas justifiée en raison de la faible probabilité P selon laquelle cet événement se produirait, combinée avec le manque d'immédiateté du risque (un "n" élevé). Par ailleurs, le préjudice pour le marché des idées serait élevé puisque la mesure risquerait d'interdire l'échange d'idées politiques dont certaines peuvent se révéler importantes pour le bon fonctionnement de la démocratie. La mesure risquerait de s'appliquer de manière surdimensionnée, créant des effets réfrigérants. De plus, la mesure pourrait être instrumentalisée par le gouvernement pour supprimer des propos critiques au pouvoir en place. Le même test pourrait être appliqué à une mesure visant à bloquer l'accès à des sites djihadistes. Quel est la menace réelle de ses sites, et est-ce que cette menace diminuera après la mise en œuvre de la mesure de blocage? Et surtout, comment distinguer entre un site djihadiste (le cœur de cible de la mesure) et un site dédié à l'expression d'un point de vue religieux ou politique important pour le marché des idées? La frontière entre les deux est difficile à établir, rendant les effets collatéraux inévitables, et particulièrement grave puisqu'il s'agit de points de vue politiques ou religieux. Le terme "B" de l'équation sera élevé. Dès 1927, la Cour Suprême reconnait que pour lutter contre des propos abjects, "le meilleur remède est plus de communication, non une silence imposée."[i]

Le principe de confrontation ouverte des idées est couplé à un deuxième: le gouvernement n'est pas fiable pour faire l'arbitre entre une bonne et une mauvaise idée. Selon cette thèse, le gouvernement sera forcément en conflit d'intérêts, et choisira de supprimer des idées qui constituent une menace pour le pouvoir politique en place. En influant sur le marché des idées, le gouvernement peut ainsi fausser le fonctionnement de la démocratie elle-même, créant un dérapage systématique et irrattrapable.[i]

Coase (1977) souligne certaines incohérences dans ce raisonnement, et suggère que la protection du marché des idées résulte d'un lobbying de l'élite intellectuelle, principal "producteur" d'idées affecté par une éventuelle mesure de régulation. Comme tout producteur, l'élite intellectuelle préférera un marché où la production des idées n'est pas limitée. Posner (2011) propose une autre explication. La production d'idées nouvelles, surtout lorsqu'elles sont bonnes, demande un investissement. Celui qui crée une nouvelle idée ne bénéficie pas généralement d'un retour sur investissement. Les principaux bénéficiaires de l'idée sont la collectivité. La fabrication de bonnes idées est donc un bien public, comme la défense nationale. Ainsi, l'Etat doit encourager la production d'idées, notamment en réduisant des effets réfrigérants tels que des risques de responsabilité pénale.

La liberté d'expression et l'autorégulation

Le Premier Amendement protège le citoyen contre les mesures prises par l'Etat. Les contrats privés ne sont pas concernés par le Premier Amendement, du moins pas directement. Cela signifie-t-il que les contrats ne peuvent jamais être remis en cause sur le fondement de la liberté d'expression ? Certains auteurs estiment que les contrats peuvent être contestés au titre du Premier Amendement.[i]

Cependant, il existe des différences importantes entre des mesures prises par un gouvernement et des mesures prises par des acteurs privés par voie contractuelle. Les acteurs privés agissent généralement dans un contexte de consentement et de concurrence, alors que l'Etat est en situation de monopole. En matière de liberté d'expression, l'Etat est considéré comme le monopoleur "le plus dangereux".[i] La concurrence dans le secteur privé signifie qu'un utilisateur peut changer de plateforme s'il estime que les conditions d'utilisation sont trop restrictives. La situation serait plus complexe si l'ensemble des grandes plateformes adoptait le même règlement interne. Kreimer (2006) a étudié l'utilisation de l'autorégulation sous l'ère McCarthy pour conclure que l'autorégulation peut être un outil redoutable de la censure. Si YouTube, Facebook et Twitter existaient à l'époque de McCarthy, on pourrait imaginer sans trop de difficulté que ces plateformes, sous la pression indirecte du puissant sénateur, interdiraient dans leur règlement intérieur tous propos communistes. Dans certains pays non-démocratiques, l'Etat n'a pas besoin d'adopter une loi pour faire comprendre aux plateformes qu'il convient de bloquer l'accès à certains contenus. L'action de l'Etat s'exerce par contrainte indirecte sur les acteurs privés.[i]

