

# Freedom in the Days of the Internet

Regulating, Legislating and Liberating  
the Internet While Protecting Rights  
and Unlocking Potentials

Bart Schermer and Ton Wagemans





# Freedom in the Days of the Internet

Regulating, Legislating and Liberating  
the Internet While Protecting Rights  
and Unlocking Potentials

Bart Schermer and Ton Wagemans



Deutsche Post DHL



The direct financing of CES publications which supports specific research or the presentation of a CES publication will be considered sponsored research. The arrangement shall not:

- inhibit free dissemination of results of scholarly activity and research or;
- stipulate any predetermined result or policy stance, either personally or institutionally.

## CREDITS

Centre for European Studies  
Design: RARO S.L.  
Printed in Brussels by Drukkerij Jo Vandenbulcke  
Brussels  
Centre for European Studies  
Rue du Commerce 20  
Brussels, BE – 1000

The Centre for European Studies (CES) is the official think-tank of the European People's Party (EPP) dedicated to the promotion of Christian democrat, conservative and like-minded political values.

For more information please visit:

[www.thinkingeurope.eu](http://www.thinkingeurope.eu)

This publication receives funding from the European Parliament.

© Centre for European Studies 2010

Photos used in this publication: Centre for European Studies 2010

The European Parliament and the Centre for European Studies assume no responsibility for facts or opinions expressed in this publication or their subsequent use. Sole responsibility lies on the author of this publication.

## Management Summary

Over the past three decades, Europe has transformed itself from an industrial society into an information society. In particular the rise of the Internet has been instrumental in this transformation. The Internet has opened up new possibilities for economic activity, innovation, social interaction and democratic participation. However, it has also given rise to new societal issues such as cybercrime, invasion of privacy, the curbing of free speech and infringement of intellectual property. These issues raise moral, ethical and legal questions. The goal of this study is to examine these issues in light of the current technological, economic and societal developments.

### Technological trends

The pace of innovation on the Internet is rapid. Broadband and the roll-out of next-generation networks have spurred the development and growth of new online services, which, in turn, have fuelled the demand for more broadband capacity. Stimulating this virtuous circle is a key goal of the 'Digital agenda for Europe'.<sup>1</sup> The rapid adoption of broadband and the convergence of infrastructures such as telephony and television with the Internet have allowed for the development of a host of new applications and services. The new applications and services are significantly changing the way we use the Internet. In just a few years' time, the

---

<sup>1</sup> European Commission, 'A digital agenda for Europe', Communication, COM(2010) 245, Brussels, 19 May 2010.

Web, which is often equated with the Internet, has changed from a passive information source into a medium that allows for active user participation (Web 2.0). The next step in the development of the Internet is that it will be available, at any time and place, through mobile Internet, cloud computing and ubiquitous computing. In the near future we will live in the Internet, rather than go *on* the Internet.

## Societal trends

The Internet has already had a significant impact, and its further evolution will no doubt continue to influence our society, culture and economy. We can clearly see its influence in the changing behaviour and expectations of users. Because the Internet permeates our daily lives, we now to expect to be able to access relevant and context-sensitive information wherever and whenever we please. Context-sensitive information is accessed through applications (apps) on mobile devices such as smart phones and tablets, and through connected appliances such as radios, televisions and even refrigerators. We can already see that Internet traffic is shifting away from the traditional World Wide Web towards these mobile applications. While this new on-demand culture, in which information is always available, is of great benefit to consumers and businesses, it also poses new ethical and legal questions—for instance, regarding the right to privacy and intellectual property. Moreover, it changes the balance of power on the Internet, shifting more influence towards companies in control of the hardware, content platforms and operating systems running these applications. The Internet has also had a substantial impact on business and business models. Supply chain management systems, for instance, have merged with the

Internet, making logistics more effective, efficient and transparent. That has allowed for the creation of new integrated business models in both business-to-business and business-to-consumer relations. The 'Internet of Things' is set to change logistics, supply chain management, retail and marketing even further. Technologies such as RFID (Radio Frequency Identification) and 2D barcodes promise to reduce costs, stock depletion, theft and CO2 emissions, while at the same time making shopping easier, more personalised and more fun for consumers. However, these same technologies also raise questions about privacy and data protection.

A second trend is the changing role of users. Web 2.0 has enabled users to actively participate on the Internet. User-generated content, crowdsourcing and co-creation act as catalysts for culture and creativity, but they also raise questions about intellectual property and freedom of expression.

A third trend is that the Internet is no longer a 'cyberspace' that is disconnected from our physical world. To an increasing extent the Internet surrounds us in our daily lives. Ubiquitous computing and mobile Internet will bring us the Internet of Things, while augmented reality allows us to project a virtual layer of information over our physical world. Furthermore, the exchange of virtual goods in virtual worlds means that our real economies are mixing with those of virtual worlds, raising questions about privacy, freedom of expression and intellectual property.

A last trend that deserves mention is our increased dependency as a society on the Internet. The Internet has become a critical infrastructure for the future of Europe and

an integral part of everyday life. Its disruption could have serious (economic) consequences. Furthermore, dependency creates vulnerability; our dependence can be exploited by malevolent parties such as cybercriminals.

## Regulating the online world

Technological trends and the societal changes that accompany them have had a profound influence on Europe. Given the importance of the Internet for European society and the economy, regulation of online behaviour is necessary. The nature of the Internet, however, poses significant challenges for effective regulation. A first is anonymity. While anonymity allows people to express their thoughts and feelings without fear of persecution, the anonymous nature of the Internet can also be abused by cybercriminals. A second challenge is the boundless nature of the Internet. Because it does not occupy physical space and thus has no borders, attempts to regulate the behaviour of Internet users often run into issues of competing sovereignty and jurisdiction. A third challenge is posed by 'technological turbulence'. Because of the rapid pace of innovation and development on the Internet, any regulatory approach is bound to lag behind technological reality, leading to friction and legal uncertainty. A final challenge is posed by the fact that the networks, services, content and applications that comprise the Internet are for the most part supplied by private entities whose interests are varied and may not always align with each other or with those of the regulator. All of these characteristics make regulating online behaviour a very difficult task indeed. Most if not all of the online dilemmas described in this report have their roots in these regulatory challenges.

Regulating (or not regulating) the Internet may affect the interests and rights of different actors in society.<sup>2</sup> In order to keep the Internet an open communication infrastructure for vibrant social interaction as well as an engine for economic growth in Europe, we must ensure that the values and norms of the European Union (EU) are reflected in this infrastructure. Important regulatory goals for the Internet are based on values such as trust, safety, security, freedom, innovation, equality, fairness, reciprocity and decency. From these values we may deduce three primary regulatory goals:

1) to stimulate trust in the infrastructure, platforms and services that make up the Internet by ensuring a secure, safe and fair online environment;

2) to ensure that fundamental rights and liberties are protected in an online environment;

3) to create an open and level playing field for economic actors that stimulates growth and innovation.

When it comes to describing the different options for regulating the Internet, we may distinguish four different approaches: self-regulation, state regulation, co-regulation and regulation through digital architecture (code as law). Each of these regulatory approaches has particular strengths and weaknesses.

---

<sup>2</sup> When we talk about 'regulating the Internet', we refer to the regulation of the online ecosystem (e.g. the behaviour of end users and other online actors), rather than the regulation of the technological infrastructure itself.

Self-regulation was the predominant mode of regulation when the Internet was still in its infancy. But as the Internet has matured and grown in size, scope and importance, questions about the limits of self-regulation, most notably its voluntary nature, have been raised. Given the Internet's importance for European society and the economy, state-issued regulation is now the most important mode of regulating the online ecosystem. However, the borderless nature of the Internet and the fact that most of the infrastructure is in the hands of private entities also impose significant limits on the effectiveness of state regulation. A third option is co-regulation. In this approach the government sets the boundaries of the legal framework, which is then filled in by the relevant actors. The co-regulatory approach thus combines aspects of self-regulation and state-issued regulation. While co-regulation can be an effective option for regulating the behaviour of users online, its effectiveness is dependent on the participation of all the actors involved. A final mode of regulation is regulation through architecture. By regulating the behaviour of actors online through technology, enforcement of rules may be more certain. However, implementing law in computer code is challenging and may present risks to further investment and innovation. Moreover, 'code as law' solutions may be at odds with fundamental human rights such as privacy and freedom of speech. Examples of the 'code as law' approach are filtering and blocking, digital rights management and mandated net neutrality.

Regulating the Internet may affect the rights and interests of actors in the information society, including the safety and security of citizens online, the right to privacy, freedom of expression, the right to (intellectual) property and the free

and correct functioning of the internal market. The most important question when it comes to regulating the online world is how we balance different rights and interests, and how we can ensure the greatest freedom online for individuals, groups and organisations without harming the rights and freedom of others and the good of society as a whole, for example security and economic growth.

## Online dilemmas

In this report we identify four online dilemmas in which the issue of effective regulation and the balancing of different rights and interests feature prominently. They are innovation, freedom of expression, privacy and intellectual property.

### Innovation

The Internet is a key driver of the future prosperity of Europe. Building an online ecosystem that optimally facilitates the development (and subsequent consumption) of new applications and services is thus a key policy objective for Europe. Important challenges in this area are the creation of a single digital market and the question of which approach is best for stimulating an open and competitive online environment.

The first challenge is to create a truly single digital internal market for Europe. Currently the European market is too fragmented, stifling innovation and hindering cross-border e-commerce transactions. Further harmonisation of national and EU legislation is therefore necessary.<sup>3</sup>

---

<sup>3</sup> See Single Market Act – Frequently Asked Question, MEMO/10/528, 27 October 2010.

The second challenge is to determine whether *ex ante* legislation is necessary to keep the Internet a free and open environment, or whether a more targeted legal approach with *ex post* enforcement is more prudent. This question is central to the discussions about net neutrality and interoperability.

Net neutrality is the idea that an information network should aspire to treat all content, sites and platforms equally.<sup>4</sup> While both proponents and opponents of net neutrality agree that to be an optimal climate for innovation, the Internet should be an open environment, they disagree on what is the most effective regulatory mechanism to ensure that openness. Those in favour of net neutrality argue that mandating network operators not to influence the flow of data on their networks (i.e., net neutrality) is the only way to ensure an open online ecosystem. Opponents of net neutrality argue that it is ineffective and unnecessary and that it upsets the free market. They believe that ensuring the integrity and trustworthiness of the networks, quality of service and effective congestion management in the face of rising consumption requires traffic management practices and the ability to provide tiered service offerings. All of this, they hold, can be achieved without compromising consumers' basic right to unfettered broadband Internet access. Given that any policy choice on net neutrality may have far-reaching consequences for innovation in Europe, it is necessary to explore all possible options. Alternatives to mandated net neutrality include transparency and competition, as well as effective supervisory powers should abuses of a dominant position be detected. Moreover, in discussing neutrality rules on the Internet, we should also

---

<sup>4</sup> T. Wu, 'Network neutrality FAQ'; available at [http://timwu.org/network\\_neutrality.html](http://timwu.org/network_neutrality.html).

take into account the changing nature of Internet services and use in Europe and the possible shifts in the balance of power and influence between ISP, content delivery networks and large Internet content companies. Because incidents are few and for the most part have been solved without the need for regulatory intervention, the Body of European Regulators for Electronic Communications (BEREC) believes that, at present the existing legal framework provides adequate protection for users. As such, BEREC argues that further regulatory intervention with respect to net neutrality is not necessary at this point.<sup>5</sup>

When it comes to interoperability, a first challenge is that the European standardisation process is often too slow to keep up with the rapid pace of development on the Internet. Therefore, the European Commission is currently modernising its standardisation policy. A second challenge is how to ensure that companies do not use de facto standards in a manner that implies unfair competition. The Commission is currently contemplating the idea of imposing *ex ante* legislation in order to ensure openness and interoperability. This approach is controversial, however, as it may lead to legal uncertainty and may influence the free market (i.e., the freedom of businesses) to a significant degree.