Certaines grandes plateformes Internet interdisent, dans leurs conditions générales d'utilisation, les contenus destinés à provoquer la haine raciale ou religieuse, remplissant ainsi le vide laissé par la jurisprudence *R.A.V c/ City of St Paul*. Les plateformes ne surveillent pas les contenus postés par les internautes, mais réagissent aux signalements. Rosen (2013) décrit les personnes qui, au sein des plateformes, sont en charge de gérer les questions délicates de retrait. Ces personnes, appelées les "décideurs", ont, selon le Professeur Rosen, plus d'impact sur les types de contenus visibles sur Internet que les juges et les autorités de régulation. Les plateformes ont créé un groupe de travail sur les contenus haineux présents sur Internet (*Anti Cyber Hate Working Group*) dont les objectifs sont de développer des méthodes qui permettent aux plateformes de se positionner vis-à-vis de contenus controversés tels que la vidéo "*L'innocence des musulmans*" postée sur YouTube (qui a provoqué des émeutes et même l'intervention du Président Obama devant les Nations Unies). Un autre exemple cité par le Professeur Rosen est l'échange de tweets antisémites dans l'affaire "#Unbonjuif".

Les plateformes emploient un réseau de personnes qui évaluent les signalements dans un premier temps et déterminent ceux qui doivent donner lieu à un retrait instantané et ceux qui doivent être soumis à leur superviseur chargé de s'assurer du respect des politiques de contenus. Des contenus qui poussent à la violence de manière précise, envers un groupe de

personnes bien déterminé, sont généralement enlevés. En revanche, des contenus qui critiquent une institution, un Etat ou une religion de manière générale ne sont pas enlevés immédiatement. Si le contenu est manifestement illégal dans un pays donné, par exemple les tweets "#Unbonjuif" en France, l'accès au contenu dans ce pays peut être bloqué si la technologie le permet.

Rosen parvient à la conclusion que la méthodologie appliquée par les plateformes, bien qu'étant imparfaite, aboutit à des résultats qui ne sont pas très éloignés de ce qu'aurait décidé un tribunal confronté au même problème de contradiction entre les lois de différents pays. Il s'agit ainsi d'une forme d'autorégulation qui permet de trouver un équilibre prenant en compte des considérations à la fois juridiques et pragmatiques.[39]

Le test de proportionnalité

Lorsqu'une mesure a un impact défavorable sur un droit fondamental, la mesure doit faire l'objet d'un test de proportionnalité. Ce test peut être assimilé à une analyse coûts-bénéfices. Le test de proportionnalité peut se limiter à vérifier que l'impact défavorable sur le droit fondamental est plus que compensé par les effets bénéfiques de la mesure pour la société. Il s'agit dans ce cas d'un test qui vérifie simplement si les bénéfices excèdent les coûts. Cependant, la jurisprudence exige généralement non seulement que les bénéfices nets soient positifs, mais que le calcul des coûts inclut les coûts d'opportunité, à savoir les bénéfices non-réalisés en ne poursuivant pas une autre piste alternative. Lorsque les coûts d'opportunité sont pris en compte, le test nécessite de choisir la mesure qui, parmi tous les choix alternatifs, permet de maximiser le bien-être social. Cette recherche de pistes alternatives se reflète dans la jurisprudence de la Cour européenne de justice qui exige l'identification du "moyen le moins préjudiciable" pour atteindre l'objectif recherché. Robert Alexy (2012) a construit une méthode pour comparer différentes mesures et leur impact sur les droits fondamentaux. Alexy attribue un score à différentes mesures selon leur niveau d'impact sur les droits fondamentaux. SURVEILLE, un projet financé par la Commission européenne, poursuit une méthodologie similaire pour évaluer différentes mesures de surveillance et leur impact sur les droits fondamentaux.