## Freedom of expression

Freedom of expression is a fundamental human right and a prerequisite for our democratic society. The Internet has been a great stimulus to freedom of speech in Europe,

---

<sup>5</sup> Body of European Regulators for Electronic Communications, 'BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe', BoR (10) 42, 30 September 2010.

because it allows people to easily voice their opinions (possibly anonymously), connect with other users, make direct contact with their elected representatives and find information online. At the same time, however, the Internet also allows for freedom of expression to be abused, and it opens up new possibilities for criminal behaviour.

Law enforcement on the Internet is a prerequisite for a safe and secure online environment, but at times it may be at odds with freedom of expression. Freedom of expression is a particular concern when technical measures such as filtering and blocking are considered by policymakers. Given the impact filtering and blocking may have on the free flow of information and the right to privacy particular care needs to be taken in their implementation. First of all, effectiveness should be assessed. Second, we must consider whether their application passes the tests of proportionality and subsidiarity. Options that are less far reaching may include strengthening traditional law enforcement, creating public-private partnerships and strengthening international cooperation procedures for mutual legal assistance and criminal prosecution. Finally, we must take into account the risks of the slippery slope and those of function and mission creep.

## **Privacy**

The Internet creates both opportunities for and threats to the privacy of users. The relative anonymity of the Internet protects users' privacy, but at the same time vast amounts of personal data are stored daily, with or without the consent of users. Privacy in general and the protection of personal data in particular are therefore key issues when it comes to freedom online. It is important to recognise that while

privacy is a right in itself, it is often more a means than an end. Privacy protects, among other things, our individuality, freedom and reputation. By separating contexts, shielding information from third parties and limiting the processing of personal data to those instances where it is necessary, we can protect privacy.

While privacy is a fundamental right, it is not absolute. The amount of privacy granted to an individual must always be balanced against society's need for openness and disclosure. Ideally, individuals should be able to enjoy the maximum amount of privacy, but there are instances where the legitimate interests of society (for instance, public health or security) may outweigh the individual's right to privacy. Moreover, we must acknowledge that (personal) data is the lifeblood of the information society and that without the ability to process personal data, it would be impossible to operate many of our modern information services.

In order to preserve privacy and stimulate the free flow of personal data, we must raise awareness about privacy issues, heighten transparency, strengthen oversight, employ mechanisms for privacy by design and put users in control of their personal data. Finally, we must continue to rethink privacy legislation in order to keep up with technological and societal developments.

## **Intellectual property**

The Internet and digitisation have radically altered the landscape for the creation and distribution of content. Movies, music, games, software and e-books can be copied and distributed at minimal cost and without loss of quality. While the Internet has revolutionised content creation and

distribution, it has also had a negative side effect in that intellectual property infringement now takes place on a massive scale, putting severe stress on intellectual property and its enforcement. For a knowledge-based economy such as Europe's, the creation and free flow of information is of vital importance. We must therefore create an environment that stimulates the creation and consumption of content. To create such an ecosystem online, we must ensure the protection of intellectual property while also ensuring the free flow of information.

Stimulating the development of new business models is necessary for the creation of a market for legal content that suits consumer needs and wishes. In order to facilitate the growth of new business models, we must strengthen and harmonise the internal market, combat piracy and illegal file sharing and look for alternative compensation mechanisms. Furthermore, creators need to be enabled to protect, market and monetise their works using mechanisms such as the Creative Commons, content platforms and easy-to-use (micro) payment schemes. Such an approach is not limited to professionally created content but is also applicable to user-generated content.

## Conclusion

Our modern-day Internet is an environment that allows for great freedom, but with freedom comes responsibility. If we want to keep the Internet an open, safe, and vibrant online environment, we must ensure that we take into account and protect the rights and interests of all members of society. The greatest challenge for Europe is to ensure the highest degree of (online) freedom for all. This means balancing the

rights and interests of individuals, groups and institutions with those of others as well as with the general good of our society. In balancing these rights, we must make sure that we do not play a zero-sum game, whereby values are exchanged for one another. Rather, we must aim to ensure that these values are maximised to the greatest extent possible. For instance, we must not exchange privacy for security, but seek an approach that strengthens security while maintaining privacy. In those cases where values do compete with each other, a political choice needs to be made.

In this study the Centre for European Studies endeavours to provide a general overview of the legal, moral and ethical questions that may arise in attempts to regulate the online world. While possible solutions and policy options for the various online dilemmas are tentatively offered, no political answers are formulated. The reason for this is that fair and effective regulation is very much context dependent. This study can be used as a basis to explore the different dilemmas further and to formulate more detailed political positions on the individual issues.



# Table of Contents

|  |           |
|--|-----------|
| <b>1 Introduction</b> .....                        | <b>20</b> |
| 1.1 Problem Statement and Goal .....               | 20        |
| 1.2 Research Questions .....                       | 21        |
| 1.3 Research Approach .....                        | 22        |
| <b>2 Trends in Technology and Services</b> .....   | <b>23</b> |
| 2.1 Next Generation Networks .....                 | 23        |
| 2.2 Convergence .....                              | 24        |
| 2.3 Web 2.0, Cloud Computing, Web 3.0 .....        | 24        |
| 2.4 Virtual Worlds .....                           | 26        |
| 2.5 Ubiquitous Computing .....                     | 27        |
| <b>3 Societal Changes</b> .....                    | <b>28</b> |
| 3.1 Changing Services .....                        | 28        |
| 3.2 Changing Roles of Users .....                  | 30        |
| 3.3 Mixing of the Physical and Virtual Space ..... | 32        |
| 3.4 Increased Dependency on the Internet .....     | 32        |
| <b>4 Regulating the Internet</b> .....             | <b>33</b> |
| 4.1 How to Regulate the Internet? .....            | 35        |
| 4.1.1 Internet Architecture .....                  | 35        |
| 4.1.2 Regulatory Challenges .....                  | 39        |
| 4.1.3 Regulatory Approaches .....                  | 41        |
| 4.2 Freedom and the Internet .....                 | 46        |
| <b>5 Innovation and the Internet</b> .....         | <b>49</b> |
| 5.1 Background .....                               | 49        |
| 5.2 Challenges .....                               | 51        |
| 5.2.1 Net Neutrality .....                         | 52        |

- 5.2.2 Lack of a Single (digital) Market ..... 57
- 5.3 Interoperability ..... 57
- 5.4 Possible Solutions ..... 60
  - 5.4.1 Net Neutrality: Free Market or *ex-ante* Regulation? ..... 60
  - 5.4.2 Harmonisation and the Single Market ..... 64
  - 5.4.3 Interoperability: Free Market or *ex-ante* Regulation ..... 65
- 6 Freedom of Expression and the Internet ..... 68**
  - 6.1 Background ..... 68
    - 6.1.1 Notice and Takedown ..... 69
    - 6.1.2 Blocking and Filtering ..... 71
  - 6.2 Challenges ..... 74
    - 6.2.1 Effectiveness of Filtering ..... 74
    - 6.2.2 Proportionality and Subsidiarity ..... 75
    - 6.2.3 The Slippery Slope ..... 75
    - 6.2.4 Filtering and Foreign Policy ..... 76
    - 6.2.5 Filtering and Net Policy ..... 77
  - 6.3 Possible Solutions ..... 77
    - 6.3.1 International Cooperation ..... 77
    - 6.3.2 Public-Private Partnerships ..... 78
    - 6.3.3 Checks and Balances ..... 78
- 7 Privacy and the Internet ..... 79**
  - 7.1 Background ..... 79
    - 7.1.1 The Right to Privacy ..... 80
    - 7.1.2 Informational Privacy and Data Protection . 81
    - 7.1.3 The Limits of Privacy ..... 82
  - 7.2 Challenges for Europe ..... 83
    - 7.2.1 Persistence and Reputation ..... 83
    - 7.2.2 Context- and Audience Separation ..... 84
    - 7.2.3 Privacy, Dignity and Personal Autonomy .. 85

|           |   |            |
|-----------|---|------------|
| 7.2.4     | Digital Footsteps                               | 86         |
| 7.2.5     | Globalisation of Privacy Issues                 | 87         |
| 7.3       | Possible Solutions                              | 87         |
| 7.3.1     | Awareness                                       | 87         |
| 7.3.2     | Transparency and Control                        | 88         |
| 7.3.3     | Accountability and Enforcement                  | 89         |
| 7.3.4     | Privacy by Design                               | 90         |
| 7.3.5     | Rethinking Privacy                              | 90         |
| <b>8</b>  | <b>Intellectual Property and the Internet</b>   | <b>91</b>  |
| 8.1       | Background                                      | 91         |
| 8.2       | Challenges                                      | 93         |
| 8.2.1     | (Illegal) File Sharing and Copyright            | 93         |
| 8.2.2     | Enforcing Copyright in a<br>Digital Environment | 95         |
| 8.2.3     | Digital Rights Management                       | 98         |
| 8.2.4     | Slow Emergence of New Business Models           | 98         |
| 8.2.5     | User Generated Content                          | 100        |
| 8.3       | Possible Solutions                              | 101        |
| 8.3.1     | Stimulating New Business Models                 | 101        |
| 8.3.2     | A Single Digital Market                         | 102        |
| 8.3.3     | Enforcement of Intellectual Property            | 102        |
| 8.3.4     | Alternative Compensation Mechanisms             | 105        |
| 8.3.5     | Unlocking the Creative Potential of Users       | 106        |
| <b>9</b>  | <b>Conclusions</b>                              | <b>108</b> |
| <b>10</b> | <b>Bibliography</b>                             | <b>110</b> |
| 10.1      | Literature                                      | 110        |
| 10.2      | Official Publications                           | 116        |
| 10.3      | Speeches  | 116        |
| <b>11</b> | <b>Appendix: Glossary</b>                       | <b>117</b> |

# 1 Introduction

In only a few decades, the Internet has become an integral part of life in Europe. A network of networks, it drives economic growth and innovation, brings people together and creates opportunities for fulfilling their goals and potential. The European Commission (EC) sees the Internet as a critical part of Europe's future. Developing Europe as an information society is one of its seven flagship initiatives under the *Europe 2020* strategy,<sup>6</sup> and the EC has outlined its strategy in the 'Digital agenda for Europe'.<sup>7</sup> The agenda includes seven priorities for action: a) creating a digital single market; b) improving the framework for interoperability between Information and Communications Technology (ICT) products and services; c) boosting Internet trust and security; d) guaranteeing the provision of speedier Internet access; e) encouraging investment in research and development; f) enhancing digital literacy, skills and inclusion; and g) using ICT to address challenges such as climate change, rising health care costs and the ageing population. To achieve those goals, a sustainable legal framework is necessary.

## 1.1 Problem statement and goal

If it is to achieve the ambitious goals set forth in the 'Digital agenda for Europe' and ensure growth, prosperity, freedom and security, Europe faces important policy choices, many of them likely to involve regulating the online environment.

---

<sup>6</sup> European Commission, 'Europe 2020: a strategy for smart, sustainable and inclusive growth', Communication, COM(2010) 2020, Brussels, 3 March 2010.

<sup>7</sup> European Commission, 'A digital agenda'.

Regulating the Internet—or failing to—may affect the freedom of individuals, groups and organisations. Thus, a careful study of the possible effects of regulation is critical.

In this paper, the Centre for European Studies (CES) will explore Internet regulation, focusing on the issue of freedom. We will look at the various actors and interests involved and examine how regulatory choices are likely to affect them. The goal of this study is to inform decision-makers and policymakers about the possibilities for and limitations of Internet regulation.

The main problems to be explored are twofold:

1. What are the moral, political and legal dilemmas posed by the Internet in the context of contemporary technological, economic and social developments?
2. What are the options for Internet regulation, and what are their consequences?

## 1.2 Research questions

In approaching these problems, we will attempt to answer the following questions:

- What are the current technological trends?
- What are the related social trends?
- Which moral and legal issues might arise out of those developments?
- How will regulation affect different rights and interests?

## 1.3 Research approach

The goal is to provide an overview of the questions raised in an examination of freedom and the Internet, so this study is exploratory and explanatory in nature. Using a literature study, we itemise various aspects of regulation and explain their relevance to the issue of freedom on the Internet.

The report is divided into two parts. The first provides background information on the future development of the Internet, the social changes that will likely accompany it and the possibilities for and limits of regulation. The second looks at four topics that raise ethical, legal and political questions: innovation, freedom of expression, privacy and intellectual property.<sup>8</sup>

In chapter two we explore relevant technological trends, and in chapter three, explain their social impact. Chapter four is devoted to a discussion of the possibilities for and limitations of Internet regulation, as well as questions about freedom. In chapters five through eight, we deal with some of the key topics raised, and examine what moral and legal questions arise and how regulation might affect the rights and interests of those involved. Chapter nine presents our conclusions.

---

<sup>8</sup> Since this study is primarily concerned with freedom and the effects online regulation, it does not cover important topics such as the digital divide, media literacy and digital sustainability.

## 2 Trends in technology and services

In this chapter we describe the technological trends relevant to developing the Internet in Europe, forecasting about 5 to 10 years into the future, while continuing to focus on current developments.

### 2.1 Next generation networks

In her ‘Digital agenda for Europe’, Commissioner Kroes set the ambitious goal of providing all Europeans citizens with Internet speeds of 30 Mbps or more by 2020, with half of European households subscribing to connections of 100 Mbps or more. Achieving that goal implies substantial investment in broadband connections.

Over the next few years, we will see the deployment of high-speed, fixed-line infrastructure, much of which will provide fibre connections to the ‘curb’ and even the home (FttC, FttH). We will also see a strong growth in wireless infrastructure. With the arrival of third-generation mobile networks (3G) and Internet-friendly mobile platforms such as smartphones, netbooks and tablets, the use of mobile broadband has skyrocketed in Europe.<sup>9</sup> That trend is set to continue well into the future with the development of 4G networks and WiMax.

Broadband connections will supply European citizens with the speed for data-sensitive applications and services

---

<sup>9</sup> International Telecommunications Union (2010), *Measuring the Information Society*, version 1.0.1

such as Video on Demand (VOD), Internet Protocol television (IPTV) and next-generation computer games. Apart from those consumer-oriented services and applications, broadband and next-generation networks will provide citizens, businesses and public institutions with the bandwidth for professional ‘telepresence’ applications and services. Examples include distance health care, high-quality videoconferencing and the ability to work from home.

## 2.2 Convergence

The convergence of telecommunications infrastructure and services is a trend that started several years ago. Its most visible aspect is Triple Play Packages, in which traditional telecom operators and cable companies combine television, Internet and voice telephony. The convergence of telecommunications infrastructure and the switch to IP (Internet Protocol) for all services will have a profound impact on the Internet, making it increasingly difficult to distinguish between the classic Internet, television, mobile Internet and other forms of telecommunication.

It is important to note that convergence will not only take place on the infrastructure level (i.e. the switching to all-IP networks) but also at the application and service level through interoperable services and application programming interfaces (APIs).

## 2.3 Web 2.0, Cloud Computing, Web 3.0

Until a few years ago, the World Wide Web was predominantly a static information source. Users could go

online and retrieve information, but participation and interaction were limited. Only tech-savvy users with the knowledge to build a website were able to express themselves online. With the arrival of broadband connections and new standards and programming tools—Extensible Markup Language (XML), Asynchronous JavaScript and XML (AJAX) and Simple Object Access Protocol (SOAP)—it became possible to create websites that allow for much more user interaction, leading to what is now called Web 2.0.

## Web 2.0

Web 2.0 is the buzzword for the evolution of the Web from a static medium to one focused on user participation, creation and collaboration. Thanks to Web 2.0 applications and platforms, such as YouTube, Facebook, Wordpress, Wikipedia and Flickr, users can express themselves and share their thoughts, pictures, movies and music.

## Cloud Computing

Closely linked to the development of Web 2.0 is that of Cloud Computing. While consumer-oriented platforms such as YouTube, Twitter and Facebook capture the public's imagination, the trend that has services moving into the 'Internet cloud' is easily as important for the future of Europe. Cloud computing is a fashionable name for Internet-based computing. Instead of having all computer resources available locally—fast computers, hard drives, software, etc.—the user gets the resources from service providers on the Internet, i.e., from the cloud.<sup>10</sup> An important benefit is that the end user

---

<sup>10</sup> Software as a Service (SaaS), Platform as a Service (PaaS) and Hardware as a Service (HaaS) can be seen as examples of cloud computing services.

needs neither expensive equipment nor deep computing knowledge. Moreover, users can have the same information available across a number of hardware platforms, such as smartphones, desktop computers, laptops and tablets.

### **Web 3.0**

Web 3.0 will be the next stage in the evolution of the Internet. While definitions for Web 3.0 vary wildly, a recurring theme is the ability of computers to understand natural language, which would enable us to communicate with the Internet in a more natural and intuitive way. Instead of typing words in a search query, for instance, we could type a full sentence that would be understood by computers.

## **2.4 Virtual worlds**

Increased computing power and broadband make it possible to render three-dimensional virtual worlds. Millions of people interact, socialise and play in virtual worlds, of which there are two: the Massive Multiplayer Online Games (MMOs) and the worlds aimed at social interaction and creation, the Multi-User Virtual Environments (MUVES). Popular examples of MMOs include World of Warcraft, Lineage, Guild Wars, EVE and Lord of the Rings. Popular MUVES are Second Life, Project Entropia and Habbo Hotel.

Virtual worlds often mimic conditions in the physical world, such as scarcity. Virtual scarcity leads to the establishment of virtual economies in which players trade goods and services for virtual currency. But virtual currencies can be exchanged for real money, mixing the virtual with the real economy.

## 2.5 Ubiquitous computing

Moore's law states that transistor density will double roughly every two years. The exponential growth of computing power, including storage capacity, broadband capacity and memory, has combined with another trend, miniaturisation, to allow the integration of computing power into everyday objects, from cars to thermostats. Thus computing is ever more pervasive. The notion that computing power will spread into every corner of our physical world has been labelled 'ubiquitous computing' or 'pervasive computing' by computer scientists.

All these objects will eventually be networked, creating an 'Internet of Things'. Communication in this Internet of Things will be not merely between people, but also between people and machines and even just between machines (M2M). One step beyond an Internet of Things is the idea of ambient intelligence. In that vision, we will be surrounded by a digital infrastructure that is context-aware and able to intelligently interact with us, possibly even anticipating our needs and wishes and acting accordingly.

While such services may seem like visions from a distant future, their first contours are already visible. Geolocation applications on mobile phones, public-transport tickets using radio-frequency identification (RFID), smart energy meters and intelligent cars are their first manifestations. What is relevant for this report is that with the development of ubiquitous computing, we will live *in* the Internet rather than go *on* the Internet.<sup>11</sup>

---

<sup>11</sup> C. van 't Hof, R. van Est and F. Daemen (eds.), *Check in / Check out: Public Space as an Internet of Things* (Rotterdam: NAi Publishers, 2011).

## 3 Societal changes

In this chapter, we describe social changes driven by technological development and/or inspired by it. New technologies, services and social change are processes that influence each other. A technological development may change society, or society may fuel the development of new technologies and services. That interaction is not our focus. We want to describe significant social changes that are already observable and their impact on the future of European citizens and businesses.

### 3.1 Changing services

The Internet has created significant changes for businesses over the past two decades. It is used both as a medium to support traditional processes, such as Electronic Data Interchange, Supply Change Management and electronic invoicing, and as a platform for new services, including electronic commerce, online social platforms, cloud computing and search engines. That has made it an important driver of economic growth in Europe. The value added of the ICT industry on the European economy is about €600 billion (4.8% of GDP). Almost half of the productivity gains over the past 15 years can be attributed to ICT,<sup>12</sup> and research estimates that broadband development will create 345,000 to 2,112,000 jobs between 2006 and 2015.<sup>13</sup>

---

<sup>12</sup> J. Van Reenen et al., *The Economic Impact of ICT* (London: London School of Economics, 2010).

<sup>13</sup> M. Fornefeld, G. Delauney and D. Elixmann, *The Impact of Broadband on Growth and Productivity* (Düsseldorf: Micus Consulting, 2008).

The Internet has had a significant impact on traditional businesses and models. Supply-chain management systems, for instance, have merged with the Internet, making logistics more effective, efficient and transparent. That has allowed for the creation of new, integrated business models both in business-to-business and business-to-consumer relations. The Internet of Things is set to change the environment even more. Technologies such as RFID and 2D barcodes promise to reduce costs, out-of-stock shortages, theft and CO2 emissions, while at the same time making shopping easier, more personalised and more fun for consumers.

The Internet has also allowed for the creation of new services, including e-commerce sites, auction sites, digital content stores, cloud computing, virtual worlds, mobile-commerce, social networking platforms and interactive advertising.<sup>14</sup> All of those services give users almost instant access to information, goods and services.

User behaviour and expectations have been significantly altered by those developments. Users demand that information, services, goods and entertainment be available on request 24/7. The Internet has, therefore, changed many markets from push to pull. That trend is likely to continue, because to an increasing extent, the Internet is always available, any place, any time. We are now surrounded by it, and use tablets, smart phones and networked appliances to access specific, context-sensitive information,<sup>15</sup> using

---

<sup>14</sup> Advertising drives many of the new Web 2.0 services. The Interactive Advertising Board estimates that the 'consumer surplus' derived from interactive advertising was 100 billion euros in 2010. See: McKinsey & Company, 'Consumers driving the digital uptake: the economic value of online advertising-based services for consumers', September 2010. Available at: [http://www.iab.net/insights\\_research/947883/consumers\\_driving\\_digital\\_uptake](http://www.iab.net/insights_research/947883/consumers_driving_digital_uptake)

<sup>15</sup> C. Anderson and M. Wolf, 'The Web is dead. Long live the Internet', *Wired* (online version), 17 August 2010, [http://www.wired.com/magazine/2010/08/ff\\_webrip/all/1](http://www.wired.com/magazine/2010/08/ff_webrip/all/1).

technologies such as mobile Internet, cloud computing and ubiquitous computing.

## 3.2 Changing roles of users

The typical user used to be a passive actor who accessed the Internet for information retrieval and communication through email or chat. With the arrival of Web 2.0, the role of the user has become participatory. That can clearly be seen in the boom of online creativity and the importance of the Internet as a discussion forum.

### Content 2.0

The high cost of making movies, music and photographs used to limit their production to professionals, but cheap and relatively easy-to-use tools have put creative power in the hands of every consumer.<sup>16</sup> Distribution platforms such as YouTube, Flickr, Vimeo, Picasa and MySpace allow users to easily distribute their content online. The result is that Web 2.0 is changing the user from a consumer to a ‘prosumer’. The creation of user-generated content (UGC) has exploded over the past few years. On YouTube alone, more than 24 hours of video are being uploaded every *minute*.<sup>17</sup>

Web 2.0 also allows users to collaborate in the creative process through crowdsourcing and co-creation.

---

<sup>16</sup> Examples include Adobe’s Photoshop Elements, Apple’s iMovie, Steinberg’s Cubase and Propellorheads’ Reason.

<sup>17</sup> [http://www.youtube.com/t/fact\\_sheet](http://www.youtube.com/t/fact_sheet).

Crowdsourcing aims to unlock popular wisdom by outsourcing to large groups of people tasks traditionally performed by employees or contractors. Companies and public institutions increasingly consult users in the development of goods and services. Users also actively collaborate in creating content. Wikipedia is the most visible example, and its success is so impressive, it has led to the development of Wikinomics, an economic idea based on openness, sharing and peering in a global context.<sup>18</sup>

## Democracy 2.0

The participatory nature of the Internet opens doors to the political process. Not only can citizens use it to learn more about political topics, it allows for grassroots participation.