Tout système de mise en équilibre de droits fondamentaux doit veiller à ne pas fragiliser l'essence même du droit. Il existe un seuil minimum de protection du droit en dessous duquel on ne peut pas s'aventurer, sous peine de détruire l'essence même du droit. Nussbaum (2002) suggère d'attribuer un coût infiniment élevé à une mesure qui conduirait à passer en dessous du seuil critique de protection du droit.

Chapitre 4 – les choix institutionnels

Il existe quatre catégories d'approches institutionnelles:

- Les lois générales sur la propriété et sur la responsabilité, le respect desquelles est assuré par les tribunaux;

- La réglementation créée et mise en application par une autorité administrative;

- L'autorégulation, qui peut être unilatérale par le biais de conditions générales d'utilisation, ou multilatérale par le biais de codes de conduite ou chartres collectives,

- La co-régulation, qui permet à l'état de déléguer à l'entreprise une partie de la responsabilité de la mise en application de la norme, mais en étroite collaboration avec l'état.

Chaque approche institutionnelle présente des avantages et des inconvénients. Les lois sur la responsabilité et sur la propriété sont toujours présentes, et représentent la fondation sur laquelle les autres approches sont construites. Bien souvent, il existe pour les services internet des conditions générales d'utilisation, qui créent des droits et obligations supplémentaires à l'intérieur du cadre créé par les lois sur la responsabilité et sur la propriété. Les lois générales sur la responsabilité et sur la propriété permettent aux tribunaux d'être souples, et adapter l'application des lois aux nouveaux développements technologiques, et aux nouveaux contextes sociaux. Cependant, l'adjudication par les tribunaux présente des inconvénients. L'inconvénient le plus important est la perspective temporelle des tribunaux. Ceux-ci ont pour mission de régler un litige concernant des faits qui se sont passés il y a des mois, voire des années. Le tribunal n'a pas pour mission première de donner des signaux aux acteurs économiques pour l'avenir, même si pour certains juges l'effet de leur décision sur le marché va quand même rentrer en ligne de compte. En raison de leur mission de régler un litige précis, les tribunaux peuvent rendre des décisions qui semblent incompatibles entre elles, ce qui crée des incertitudes pour les acteurs du marché. De plus, certains juges ne sont pas spécialistes de la technologie, ce qui peut réduire leur efficacité par manque d'information. Enfin, le temps judiciaire est lent comparé au rythme des évolutions technologiques.

La régulation par des autorités administratives spécialisées permet de palier à certains de ces inconvénients. Une autorité de régulation aura une vision prospective du marché, et tentera d'établir des règles claires pour guider les acteurs du marché et ainsi réduire l'incertitude. L'autorité de régulation sera également spécialisée, et aura un meilleur accès à l'information grâce à ses contacts réguliers avec les entreprises régulées. Le revers de la médaille est que l'autorité de régulation peut être trop influencée par les entreprises qu'elle régule. On parle alors de "capture" du régulateur par l'industrie.

L'auto-régulation, qu'elle soit unilatérale (conditions générales d'utilisation), ou multilatérale (chartes, codes de bonne conduite) est en principe bien adaptée à la fois aux acteurs et aux problèmes posés, puisque ce sont les acteurs eux-mêmes qui définissent les mesures de régulation à mettre en œuvre. Les acteurs disposent souvent de la meilleure information sur ce qui est faisable et efficace pour traiter un problème donné. L'inconvénient de l'auto-

régulation est que l'intérêt public peut être sous-représenté dans l'élaboration des solutions d'auto-régulation. Un autre inconvénient est le phénomène de passager clandestin. Certaines entreprises souscriront à des codes de bonne conduite pour bénéficier de l'image y associée sans pour autant mettre en œuvre des mesures exigées par le code. L'auto-régulation pose un problème de discipline des membres du groupe. L'autodiscipline fonctionne bien lorsque les acteurs font partie d'un petit groupe et la menace d'exclure un membre du groupe a un effet disuasif. Mais lorsqu'il existe un grand nombre d'acteurs, et l'exclusion d'un groupe ne crée pas de réel préjudice pour une entreprise, maintenir un niveau élevé de conformité parmi les acteurs peut s'avérer difficile.

La co-régulation émerge comme une solution intermédiaire entre la régulation détaillée édictée par une autorité de régulation, et l'auto-régulation. Dans la co-régulation le régulateur délègue aux entreprises certains pouvoirs normatifs. Cette délégation s'est faite en matière de droit de l'environnement et devient fréquente en matière de régulation des données à caractère personnel. On parle d'*accountability*. Dans une approche d'*accountability*, cette délégation s'accompagne du devoir de rendre compte de la bonne exécution de la mission. Cela signifie que l'entreprise doit disposer d'une structure de gouvernance pour assurer la qualité de la norme qu'elle crée. Des contrôles internes seront nécessaires pour assurer que la norme développée au sein de l'entreprise tient compte des objectifs du régulateur. Certaines démarches seront nécessaires en interne (études d'impact…) pour établir la norme et pouvoir démontrer qu'elle a été adoptée dans de bonnes conditions. On essaiera d'appliquer au sein de l'entreprise les mêmes démarches qu'un régulateur aurait appliquées si le régulateur avait élaboré la norme. On imite la fonction de régulation, en le déplaçant à l'intérieur de l'entreprise.

Un exemple-type de co-régulation est l'adoption de *Binding Corporate Rules* (BCR). Les BCR désignent un code de conduite interne qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne. L'adoption de BCR permet notamment d'être en conformité avec les principes de la Directive 95/46/CE, de communiquer sur la politique d'entreprise en matière de protection des données personnelles et d'assurer un niveau de protection satisfaisant lors des transferts de données personnelles[i]. On retrouve ici deux ingrédients essentiels de l'*accountability* et de la co-régulation : la conformité et la transparence.

Chapitre 5 – L'utilisation d'études d'impact et d'analyses coûts/bénéfices dans l'élaboration de la régulation

Dans le cadre de la méthodologie préconisée par l'OCDE (2011, 2012) et la Commission Européenne (2015a), un besoin de régulation doit s'apprécier par rapport à un objectif bien défini, généralement une défaillance du marché démontrée, et un modèle de référence qui décrit comment cette défaillance de marché est susceptible d'évoluer en l'absence de régulation. Ce

modèle de référence n'est pas statique, mais doit prendre en compte l'évolution probable du marché et de l'environnement réglementaire dans les années à venir (Renda *et al.*, 2013). Dans le cas d'une proposition de réglementation spécifique visant à limiter l'accès à des contenus illicites, la première étape est de définir avec précision les défaillances du marché en cause – abus de pouvoir de marché, externalités négatives, asymétries d'information. Le scénario de référence décrit comment les règles et lois en vigueur peuvent être mobilisés pour éliminer ces défaillances : droit de la concurrence, règlement européen relatif à la protection des données personnelles, lois sur la protection du consommateur, actions de groupe, etc ... S'il existe des initiatives de droit souple (autorégulation, corégulation) – par exemple pour la lutte contre des contenus illicites – l'application prospective de ces approches doit aussi être prise en compte.

Une fois un scénario de référence déterminé, il doit être comparé avec les diverses options réglementaires proposées. Chacune de ces options doit être comparée au scénario de référence, en termes d'efficacité. Par exemple, si le problème est un abus de pouvoir de marché vis-à-vis d'entreprises (à l'égard d'hôteliers, par exemple), le niveau de ce problème doit être comparé, entre le scénario de référence et l'option de régulation proposée. Si le niveau du problème est égal à 10 dans le scénario sans régulation, et il n'est que 8 dans le scénario régulation, le bénéfice escompté de la mesure sera égal à 2.