An important tool for discussing political issues and for mobilising support, the Internet allows politicians, pressure groups and NGOs to directly engage with the public and amass followers. The Obama campaign team illustrated the power of the Internet in the 2008 US presidential election, carefully orchestrating and executing a Web 2.0 campaign to mobilise followers, raise funds and give voice to citizens' opinions and preferences.<sup>19</sup> More recently, the power of social media was used to turn the world's attention to the oppressive regime in Iran. In the wake of the 2009 Iranian presidential vote, Twitter, YouTube and other social media exposed the regime's violent reaction to opposition protests.

---

<sup>18</sup> D. Tapscott and A.D. Williams, *Wikinomics: How Mass Collaboration Changes Everything* (New York: Penguin Books, 2006).

<sup>19</sup> See [www.barackobama.com](http://www.barackobama.com) and [my.barackobama.com](http://my.barackobama.com).

### 3.3 Mixing of the physical and virtual space

Ubiquitous computing has mixed the physical world with cyberspace. The result is a perception of a world that contains elements from both.<sup>20</sup>

Augmented reality, one example, works by using technology to enhance the physical world through location-aware systems that layer networked information over our everyday perceptions.<sup>21</sup> Augmented reality integrates the digital and the physical worlds into a coherent whole.<sup>22</sup> The trade in virtual goods that occurs in virtual worlds and over social networks such as Facebook is another example. These virtual goods exist only in cyberspace, but they are paid for with real money, leading to a mixing of physical and virtual economies.

### 3.4 Increased dependency on the Internet

The Internet will continue to provide Europe with social and economic benefits, but its future development is not without risks. Our increasing dependence on the Internet and the mixing of the physical and virtual worlds are of particular concern.

The Internet is already a critical infrastructure for Europe. Without it, many activities would become impossible or at

---

<sup>20</sup> For excellent descriptions in fiction of this possible future see C. Stross's *Halting State* (New York: Ace Books, 2007) and *Rainbow's End* by V. Vinge (New York: Tor Books, 2006).

<sup>21</sup> J. Smart, J. Cascio and J. Paffendorf, 'Metaverse roadmap: pathways to the 3D web', Acceleration Studies Foundation 9, 2007.

<sup>22</sup> An example of augmented reality is the Layar Augmented Reality Browser (see: [www.layar.com](http://www.layar.com)).

least very difficult. We have grown dependent on the Internet, and the trend is likely to continue as we integrate it more and more into our lives.<sup>23</sup>

Dependence creates vulnerability, which can be exploited through various forms of abuse, from cyberwarfare, cyberterrorism and cyberactivism to cybercrime, all of which seriously threaten the freedom of European citizens online. Paradoxically, taking measures against those abuses, through filtering or far-reaching investigative powers, could have the same effect.

## 4 Regulating the Internet

In this chapter we describe the purpose and goals of Internet regulation and the ethical and moral themes underlying it.<sup>24</sup> We also examine possible modes of regulation: by law, self-regulation, co-regulation and through architecture.

Why regulate the Internet? The Internet has become an integral part of human life in Europe and a critical

---

<sup>23</sup> Those unable to access or use the Internet effectively will be at a serious disadvantage. The existence of a 'digital divide' between those who can afford modern computing equipment and Internet connections and those who cannot is a cause of concern. Another is that not everybody will be equally skilled in using the Internet (exclusion). While these topics are important, they are not the focus of this study and will therefore not be discussed further.

<sup>24</sup> It should be noted that when we talk about 'regulating the Internet' we are referring to the regulation of the online ecosystem (i.e. regulating the behaviour of end users and other actors online), rather than the regulation of the Internet as a technological infrastructure.

infrastructure for the economy and the safety and well being of citizens. Given its importance, there is an ever-louder call for regulating the online world. Society, without regulation, would be reduced to anarchy, described by Hobbes as the 'state of nature'.<sup>25</sup> Thus, regulation is a necessary technique for ordering society. Or as Kelsen describes it,

The living together of human beings is characterised by the setting up of institutions that regulate this living together. Such an 'institution' is called an 'order'... Society is ordered living together, or, more accurately put, society is the ordering of the living together of individuals. The function of every social order is to bring about certain mutual behavior of individuals; to induce them to certain positive or negative behavior, to certain action or abstention from action. To the individual, the order appears as a complex of rules that determine how the individual should conduct himself. These rules are called norms.<sup>26</sup>

To keep the Internet open for social interaction and as an engine of economic growth, we must ensure that the EU's values and norms are reflected in its infrastructure. Important regulatory goals for the Internet are based on values such as trust, safety, security, freedom, innovation, equality, fairness, reciprocity and decency. From those values, we may deduce three primary regulatory goals:

---

<sup>25</sup> T. Hobbes, *Leviathan: Or The Matter, Forme, & Power of a Common-Wealth Ecclesiasticall and Civill* (1651; repr. Harmondsworth: Penguin Classics, 1982).

<sup>26</sup> H. Kelsen, 'The law as a specific social technique', *The University of Chicago Law Review*, 9(1) (1941): 75–97.

- 1) to stimulate trust in the infrastructure, platforms and services of the Internet by ensuring a secure, safe and fair online ecosystem;
- 2) to ensure that fundamental rights and liberties are protected online;
- 3) to create an open and level playing field for economic actors that stimulates growth and innovation.

## 4.1 How to regulate the Internet?

To attain those goals, we need an effective regulatory framework. However, regulating the online world is not as easy as it sounds.

### 4.1.1 Internet architecture

Before we discuss how to regulate it, it is important to understand how the Internet works. Without that understanding, it will be difficult to formulate a strategy that takes into account the interests of all parties.

#### **How does the Internet work?**

The Internet is a public and global system of interconnected computer networks, a network of networks consisting of millions of private, public, academic, business and government networks linked by a broad array of electronic and optical networking technologies. The Internet functions because all parties involved use the same standard Internet core protocols, known as the Internet Protocol Suite, the standardisation of which is undertaken by the Internet

Engineering Task Force (IETF). It has no centralised governance in terms of technological implementation or policies for access and usage; each constituent network sets its own standards.

The protocols that make up the suite, of which Transmission Control Protocol (TCP) and Internet Protocol (IP) are the most important, allow users to connect to the Internet, find other users and communicate with them. All the computers and other equipment connected to the Internet are assigned a number through which they can be found. Such a number is called an IP address and looks something like this: 86.38.226.210. The Internet Protocol Suite is constructed as a set of layers.<sup>27</sup> Each layer deals with a specific part of the data transmission and provides services to the layer above it. The lowest layer is the link layer; the highest layer is the application layer. The whole IP suite runs on a physical infrastructure made up of network equipment: computers, cables, routers, switches, etc.

---

<sup>27</sup> Different models exist to describe the layered structure of the Internet. We have used the four-layer approach of the TCP/IP model (RFC 1122). Another model commonly used is the ISO-OSI Model, which describes seven layers instead of four.

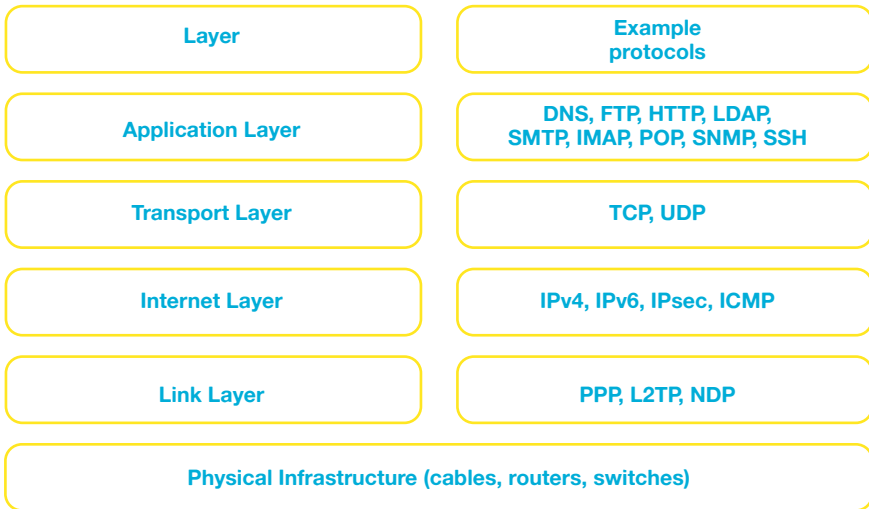


Figure 1: The layered structure of Internet

The institutional structure of the Internet is also layered. In other words, different entities are responsible for different functions and parts of the Internet (see figure 2).

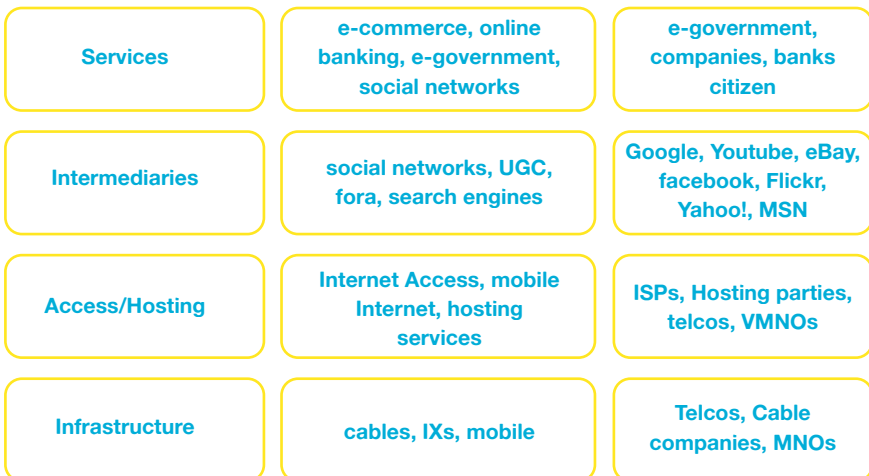


Figure 2: Institutional organisation of the Internet

At the bottom are the parties responsible for the physical infrastructure of the Internet and the transmission of data. They include the operators of public telecommunications networks, such as traditional telecom operators, cable companies and mobile network operators. The next layer is that of Internet access and hosting. Organisations at this level provide access to end users. Often, the operators of public telecommunications networks also provide the service. The next layer is the intermediary, an increasingly popular and important category on the Internet. Intermediaries provide service platforms—examples include eBay, YouTube and Facebook—that third parties, such as companies and consumers, can use. On the final level, services such as e-commerce, online banking and social networking are provided.

When examining this layered structure from a regulatory perspective, it is important to realise that understanding how these layers operate and interact can help inform a regulatory strategy. We must note however, that while the layered model of the Internet provides a good conceptual model of the technological and institutional ordering of the Internet, in practice the distinction between different layers is not as clear as portrayed here. Layers are not always so easily distinguishable, many entities are involved at different layers, and the layers do not necessarily equal markets. Therefore, regulation in one layer is not disconnected from (regulatory) actions taken in other layers.

## 4.1.2 Regulatory challenges

Few argue that the online world should have no regulation, but significant challenges exist when it comes to deciding specifics. The following challenges make an effective strategy problematic.

### **Anonymity**

Communication and contact on the Internet take place over a distance, so a first challenge is the anonymity of users. Anonymity enables them to express themselves and explore their interests and identities without fear of being scrutinised. It also makes regulating the behaviour of users more difficult, and exploitation by free riders and criminals possible. So a balance must be struck between anonymity and accountability.

### **Space**

A second challenge is that the Internet has no borders, so any regulatory strategy will run into problems of competing sovereignty and jurisdiction.<sup>28</sup>

Two states can have differing opinions on how a particular matter should be regulated. Denying the Holocaust is a criminal offence in many European countries; in the United States, it falls within the free-speech protection provided by the First Amendment to the Constitution. By setting up a server in the United States, a Holocaust revisionist can reach

---

<sup>28</sup> L. Lessig, *Code and Other Laws of Cyberspace, Version 2*, (New York: Perseus Books, 2006).

residents of European countries, where Holocaust denial is illegal.<sup>29</sup>

Enforcing regulation also runs into jurisdictional problems. Law enforcement agencies may not operate in the jurisdiction of another country without prior permission, but requests for mutual legal assistance can be costly and labour intensive, severely hampering international investigations. So moving criminal operations abroad, preferably to a country with little online enforcement, is a tactic many cybercriminals employ.