Il faut ensuite estimer les coûts directs et indirects de chaque option de régulation par rapport au scénario de référence. Les coûts directs comprennent les coûts de mise en œuvre du nouveau cadre réglementaire - création d'une nouvelle autorité administrative, ressources humaines et financières additionnelles mobilisées -- ainsi que les coûts directs pour les entreprises impactées par les nouvelles obligations réglementaires (là encore en termes de ressources humaines, coût des prestataires (par exemple cabinet d'avocats, sociétés informatiques) si une partie du travail est externalisé …). Enfin, les coûts indirects comprennent notamment les effets sur l'innovation, sur des droits fondamentaux, sur la concurrence, ou sur le caractère ouvert de l'Internet.

Aux termes de cette analyse, l'option qui dégage le bénéfice net (bénéfices moins coûts) le plus élevé doit être privilégiée. Toutefois ce type d'analyse n'est pas simple à mettre en œuvre sur les marchés numériques compte tenu de leur forte volatilité économique et imprévisibilité technologique. La réglementation des marchés numériques est particulièrement propice aux erreurs et inefficacités. Shelanski (2013) explique que les coûts associés à une réglementation inadaptée sont beaucoup plus élevés que les coûts qui auraient été supportés en l'absence d'intervention (scénario de référence). Cela s'explique par le fait que dans les marchés numériques à évolution rapide, le marché règle souvent la question sans intervention de l'Etat. L'imprévisibilité des marchés émergents a été reconnue par la Commission Européenne dès 2007 dans le cadre de sa recommandation sur la régulation des marchés de communications électroniques. "En général, les marchés nouveaux et émergents sont instables, présentant l'incertitude de l'offre et de la demande et des fluctuations dans les parts de marché. Ils sont

caractérisés par un degré élevé d'innovation qui peut conduire à des changements brusques et inattendus (par opposition à une évolution naturelle au fil du temps)" (Commission Européenne, 2007).

En appliquant la méthodologie européenne, les Etats-membres devraient en principe s'abstenir de réguler précipitamment les marchés sur lesquels se développent les intermédiaires techniques. Mais cette vision très pragmatique de la régulation ne correspond pas toujours aux réalités politiques. Dans le cas des intermédiaires techniques, l'action politique répond à des pressions des citoyens et de groupes d'intérêts. Ces préoccupations peuvent s'alimenter par des craintes plus ou moins rationnelles (Sunstein, 2005). Pour répondre à ces préoccupations, une régulation peut alors s'imposer pour son pouvoir symbolique. On parle alors de la fonction "expressive" (Sunstein 1996) et "normative" (Schultz 2008) de la loi. L'efficacité de la mesure n'est qu'une considération secondaire. Néanmoins, les méthodologies "mieux légiférer" préconisées par l'OCDE et la Commission européenne visent à assurer que l'efficacité d'une mesure de régulation – à savoir ses bénéfices nets comparés au scénario de référence – n'est pas complétement occultée par ces débats symboliques ou par des enjeux corporatistes.

Certains auteurs prônent une régulation expérimentale qui intègrerait la possibilité d'ajuster la régulation en fonction des résultats observés. Il s'agit d'une régulation "adaptative" et "expérimentale". Cette approche serait particulièrement bien adaptée aux marchés numériques, où le risque d'erreur est élevé. Car il faudrait non seulement que la régulation encourage l'innovation, mais que la régulation elle-même reflète une culture d'innovation et d'expérimentation, ce qui nécessiterait des études d'impacts beaucoup plus poussées et des mécanismes de suivi.

Le défi est d'intégrer ces méthodes scientifiques dans les processus institutionnels et politiques de l'élaboration de la norme, ce qui n'est pas évident.

Chapitre 6 – La création d'une méthode pour évaluer des mesures de régulation visant à limiter l'accès à certains contenus illicites sur Internet.

Le chapitre 6 propose une méthodologie en cinq étapes pour évaluer toute mesure destinée à limiter l'accès à des contenus préjudiciables sur Internet:

Etape 1: Le régulateur ou législateur désirant adopter une mesure de régulation devra remplir un questionnaire destiné à identifier avec précision l'objectif de régulation recherché, et comment l'atteinte de cet objectif pourra être mesurée. Le questionnaire devra identifier les intermédiaires techniques qui pourraient contribuer à l'atteinte de l'objectif, et lister les actions que ces intermédiaires pourraient mettre en oeuvre, allant du moins intrusif au plus intrusif. Le questionnaire identifierait les approches utilisées à l'étranger pour traiter ce genre de problème, et ferait une liste des différentes options institutionnelles qui pourraient être envisagées. Le

questionnaire examinera les droits fondamentaux affectés par les différentes mesures proposées, et les effets sur l'écosystème de l'internet.

Etape 2: Après le questionnaire, le régulateur devra conduire une analyse couts/bénéfices. Pour ce faire, il devra d'abord élaborer un scénario de référence, pour décrire comment la situation évoluera en l'absence de toute mesure de régulation. En particulier, ce scénario de référence devra identifier le niveau d'atteinte de l'objectif au bout d'une certaine période en l'absence d'une nouvelle mesure de régulation. Cet aspect est délicat, car il faut savoir mesurer l'atteinte d'un objectif, et mesurer le taux de réussite d'une politique de contenus qui est par définition qualitative et difficile à mesurer. A titre d'exemple, on pourrait mesurer le temps qu'il faut à un internaute moyen pour trouver un site pédopornographique, ou le nombre de téléchargements illicites effectués dans une année. Pour certaines politiques de contenus, mesurer le niveau de "succès" dans l'atteinte de l'objectif sera très délicat. Comment mesurer si une régulation destinée à promouvoir la culture française atteint l'objectif recherché? L'élaboration d'un scénario de référence obligera le régulateur à bien réfléchir à ce problème.

Après l'établissement du scénario de référence, le régulateur construira des scénarii à partir de différentes approches de régulation. En ce faisant, le régulateur mesurera le niveau de bénéfices découlant de chaque approche comparé au scénario de référence. C'est ici où l'identification du niveau de "succès" dans le scénario de référence est particulièrement importante, car cela permet de mesurer la différence entre le niveau de succès dans le scénario de référence et le niveau de succès atteint dans chaque scénario alternatif. Cette différence sera le bénéfice découlant de la mesure proposée. Après avoir mesuré les bénéfices, les scénarii alternatifs doivent identifier les coûts directs et indirects découlant de chaque mesure, et comparer ces coûts avec ceux du scénario de référence. Pour évaluer les coûts indirects, et notamment les coûts liés à l'impact sur les droits fondamentaux, la thèse propose une graduation qualitative pour caractériser le niveau d'impact : Impact "très élevé", "élevé", "moyen" ou "faible". Ce système permettra d'éliminer certaines propositions, par exemple toute proposition qui conduirait à un impact "très élevé" sur la liberté d'expression ou sur la protection de la vie privée. Ce système permettra en outre d'identifier les mesures qui créent l'impact le plus faible sur les droits fondamentaux. Bien qu'il soit impossible de quantifier ces coûts en termes monétaires, cette approche permet d'éliminer certaines propositions, et pour d'autres de rendre les contreparties plus explicites. Par exemple, l'analyse coûts/bénéfices pourrait révéler que la proposition A conduit à un bénéfice net pour la société de €100 millions par an par rapport au scénario de référence, et que la proposition B conduit à un bénéfice net pour la société de €80 millions par an par rapport au scénario de référence, sans toutefois prendre en compte les coûts non-quantifiables. La proposition A crée une interférence "élevée" avec la neutralité de l'internet, alors que la proposition B crée une interférence "faible" avec la neutralité de l'internet. Le régulateur pourra alors effectuer un choix plus explicite entre les deux propositions, sachant que l'option qui préserve la neutralité de l'internet crée un coût supplémentaire de €20 millions par an.