Problems also occur in the private sector. Though private international law is more flexible than criminal law, the fear of ending up in a cross-border dispute prompts consumers and businesses to do most of their online shopping in their own country.

### **Technological turbulence**

A third challenge is the rapid pace at which the Internet is evolving. Legislators cannot match it, so the law lags behind new technologies and services. To meet that challenge, legislators try to formulate laws that are ‘technology neutral’. That ensures that a law will cover future developments, but the drawback is that it becomes vague and ambiguous in the process and could create uncertainty about when and how it applies.

---

<sup>29</sup> See also: Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

## Private infrastructure

Most Europeans view the Internet as a public space, but its infrastructure and services are for the most part privately owned. That means that regulating cyberspace and its users is less straightforward than regulating the physical world, particularly since parties that own and run infrastructure and services need not be subject to the reign of a particular state, may have interests that do not align with those of the state or may not want to enforce third-party regulations on their platform or infrastructure.

### 4.1.3 Regulatory approaches

Those challenges aside, impressive efforts have been made to regulate the Internet in Europe. Four regulatory strategies are key: self-regulation, state regulation, co-regulation and regulation through architecture.

#### Self-regulation

From its conception in the 1960s, the Internet was largely separate from the physical world. Within cyberspace, like-minded people met in relatively closed communities that shared a set of norms, values and ideas about proper online behaviour, or Netiquette.<sup>30</sup> Community administrators (admins) enforced the rules. Common penalties for the violation of the social contract were naming and shaming. In

---

<sup>30</sup> See Request for Comments (RFC) 1855, Available at: <http://tools.ietf.org/html/rfc1855>.

extreme cases, members were expelled, which was termed banning.<sup>31</sup>

‘Netizens’ believed that cyberspace should be regarded as a world unrelated to the physical world and unregulated by traditional actors such as national states and companies. That idea is echoed strongly within the *Declaration of the Independence of Cyberspace*: ‘We believe that from ethics, enlightened self-interest and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis.’<sup>32</sup>

The idea of Netiquette and the attitude towards independence and self-regulation online still echoes strongly within the Internet community. The technical operation of the Internet is still for the most part governed through self-regulatory mechanisms. But pure, consensual self-regulation presents serious challenges when it comes to regulating the behaviour of users online.<sup>33</sup> Given the rapid growth of the Internet, the kind of close-knit groups of Netizens that allow for self-regulation no longer exist. Furthermore, the Internet is no longer separated from the physical world (see paragraph 3.3). It has become so important to our everyday lives that we can no longer rely solely on self-regulation, not

---

<sup>31</sup> Such a ban can be effected by blocking the IP address of the culprit.

<sup>32</sup> J. P. Barlow, ‘Declaration of the independence of cyberspace’, 8 February 1996; available at <https://projects.eff.org/~barlow/Declaration-Final.html>.

<sup>33</sup> For more information on consensual self-regulation, see A. Ogus’ *Regulation: Economic Theory and Legal Form* (Oxford: Clarendon Press, 1994).

only because it depends on voluntary participation but also because it lacks democratic oversight.

## State regulation

Austin defined law as the commands that oblige a person or persons to a course of conduct.<sup>34</sup> Laws are promulgated by a sovereign and subsequently enforced. That top down command-and-control approach is the traditional way in which the state regulates.

As the Internet grew in size and importance, the need for regulation became apparent to most nation states, and formal, prescriptive legislation was laid down. Despite online challenges, such as the *Declaration of the Independence of Cyberspace*, nation states have proven effective in regulating the online world. In particular, state actors have sought to employ the coercive measures that may be lacking in most self-regulatory schemes to keep the online world a safe, open, fair and decent environment. State regulation has its limits, however, so while formal legislation remains the foundation for regulating the Internet, additional approaches have proved necessary.

## Co-regulation and mandated self-regulation

State regulation has overtaken self-regulation online, but self-regulation remains an important approach. Technological turbulence and the fact that Internet infrastructure and services are mainly in private hands

---

<sup>34</sup> J. Austin, *The Province of Jurisprudence Determined* (Cambridge: Cambridge University Press, 1832; Cambridge: Cambridge University Press, 1995).

means that the private sector and users must be engaged. Mandated self-regulation and co-regulation are effective instruments for achieving that.

Mandated self-regulation uses a carrot-and-stick approach: the government stipulates that an area needs to be regulated, and the actors involved elect the best approach. If they fail, the government steps in.<sup>35</sup>

With co-regulation, the government sets forth the rules and parameters that apply and leaves the detailed rules up to the actors involved. The rules can be laid down in codes of conduct, guidelines, memoranda of understanding and other soft-law instruments.<sup>36</sup> Co-regulation is more flexible and better suited to the application area, since most subject matter experts are in the field of application. That means the private sector will be less encumbered by inappropriate rules and will experience less administrative burden.

Co-regulation is an important regulatory strategy within the EU. One of the starting points of the *Electronic-Commerce Directive* (2000/31/EC) for instance is that the implementation of the directive through a soft law approach should be set in motion by Member States (Article 16).

### **Regulation through architecture (Code as Law)**

The Internet poses fundamental and difficult questions about regulation, but the answer to the machine may well be in the

---

<sup>35</sup> I. Ayers and J. Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992).

<sup>36</sup> P. Grabosky and J. Braithwaite, *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies* (Melbourne: Oxford University Press, 1986): 83.

machine.<sup>37</sup> The architecture of the Internet allows for control. Because it is based on programming rules, or computer code, what is and is not possible within its environment can be mandated. A regulator can indirectly regulate the behaviour of users by directly regulating the programming code, creating code as code or code as law.<sup>38</sup>

An example from the physical world illustrates the concept. A regulator wanting to slow traffic in a residential area to 30 kilometres an hour would issue a law to that effect. Whether to obey the law is a choice that lies with the addressee, the motorist. Traffic officers checking the speed of motorists would enforce the rule. Likely more efficient, however, would be the installation of speed bumps; when a motorist drives too fast, he risks damaging his car. So he will slow down, not necessarily out of respect for the law, but to protect his car.<sup>39</sup> Either way, the rule is obeyed. By changing the architecture of the road, the legislator influences the behaviour of the norm addressee.

The Internet, with its changeable rules, also presents possibilities for regulation through architecture. It may permit a chaotic environment as a result of the regulatory challenges mentioned above, but it can also be controlled through code as law. While the code as law approach presents opportunities for regulation, it is important not to

---

<sup>37</sup> 'The answer to the machine is in the machine' is a famous quotation of copyright expert Charles Clark. See his 'The copyright environment for the publisher in the digital world' (*Proceedings of the Joint ICSU-UNESCO International Conference on Electronic Publishing in Science*, UNESCO, Paris, 19–23 February 1996.)

<sup>38</sup> Lessig, *Code and Other Laws*.

<sup>39</sup> For the sake of brevity, we will only use masculine pronouns where the person referred to could be either male or female.

overestimate the possibilities for regulating online behaviour through architecture. Implementing legal concepts into digital code is difficult and in many cases impossible. Furthermore, we must be cognisant of the fact that overzealous regulation through architecture might pose risks to the fundamental rights of the European citizen.<sup>40</sup> Striking a balance between freedom and control, and stimulating ‘value-sensitive design’ is a key challenge for Europe.<sup>41</sup>

## 4.2 Freedom and the Internet

Before we look at freedom on the Internet, we need to examine the concept of freedom, or liberty, more thoroughly. This is not the place to make a deep philosophical inquiry into the nature of freedom, but a look at the topic can help us understand the dilemmas posed by contradictory views about the Internet.

Freedom is difficult to define. This definition will serve, however, for the purpose of this study:

‘The situation in which a person is free from interference and outside constraints.’<sup>42</sup>

The right to freedom could then be defined as

---

<sup>40</sup> D. G. Post, ‘What Larry doesn’t get: code, law, and liberty in cyberspace’, *Stanford Law Review*, 52 (2000): 1439–58.

<sup>41</sup> M. Flanagan, D.C. Howe and H. Nissenbaum, ‘Embodying values in technology: theory and practice’, in J. Van den Hoven and J. Weckert (eds.), *Information Technology and Moral Philosophy* (Cambridge: Cambridge University Press, 2008).

<sup>42</sup> L. Fuller[0], *The Morality of Law* (New Haven: Yale University, 1964).

‘The right of a person to be left to do or be what he is able to do or be, without interference by other persons.’<sup>43</sup>

The right to individual freedom is not without limits. The right to freedom of speech, for instance, can be at odds with another person’s dignity, and in the case of hate speech, it may even threaten the safety of a person or group. So the rights and interests of others, both individuals and the community as a whole, limit individual freedom. In a democratic society, the law establishes freedom’s limits. The question, then, for us is what is the limit of the collective’s legitimate intrusion into the affairs of the individual or group.<sup>44</sup> Any answer to that question is of a moral, ethical and political nature. It is not the goal of this study to pass judgment, but to indicate the relationship that exists between interests, and explain how those interests might be affected by regulation online. In the second part of this report, we examine some dilemmas in which this question features prominently.

---

<sup>43</sup> I. Berlin, *Two Concepts of Liberty* (1958); republished in I. Berlin, *Liberty*, ed. H. Hardy (Oxford: Oxford University Press, 2002): 169.

<sup>44</sup> J.S. Mill, *Utilitarianism* (1863) and *On Liberty* (1859). These two works have been republished in a single volume edited by M. Warnock (Malden: Blackwell Publishing, 2003).

## Part 2: Online dilemmas

The Internet not only provides us with new possibilities and opportunities, it also raises new and fundamental questions about how we should order our online society. How to create a fair, safe, free and open online environment is one of the key questions facing Europe and the rest of the world in the twenty-first century.

In the second part, we focus on ethical and political issues raised by the Internet. We view the issues in light of the difficulties and potential suggested by online regulation. In particular, we focus on how regulation may influence the interests of various parties and affect online freedom. We have chosen four key topics: innovation, freedom of expression, privacy and intellectual property.

In the following four chapters, we explore each of those topics and examine the interests involved. Though we discuss them separately, the issues are closely related and even intertwined.

## 5 Innovation and the Internet

The Internet is one of the most important innovations of modern times. It has changed society and will shape the future of the European economy. Internet innovation is critical for the prosperity of Europe, and an environment that encourages both innovation and growth is essential.

### 5.1 Background

In the past decade, the Internet has grown spectacularly in size and speed. Worldwide, the number of people with access increased six fold. In 2010, 1.96 billion people were connected, compared with 275 million in 1998.<sup>45</sup> In 2010 70% of EU households had Internet access, an increase of nearly 300% compared with the year 2000.<sup>46</sup> The Netherlands and Denmark are positive outliers, with more than 91% and 86% respectively. Greece, Bulgaria and Romania are negative outliers with 46%, 33% and 42% respectively.<sup>47</sup> Companies are even better connected. Across the EU, 94% of companies had access in 2009,<sup>48</sup> with 83% of those being broadband connections.<sup>49</sup> Broadband access

---

<sup>45</sup> Internet World Statistics, <http://www.Internetworldstats.com/stats4.htm> (accessed 10 March 2010); International Telecommunication Union, [http://www.itu.int/ITU-D/ict/statistics/at\\_glance/KeyTelecom99.html](http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom99.html).