Etape 3 est une consultation publique pour recueillir des commentaires sur le questionnaire et sur l'analyse coûts/bénéfices.

Etape 4 est la soumission de l'étude d'impact (questionnaire plus analyse coûts/bénéfices) à un comité de lecture indépendant. Une contre-expertise de l'étude d'impact par des personnes indépendantes est essentielle pour plusieurs raisons. D'abord, le régulateur qui conduit l'étude d'impact peut avoir un conflit d'intérêts. Il sera influencé par le résultat souhaité par sa hiérarchie, et/ou par les décideurs politiques. Ensuite, une revue indépendante permettra le partage des meilleures pratiques sur le plan national et international. A l'instar du système utilisé pour revoir les propositions de régulation en matière de communications électroniques, un comité centralisé pourra dégager une liste de bonnes pratiques à partir de l'ensemble des notifications qu'il reçoit. Cela conduira à une meilleure efficacité, car les régulateurs réutiliseront des techniques qui ont bien fonctionné à l'étranger.

Après la revue de la mesure par le comité de lecture indépendant, la mesure pourra être adoptée.

Etape 5 consiste en la revue périodique des mesures après leur mise en application, afin de mesurer le niveau de coûts et bénéfices réalisés comparé aux projections initiales. Cette étape est également utilisée dans le domaine de la régulation des communications électroniques, pour s'assurer que des mesures de régulation sont toujours bien adaptées à la situation du marché. Les mesures mal adaptées sont modifiées ou retirées.

Chapitre 7 – Conclusion

L'objectif de cette méthodologie est d'apporter plus de rigueur dans le processus d'élaboration de règles visant le blocage de contenus sur internet. Les analyses coûts/bénéfices sont appliquées en matière de régulation de l'environnement et en matière de régulation des communications électroniques. Cependant, pour les mesures visant les contenus illicites sur internet, de telles analyses sont rares, et ne tiennent pas généralement compte des coûts indirects sur les droits fondamentaux et sur l'écosystème de l'internet.

Cette thèse contribue au progrès des connaissances scientifiques dans le domaine de l'économie de la régulation de l'internet. Elle explicite les facteurs sociaux, institutionnels et technologiques qui tendent à rendre une régulation dans le domaine de l'internet bénéfique, ou au contraire inutile voire nocive, pour la société. Une approche scientifique est déjà utilisée en matière de régulation pour la protection de l'environnement aux Etats-Unis, et en matière de régulation des communications électroniques en Europe. Mais la démarche est inédite pour la régulation des contenus sur internet. En général, l'élaboration de normes dans ce domaine échappe à une analyse des coûts et bénéfices en raison, d'une part, du caractère politiquement sensible du sujet (protection des enfants, lutte contre le terrorisme…), et, d'autre part, de la difficulté de mesurer les effets qu'une régulation peut avoir sur les droits fondamentaux et sur l'écosystème de

l'internet. L'une des contributions de la thèse est de proposer une méthode pour évaluer l'impact bénéfique ou néfaste sur les droits fondamentaux découlant de différentes approches de régulation, ce qui n'a pas été fait jusqu'à présent à ma connaissance.

La méthode d'analyse proposée dans la thèse n'est pas destinée à remplacer la démarche intuitive et parfois émotionnelle de la décision politique, mais plutôt de la compléter, en exigeant une étude d'impact rigoureuse avant la prise de décision. La thèse propose une feuille de route pour cette étude d'impact.

Le chapitre 7 identifie enfin les sujets qui méritent des recherches supplémentaires, comme par exemple une approche pour quantifier des atteintes aux droits fondamentaux. De nombreux travaux ont été consacrés au problème de la quantification de la valeur de la vie humaine ou de la préservation de l'environnement naturel. Ces approches pourraient être transposées au problème des atteintes aux droits fondamentaux, ce qui conduirait à une application plus aisée des analyses coûts/bénéfices.