<sup>46</sup> Eurostat, based on EU-27, accessed 10 March 2010. (at: <http://epp.eurostat.ec.europa.eu>)

<sup>47</sup> Eurostat, based on EU-27, accessed 10 March 2010. (at: <http://epp.eurostat.ec.europa.eu>)

<sup>48</sup> Eurostat, based on EU-27, accessed 11 March 2010. (at: <http://epp.eurostat.ec.europa.eu>)

<sup>49</sup> Eurostat, based on EU-27, accessed 11 March 2010. (at: <http://epp.eurostat.ec.europa.eu>)

caused a shift of 725,000 jobs from traditional economic sectors to knowledge-based services, and the use of broadband has led to a 0.15% increase in productivity.<sup>50</sup>

While the figures look promising, on a global level Europe is falling behind in high-speed Internet, affecting our ability to innovate and compete, as well as to reap the social benefits of the digital society.<sup>51</sup> The new EC has set itself the following goal: 'To deliver sustainable economic and social benefits from a Digital Single Market based on fast and ultra-fast Internet and interoperable applications, with broadband access for all by 2013, access for all to much higher Internet speeds (30 Mbps or above) by 2020, and 50% or more of European households subscribing to Internet connections above 100 Mbps.'<sup>52</sup>

The 'Digital agenda' states that in order for Europe's digital innovation industry to flourish, obstacles must be removed and investments in innovation, Internet and ICT supported.<sup>53</sup> Only then will the Internet be a significant economic driver and citizens able to access the content they want. The 'Digital agenda' intends that by 2020, all Europeans will have access to much faster Internet, an ambitious goal that means the Commission must develop a comprehensive policy based on a mix of technologies and focusing on two parallel goals: to guarantee universal

---

<sup>50</sup> M. Fornefeld, G. Delaunay, and D. Elixmann, *The Impact of Broadband on Growth and Productivity* (Düsseldorf: Micus, 2008).

<sup>51</sup> European Commission, 'Europe 2020'.

<sup>52</sup> European Commission, 'Europe 2020'..

<sup>53</sup> European Union, 'Digital agenda for Europe: key initiatives', Memo/10/200, Brussels, 19 May 2010; available at <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/200>.

broadband coverage, combining fixed and wireless, with Internet speeds gradually increasing to 30 Mbps and above; and over time to foster the deployment and take-up of next-generation access networks (NGA) in a large part of the EU, allowing ultra-fast Internet connections above 100 Mbps.

Europe has one of the world's most competitive telecom markets, and broadband access is increasingly at the epicentre of competition between telecom providers. High-speed broadband development has so far followed a pattern of continuous, counter-cyclical waves of innovation and investment. This is especially true where there is competition among access infrastructure providers: as one player upgrades networks to higher speeds, competitive responses are triggered from other players.<sup>54</sup>

By itself, the roll-out of broadband networks is not enough. It must be accompanied by services that range from e-commerce transactions to distance health care. So with the goal of providing high-speed Internet to all Europeans, the 'Digital agenda' also sets out a strategy for new content and services. Fostering the creation of new applications and services, as well as the creation of a single digital market, are crucial goals for the EC.

## 5.2 Challenges

Much has been written about the competitiveness of Europe's ICT-industry and methods to improve it, so there is

---

<sup>54</sup> Bain & Company, 'Next generation competition: driving innovation in telecommunications', Liberty Global Policy Series, October 2009.

no need to go over it again.<sup>55</sup> We will focus instead on regulatory challenges in the area of innovation, which touches directly on the freedom of consumers and businesses, limiting ourselves to three key topics: the issue of net neutrality, the single digital market and interoperability.

### 5.2.1 Net neutrality

A first political and regulatory challenge is to facilitate the development of new applications and services. Recent discussion of online innovation has focused largely on net neutrality, a fiercely debated topic both in Europe and the United States. Proponents argue it is vital for innovation, consumer protection and freedom of speech; opponents claim it is ineffective, counterproductive and a solution in search of a problem.<sup>56</sup> In this section we limit ourselves to discussing neutrality in relation to innovation and consumer protection. In the chapter on freedom of expression, we discuss net neutrality in relation to freedom of speech.

Net neutrality is the idea that a network should try to treat all content, sites and platforms equally.<sup>57</sup> The idea is based on the argument that communication protocol operations should ideally take place at the end points of a system and

---

<sup>55</sup> European Commission, 'Europe's digital competitiveness: Report 2010', Vol. 1, Commission staff working document, SEC(2010) 627, Brussels, 17 May 2010.

<sup>56</sup> For competing views, see La Quadrature du Net, 'Protecting net neutrality in Europe', 11 November 2009 and S. Titch, 'The Internet is not neutral (and no law can make it so)', Reason Institute, Policy Study 375, May 2009.

<sup>57</sup> [http://timwu.org/network\\_neutrality.html](http://timwu.org/network_neutrality.html).

that therefore the ‘intelligence’ to execute those operations should be located at the edges of the network rather than at its core.<sup>58</sup> Most specific applications, such as the Web, email and multiplayer games, have been implemented in software on computers at the edge of the Internet. Edge-orientation is regarded as important for innovation, as it allows any new application or service to connect to users without any barriers.<sup>59</sup>

Proponents of neutrality fear that when strict adherence to end-to-end design principle is abandoned, operators may use intelligence in the core network to influence data flows to their own benefit. The ultimate consequence, they claim, would be a fragmented Internet where some services are favoured over others, and consumers are shut out of some nodes on the network. To prevent that, they want rules that mandate operator neutrality towards all content, sites and platforms, hence the term ‘net neutrality’.

Opponents agree with keeping the Internet open, but think that mandated neutrality is a fundamentally flawed approach. They argue that the Internet is by no means neutral today, and that trying to achieve neutrality through legal means will harm its development and stifle investment and innovation at both the edge and the core.<sup>60</sup> In their eyes, strict adherence to the end-to-end design principle is not only unfeasible but also counterproductive. In the early days,

---

<sup>58</sup> J.H. Saltzer, D.P. Reed and D.D. Clark, ‘End-to-end arguments in system design’, *ACM Transactions on Computer Systems* 2 (4) (1984): 277–88.

<sup>59</sup> M. Blumenthal and D.D. Clark, ‘Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world’, *ACM Transactions on Internet Technology* 1 (1) (2001): 70–109.

<sup>60</sup> Titch, ‘The Internet is not neutral’.

all intelligence may have truly resided at the edge of the network, but today there is already a lot of intelligence in the core network.<sup>61</sup> While ‘end-to-end’ is still a guiding design principle of the Internet, opponents of neutrality believe that trustworthiness, more demanding applications, cost-allocation issues and ISP service differentiation are arguments against an end-to-end approach in some cases.

### **Trustworthiness**

Moving away from strict adherence to the end-to-end principle is sometimes necessary to protect the network’s integrity. The principle depends on the end nodes all being trustworthy, and unfortunately, that is no longer the case. The increased popularity of the Internet has led to an increasing number of people who use it to send spam email or to attack computers through, for instance, denial of service attacks. Making the network more trustworthy implies more mechanisms at its centre to enforce good behaviour.<sup>62</sup>

### **More demanding applications**

As the Internet becomes more important in our lives, sophisticated applications and services such as distance health care, live-streaming and cloud computing are developed. The Internet has a limited bandwidth, however, especially near the edges of the network. Although providers upgrade networks, demand regularly exceeds available bandwidth, especially in the area of mobile Internet. And like

---

<sup>61</sup> Ibid.

<sup>62</sup> Blumenthal and Clark, ‘Rethinking’.

traffic in the physical world, demand is not distributed evenly throughout the day. ISPs may need to take steps, such as bandwidth management and prioritising traffic, to maintain quality of service and ensure optimal allocation of resources.<sup>63</sup>

The traditional Internet uses a best-effort approach to delivering data, meaning that each user obtains an unspecified, variable bit rate depending on the traffic load. In other words, each user gets the same level of service, regardless of the application he or she is using. In most cases, that approach works fine, but when the traffic load is high, best-effort may lead to an unacceptable degradation in the quality of service for such applications as VoIP, live video streaming, and online gaming, which rely on an optimal throughput of data with low latency and jitter.<sup>64</sup> That can mean longer loading times, service interruptions or no service at all, adversely affecting consumer satisfaction.

Opponents of net neutrality argue that it will deny ISPs the means to effectively manage their networks, because net neutrality stipulates that all content, sites and platforms be treated equally, that is, on the basis of best-effort delivery. That might not be an issue for p2p file sharing, but services that demand fast and stable connections, such as distance health care, video on demand and online gaming may suffer. Mandated net neutrality could lead to a degradation in the

---

<sup>63</sup> Organisation for Economic Co-operation and Development, 'Internet traffic prioritisation: an overview', 6 April 2007.

<sup>64</sup> 'Latency' refers to the amount of time it takes a bit to travel from its source to its destination. 'Jitter' refers to how variable the latency in a network is. The lower the latency and jitter in a network, the better applications such as VoIP, online gaming and streaming video will perform.

quality of service, since ISPs and content owners cannot guarantee the optimal throughput of data in a best-effort environment.

## Cost-allocation issues

Opponents of net neutrality fear that it will outlaw the traffic-management tools necessary to address cost allocation issues—when certain users use disproportionate network resources without having to pay more for the increased bandwidth consumption. P2p applications for instance, consume considerable amounts of bandwidth: an estimated 39% of all traffic worldwide is p2p.<sup>65</sup> Most p2p traffic, however, is generated by a relatively small group of users.<sup>66</sup>

Proponents of net neutrality accept deviating from it only for short-term, ordinary measures to deal with security threats, congestion and capacity constraints resulting from an unexpected problem. If the problem persists, the only sustainable solution for the benefit of all, they argue, is to invest in more bandwidth.<sup>67</sup> In practice, then, the cost of broadband would be shared across users, even when congestion and limitations are caused by a relatively small group. That poses an issue of fairness: how do we ensure that costs for bandwidth expansion are not borne by users who take up relatively little bandwidth?

---

<sup>65</sup> Cisco Systems, 'Cisco visual networking index: forecast and methodology 2009–2014', White Paper, 2 June 2010.

<sup>66</sup> The Belgian ISP Telenet, for instance, has about 20 users that download over one terabyte of data a month. That is roughly 250 DVDs worth of data each month. (Source: Telenet)

<sup>67</sup> La Quadrature du Net, 'Protecting net neutrality'.

## ISP service differentiation

ISPs may want to offer differentiated services to recoup investments in infrastructure and to address quality of service and cost allocation issues, something mandated net neutrality would outlaw. Proponents argue that if ISPs are allowed tiered and/or differentiated services, high-speed Internet would only be accessible to those with deep pockets. Opponents believe that pricing and service differentiation are part of the free market, and that it would be more difficult to recoup investments without them, thus slowing innovation.

A final argument against net neutrality is that it is a solution in search of a problem. Network operators' core business is to connect users to applications and services. Unfair discrimination against particular content, platforms or services goes against the business model, and so it is unlikely that operators will use network intelligence to the detriment of customers.

### 5.2.2 Lack of a single (digital) market

For innovation to truly soar, we need a single digital market. The 'Digital agenda for Europe' accurately maps the current issues, two of which are of particular importance to this study.

Persistent fragmentation is stifling Europe's competitiveness. We cannot reach the economies of scale needed to quickly roll out new services, a particular issue for

cloud computing. Different interpretations of the European *Data Protection Directive* (1995/46/EC), for instance, have made compliance with data protection rules throughout Europe a cumbersome, expensive process, limiting the potential to set up a European cloud. Since we lack a strong, sizeable domestic market, most of the recent successful Internet businesses are American: Google, eBay, Amazon and Facebook. Fragmentation also hurts digital content in Europe, limiting the introduction of new business models, an issue we discuss further in the chapter on intellectual property.

Digital transactions also are still too complex, with inconsistent implementation of the rules across Member States. As a result, consumers and businesses still face uncertainty about their rights and legal protection when doing business on line. Despite the introduction of the *Distance Selling Directive* (1997/7/EC) and the *E-Commerce Directive* (2000/31/EC), cross-border e-commerce still lags far behind domestic transactions, comprising less than 2% of the total volume in Europe.<sup>68</sup> A major reason is the lack of trust, sparked by different implementations of the *Data Protection Directive*, the lack of cross-border recognition of electronic signatures, different rules and standards for the security of IT systems, a lack of uniform procedures for complaints, different interpretations of liability for service providers and difficult enforcement in cross-border disputes.

---

<sup>68</sup> Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC); available at [http://ec.europa.eu/internal\\_market/consultations/2010/e-commerce\\_en.htm](http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm).

### 5.3 Interoperability

Interoperability of IT systems and services—–which depends on the use of recognised standards—is an important factor in successful innovation. Standardisation work in the EU is carried out by three independent bodies (CEN, CENELEC and ETSI), which cooperate with their national and international counterparts. Standards remain voluntary, but the EU has increasingly used them in support of its policies and legislation.<sup>69</sup> However, the rapid pace of Internet development and innovation conflicts with the slow pace at which standards are set in Europe. A first challenge is to bring the European process more in sync with the pace of today's IT sector.

A separate challenge is to deal with the use of closed standards. Private investment in research and development is at the heart of innovation. In order to gain a competitive edge, companies protect their findings through intellectual property law. When a technology, application or format becomes popular, it can become a *de facto* standard. In other words, it is not set by one of the European bodies, nor is it created by a private sector forum. To allow organisations to interoperate with their *de facto* standard, companies can license it, and users it will have to pay a fee and/or comply with certain rules. While that is part of the free market, we must take care the standards are not used to shut out competitors. The challenge is to strike a balance between the freedom to develop proprietary standards and techniques and the need to avoid anti-competitive behaviour.

---

<sup>69</sup> [http://ec.europa.eu/enterprise/policies/european-standards/index\\_en.htm](http://ec.europa.eu/enterprise/policies/european-standards/index_en.htm).

## 5.4 Possible solutions

In discussing possible solutions, we must be cognisant of the fact that the goal is to stimulate innovation, but the challenges are regulatory. The question is whether to opt for ex-ante legislation or a more targeted regulatory approach with ex-post enforcement.

### 5.4.1 Net neutrality: Free market or ex-ante regulation?

Net neutrality, in part, is a form of regulation through architecture aimed at influencing the behaviour of network operators. Insisting that all traffic be treated equally would lead to operators being banned from using network intelligence in a way deemed uncompetitive by those who favour neutrality. So while neutrality currently takes centre stage in the public debate, we should bear in mind that it is actually a *means* rather than an *end*. Its goals as far as innovation is concerned are to ensure a fair and open ecosystem for innovation and to protect consumer interests, and both proponents and opponents of neutrality support those goals. It is the method that is subject to debate. Whether neutrality is the best policy instrument to achieve the goals depends on our views on two questions: under which conditions does online innovation flourish and what is the level of trust we have in the free market and its regulation?

The answer to the first question depends on one's view of successful market models online and the role government should take in creating conditions for their correct

functioning. Proponents of net neutrality point out that the high rate of online innovation is the result of the end-to-end orientation of the Internet, which allows easy entrance to the market with little dependence on operators. The network, they believe, should consist of ‘dumb pipes’ that add no additional value beyond the transportation of data using the best-effort delivery principle. The government should mandate that the operators construct and operate their networks so that they cannot influence the flow of data.

Net neutrality opponents argue that features that enhance popular applications can be added—and have been added—to the core of the network without paralysing other applications.<sup>70</sup> They object to idea that the core of the network should consist of dumb pipes, and emphasise the value operators add by moving data in the most efficient way.<sup>71</sup> They point out that competition and innovation might be even better served by embracing a network diversity principle to allow owners to pursue separate approaches to routing traffic.<sup>72</sup> If operators are prohibited from developing the pricing mechanisms and service levels demanded by the market, future quality of service will decline, possibly leading to market failure. Above all, net neutrality opponents argue that it will deny operators the means to recoup investments in broadband infrastructure and next-generation networks.

The answer to the second question has to do with the level of trust we have in the free market in general, and the behaviour of network operators in particular. The code-as-

---

<sup>70</sup> See also Blumenthal and Clark, ‘Rethinking’.

<sup>71</sup> Titch, ‘The Internet is not neutral’.

<sup>72</sup> T. Wu and C. Yoo., ‘Keeping the Internet neutral: Tim Wu and Christopher Yoo debate’, *Federal Communications Law Journal* 59 (3) (2006): 575–92.

law approach of net neutrality is, in essence, aimed at preventing possible anti-competitive behaviour by network operators. Net neutrality proponents argue that it is the most effective mechanism to keep the Internet open. Opponents underline the fact that it is one approach, but by no means the only one. It is useful, therefore, to explore alternatives aimed at keeping the Internet open, including strong competition, oversight and transparency.

The OECD prefers a market-based solution in which competition itself safeguards against abuses of power or anti-competitive behaviour.<sup>73</sup> In that model, competition would produce a range of options to meet varying demands in bandwidth and service quality, and network operators who go against customers' interests would lose market share—likely the strongest incentive to behave cooperatively. EU Commissioner Kroes has also expressed a preference for a market-based solution.<sup>74</sup>

A market-based model would foster innovation, but it requires a competitive market for broadband, and may need to be augmented with other measures in areas or countries where little or no real competition exists. The free market also works only if customers can change network operators. The current churn in the telecom sector is relatively low in Europe; consumers and businesses want to avoid administrative hassle and periods of disconnection.

---

<sup>73</sup> Organisation for Economic Co-operation and Development, 'Internet traffic prioritisation: an overview', 6 April 2007.

<sup>74</sup> Neelie Kroes European Commission Vice-President for the Digital Agenda Net neutrality – the way forward European Commission and European Parliament Summit on 'The Open Internet and Net Neutrality in Europe' Brussels, 11 November 2010, available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/643>

Lower switching costs for consumers and businesses would stimulate competition.

A competitive market works only when consumers and businesses can make informed choices about competing services, so network operators should disclose to consumers any restrictions that apply. Article 20 of Directive 2009/136/EC already mandates that operators of public telecommunications networks provide information on procedures to measure and shape traffic, and the conditions under which access to and/or use of services and applications is restricted.

To strengthen the free market, especially in areas with little competition, government oversight is essential. Regulatory bodies should be able to examine and assess operators' procedures to ensure they do not limit competition or violate consumer rights.<sup>75</sup> One of the goals of the recently introduced Telecoms package is to strengthen oversight by national regulatory authorities (NRAs) and stimulate their cooperation within Europe.

## **The changing Internet landscape**

Finally, we must keep in mind that the Internet market is rapidly evolving. While there is no question that network operators are and will continue to be strong players, the distribution of power is changing.<sup>76</sup> Parties such as Google, Facebook and Apple, for instance, wield considerable influence. If net neutrality rules are put in place, it is

---

<sup>75</sup> Recital 34 of Directive 2009/136/EC.

<sup>76</sup> See Anderson and Wolf, 'The Web is dead'.

important to take into account their effect on new and powerful players, and determine whether neutrality rules should also apply to these players.<sup>77</sup>

In summary, the goal of maintaining an open Internet is shared by all, but it is not yet clear whether mandated net neutrality (1) is a necessary measure or (2) is indeed the best policy option. This conclusion warrants, at least for now, a cautious approach towards regulating the issue of openness and online innovation by means of mandated net neutrality. Indeed, the Body of European Regulators for Electronic Communications (BEREC) has concluded that since incidents are few and for the most part have been solved without the need for regulatory intervention, at present the existing legal framework provides adequate protection for users. It would therefore be premature to consider further intervention with respect to net neutrality on an EU level.<sup>78</sup>

## 5.4.2 Harmonisation and the single market

Creating a single internal market is one of the biggest challenges facing Europe. In its 'digital agenda', the EC outlined an ambitious program with the Commission dividing its strategy into four segments: opening up access to

---

<sup>77</sup> Google, for instance, a proponent of net neutrality rules, allegedly blocked access to the YouTube API for set-top box manufacturer Syabas because they were unwilling to enter into an advertisement agreement with Google. See E. Van Buskirk, 'YouTube Blocks Non-Partner Device Syabas as Allegations Fly', *Wired.com* (online version), 20 November 2009, <http://www.wired.com/epicenter/2009/11/youtube-blocks-non-partner-device-syabas-as-allegations-fly/>.

<sup>78</sup> Body of European Regulators for Electronic Communications, 'BEREC Response'.

content, making online and cross border transactions straightforward, building digital confidence and reinforcing the single market for telecommunication services.

In order for new digital services to truly take off, Europe needs one domestic market. The success of many American services can be attributed in large part to the sizeable, consumer-oriented market, where new services like iTunes, Hulu, Netflix, Twitter and Facebook quickly gain traction. Most European services, however, are aimed at a specific country and fail to acquire the critical mass needed to compete with overseas competitors.

Key measures need to be taken to strengthen the internal digital market: the creation of the Single Euro Payment Area (SEPA), the cross-border recognition of e-authentication mechanisms, unified e-invoicing rules and further harmonisation of legislation in Europe.

The last point is of particular importance. Member States currently have too much room for implementing legislation according to their own cultures, needs and wishes, so legislation is fragmented, making it difficult to launch truly European services. Stronger harmonisation of EU legislation is critical.

### **5.4.3 Interoperability: free market or ex-ante regulation**

Modernising the European standardisation policy is a potential solution to problems with interoperability, and the EU is currently revising its policy to bring standardisation more in

line with the global market.<sup>79</sup> In its white paper on ICT standardisation, the Commission identified several needed elements. They are 1) openness, consensus, balanced representation and transparency; 2) more flexibility in referring to standards or other documents in public procurement; 3) more synergy between ICT, R&D and standardisation; 4) open, transparent, fair and predictable intellectual property policies; 5) allowing references to specific fora and consortia outputs in EU legislation or policies; and 6) a multi-stakeholder platform for ICT standardisation.<sup>80</sup> In the 'Digital agenda for Europe', the Commission sets out its strategies to improve ICT standard setting, promote the better use of standards and enhance interoperability through coordination.

The Commission also proposes dealing with open and closed standards. As well as promoting open standards, it wants to ensure that closed standards are not used in an anti-competitive manner. The Commission will examine the feasibility of 'measures that could lead significant market players to license interoperability information', and it urges the creation of a 'European Interoperability Strategy and European Interoperability Framework'. The wording is cryptic, but the main point is that the Commission wants to mandate greater openness and interoperability between companies considered significant market players and smaller companies and services.<sup>81</sup> That might entail examining the potential of

---

<sup>79</sup> European Commission, *Modernising ICT Standardisation in the EU – The Way Forward*, White Paper, COM(2009) 324 final, Brussels, 3 July 2009.

<sup>80</sup> Ibid.

<sup>81</sup> Note that the criteria for being considered a 'significant market player' are less strict than those for being considered a 'dominant market player'. See, for instance, Commission guidelines on market analysis and the assessment of significant market power under the EC regulatory framework for electronic communications networks and services (2002/C 165/03).

ex-ante legislation. In a speech in June, Commissioner Kroes stated that she wants to examine ex-ante legislation.<sup>82</sup> She is hoping to avoid complicated, slow and expensive ex-post anti-trust cases, such as the Microsoft case, to ensure interoperability. To this end, she wants to examine mechanisms such as the mandatory publication of licence terms and pricing constraints.

While *ex-ante* legislation might stimulate interoperability, it will significantly influence the freedom of companies to do business. Proprietary standards give companies a competitive edge and allow them to control services and applications, ensuring an optimal user experience. *Ex-ante* legislation may therefore have a negative effect on innovation, discouraging private investment. So far it is unclear under which conditions companies would be subjected to the legislation, creating legal uncertainty. *Ex-ante* legislation, therefore, needs careful consideration and the weighing of the interests of all parties.

The ongoing discussion around openness of platforms, enabling devices, content production and content aggregation can be misleading as differing and sustainable business models have both open and closed elements to them. In general, a trend towards more open and collaborative business models can be identified, with the Internet players establishing differing control points around which monetisation is generated. Typically, core assets for monetisation are kept closed, whilst supporting assets are kept open to drive value to closed elements. Those trends

---

<sup>82</sup> N. Kroes, 'How to get more interoperability in Europe' (speech at the Open Forum Europe 2010 Summit, *Openness at the Heart of the EU Digital Agenda*, Brussels, 10 June 2010).

demand greater flexibility in the regulatory framework, both on when and in what circumstances to regulate, and when to show forbearance.

## 6 Freedom of expression and the Internet

One of the great benefits of the Internet is the ease with which people can express themselves, find information and engage in political debate. The relative anonymity of the Internet allows people to seek information without scrutiny and voice their opinions more freely. It is, therefore, a key technological driver for the democratic process, empowering citizens and stimulating freedom of expression.

### 6.1 Background

Freedom of expression in Europe is outlined in article 10 of the *European Convention on Human Rights*, and in article 11 of the *Charter of Fundamental Rights of the EU*. The articles stipulate that everyone has the right to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of borders. Freedom of expression is a prerequisite for a democratic society based on the rule of law, and the right to freedom of expression also plays a significant role in the protection of other human rights. Safeguarding the free flow of information online and ensuring that citizens have access to the Internet is vital for the

protection of freedom and democracy in Europe. Given the borderless nature of the Internet, it can also be used to create openness and media diversity in authoritarian regimes outside Europe, such as Iran and Burma.<sup>83</sup>

But the Internet's openness and anonymity has a downside. It can be used to incite hatred, share illegal content, such as child pornography, and engage in criminal conduct. Freedom of expression online is thus not without its limits. To ensure a safe, open, decent and tolerant online environment it is necessary to strike a balance between freedom of expression on the one hand, and the legitimate rights and interests of individuals and society on the other.

To uphold the law online, different mechanisms may be used. In addition to traditional law enforcement, measures such as notice and takedown (NTD) and filtering, aimed at removing or blocking illegal content, are available. Those mechanisms, however, may impede the free flow of information. In this chapter, we discuss the practical, ethical and legal issues associated with different enforcement mechanisms, focusing on notice and takedown and filtering, in a European and a global context.

### 6.1.1 Notice and takedown

For information to be visible online, it must be hosted by service providers, such as ISPs, video platforms and social

---

<sup>83</sup> This point was made by the Dutch Minister of Foreign Affairs Maxime Verhagen in a speech given at the 'Internet and freedom of expression' meeting in Paris on 8 July 2010.

networks.<sup>84</sup> When information is deemed harmful, illegal or infringing, steps can be undertaken to have it removed by the service provider at the behest of private parties or the government. Notice and takedown is the mechanism that facilitates that process.

The notice and takedown regime is outlined in article 14 of the *E-Commerce Directive*. The article states that a provider is not liable for the information on his servers if he has no knowledge of its illegal nature. Once the provider is made aware of its nature, possibly through a notice, he must expeditiously remove or disable access to it—takedown.

In theory, the notice and takedown regime is an elegant way to deal with harmful and illegal content online, but it is not without controversy. The key criticism is that it is not particularly effective in practice.

The NTD regime places a considerable burden of costs and liability risks on the service hosting the content. Because both removing and not removing content may lead to liability, the NTD mechanism must be very thorough in order to avoid mishaps. That means the process is often slow, leaving the content online for a period of time. Moreover, while most ISPs and services operate NTD systems to the best of their abilities, a significant number of rogue ISPs and platforms do not heed NTD requests. An example is the illegal file-sharing website The Pirate Bay, which mocked organisations sending NTD requests.<sup>85</sup>

---

<sup>84</sup> Information can also be hosted by individual users, for instance, by consumers who use peer-to-peer filesharing applications or users that operate their own webservers. This group is not taken into account in this section.

<sup>85</sup> See [www.thepiratebay.org/legal](http://www.thepiratebay.org/legal).

Another issue with the NTD approach is that it is an *ex-post* mechanism. In many cases, once the problematic information is published, the damage is already done. The longer the information stays online, the more extensive the damage will be. That reality is exacerbated by the fact that any information put online will quickly be copied to different locations.

A final issue is that it is easy for criminals to shift their content to a new platform. That means that when using a NTD approach, regulators have to play a constant game of cat and mouse.

### 6.1.2 Blocking and filtering

Since traditional law enforcement is often ineffective, and the notice and takedown method too slow and cumbersome, legislators turn towards code-as-law solutions, such as blocking and filtering content. While that may be efficient, it can also be at odds with freedom of expression and information, even constituting an unacceptable form of censorship, as seen in countries such as Iran, China and Burma. Unsurprisingly, Internet filtering is a highly controversial topic. In this section we describe how different filtering mechanisms work, as each may impact freedom of expression in a different way.

#### **Site blocking**

ISPs have the power to block access to an IP-address and/or the associated URL if it is deemed to contain

harmful or illegal content. When a blockade is issued, access to that website is blocked for all subscribers. The problem is that all content on the website is blocked for all visitors. Moreover, it is not clear whether blocking is effective in the long run, because website administrators can switch IP-addresses or create a new URL to avoid the blockade, and subscribers may use proxies and virtual private networks to get around it.

### **Port and protocol blocking**

In some cases, it may also be technically possible to block certain transfer protocols and corresponding ports. The simplest way to do this is by closing off the port used by the protocol, but this measure may be circumvented by making use of standard ports (which cannot be blocked as they are also used for essential services such as e-mail and surfing the web) or changing ports at regular intervals. One response may be to detect the protocol in use and block traffic using that protocol. However, that could also result in over-blocking.

### **Filtering by means of content recognition**

A third way to filter and block illegal content is automatic file recognition, which allows data transfers from those files to subsequently be blocked. It also creates the potential to scan for illegal content. Several techniques can identify files: hash matching, fingerprinting and watermarking. Content recognition allows the blocking of illegal content without impeding legitimate communication. It must be noted that while it is possible to scan content that is stored and resides on a server, scanning content that is travelling through a network is far more difficult with current technology.

With hash matching, a mathematical formula is applied to a file to generate a unique alphanumeric string or hash value unique to that particular file and all its copies. Possible matches can be found by calculating the hash values of files and comparing them with a database with known hash values. If there is a match, the content in question is illegal. Hash values are unique to the bits that files are composed of, not their contents. When files are converted from -.mpg to -.avi, for example, the hash values will no longer correspond. Fingerprinting is similar to hash matching, but instead of identifying bits, it identifies content. Fingerprints are attached to original files and remain intact even if the files are subsequently altered. As in hash matching, the fingerprints of certain files can be compared with a database of known fingerprints. Watermarking affixes unique and, preferably, invisible digital watermarks to files. When watermarked files are found, running them through a database with known watermarks can identify them.

### **Deep packet inspection**

To enable filtering, it is often not enough to scan the header of an IP packet, so some routers now offer the option of scanning the contents. Deep Packet Inspection (DPI) enables ISPs to inspect headers, which contain information on traffic type, sender and recipient, and also the data within, the so-called payload. In that manner, traffic types and content can be determined more accurately. ISPs primarily use DPI to manage traffic more efficiently and identify malicious IP packets that may be used to orchestrate attacks on their networks. The use of DPI is controversial because, according to opponents of DPI, it allows ISPs to search through communications, which might constitute an invasion of privacy. As a result, ISPs are

reluctant to use the technology on behalf of third parties, for instance government. The question is whether ISPs can indeed be said to ‘peek’ inside communication. Examining the contents of one single packet, for instance, suffices to establish the type of protocol involved. In the case of content recognition, the inspection of a small number of packets may be enough to determine whether the contents of the entire file match one that has been identified as illegal. Nevertheless, examining IP packet payloads is potentially a more invasive measure than checking packet headers and should therefore be applied with due consideration.

## 6.2 Challenges

Filtering can be such an effective mechanism in influencing the flow of information that its application is highly controversial. It can be an effective way to combat harmful, illegal and infringing content, but it can also be used to limit the free flow of information and facilitate censorship. Filtering is one of the most heavily debated subjects in the area of Internet regulation. In this section we discuss the challenges that filtering poses for society.

### 6.2.1 Effectiveness of filtering

While discussion of the relation between filtering and freedom of expression takes centre stage, we must first consider whether filtering is effective. If it can be easily circumvented, it cannot be considered an effective enforcement mechanism. Whether filtering is also a solution

to a particular policy problem is context dependent. In the case of child pornography, for instance, opponents of filtering the pornography argue that it only masks the problem and does not deal with its root, the production of child abuse images. They want more effective law enforcement. Proponents of filtering argue that it is better than doing nothing. Even if we devote significantly more resources to seeking out child abusers and pornography, we will still have an enormous amount of it online. By filtering, they argue, we at least discourage the demand side, making it more difficult to find child pornography. Warnings can also be issued to users, reminding them they are looking for illegal content and possibly scaring them off.

### 6.2.2 Proportionality and subsidiarity

Filtering is without doubt a potential threat to freedom of expression online, so in discussing the application of filtering, we must consider whether there are measures available that are less infringing. We must also decide whether an individual issue is serious enough to warrant filtering and blocking.

### 6.2.3 The slippery slope

One of the main criticisms of filtering is that it moves us onto a slippery slope: while option A might be fine for filtering, it will inevitably lead to situation B, in which filtering is totally

unacceptable. Again, child pornography serves as an example. While it may be acceptable to filter child pornography, the fear is that once a filter system is in place, the door will be open for filtering other topics, such as those on radical websites and, in the end, perhaps free speech itself.

A related matter is ‘mission creep’, the situation in which the original goal of an application is gradually extended to additional purposes. There are many examples of mission creep and it should be taken into account when discussing filtering applications.

The slippery slope is a serious risk, but it is also a well-known logical fallacy: the fact that there is a risk of sliding down the slippery slope is, in itself, not an argument not to proceed with option A.<sup>86</sup> Also, technical and legal safeguards can be put in place to ensure that filtering does not get out of hand, but that will take political will and the formation of a broad consensus.

### 6.2.4 Filtering and foreign policy

The globalisation of the Internet has led to a situation of competing sovereignty. What is considered legal in Europe may be illegal in another country. In authoritarian regimes in particular, filtering is common and often aimed at limiting freedom of expression. How Europe should respond to that is a foreign policy question: to what extent does Europe want to involve itself in the domestic affairs of other countries?

---

<sup>86</sup> For an analysis of slippery slope mechanisms, see E. Volokh, ‘The mechanisms of the slippery slope’, *Harvard Law Review* 116 (4) (2003): 1026–1137.

## 6.2.5 Filtering and net neutrality

Filtering can be seen as a violation of the principle of net neutrality, which, we have shown, aims to treat all data traffic equally. Net neutrality, therefore, can be seen as one means of strengthening freedom of expression. It is questionable, however, whether it would provide legal protection beyond that available through the Convention and the Charter, since governments can set aside neutrality rules if the situation demands it.

## 6.3 Possible solutions

No clear-cut solutions exist to lift the tension between filtering and freedom of expression. The key issue is to strike a balance between effective enforcement and freedom. The first imperative, then, is to explore whether any less infringing options are available. We need to look at other policy options that could strengthen enforcement online. Only when less intrusive options are unavailable, or when they are prohibitively expensive, should we turn to filtering.

### 6.3.1 International cooperation

Law enforcement of the Internet often has an international dimension, and a major bottleneck is the cooperation between various enforcement agencies. Strengthening enforcement in a European and global context would allow

the issue of illegal content to be addressed more effectively, reducing the need for filtering applications.

### 6.3.2 Public-private partnerships

The private sector can play an important role in maintaining a safe online environment through raising awareness, exchanging information and cooperating with enforcement agencies.<sup>87</sup> An example of a successful public-private partnership is the standardised notice and takedown (NTD) procedure in the Netherlands, set up by the government in close cooperation with the private sector.<sup>88</sup>

### 6.3.3 Checks and balances

More resources and better international cooperation will strengthen law enforcement, but it is unclear whether that will be adequate to stem the tide of illegal content. So, in those cases where there are no real alternatives, filtering might become an acceptable policy option. But if we are to deploy filters we must ensure that they do not violate freedom of expression and other rights. We must also ensure that the risks of mission creep and the slippery slope are avoided through strong checks and balances,

---

<sup>87</sup> European Commission, 'Towards a general policy on the fight against cyber crime', Communication, COM(2007) 267 final, Brussels, 22 May 2007.

such as regular reviews, sunset clauses and very strict purpose limitations.

## 7 Privacy and the Internet

In the matter of privacy, the Internet offers both opportunities and threats. Its relative anonymity protects users' privacy, but at the same time vast amounts of personal data are processed every day, with and without users' consent. Privacy and the protection of personal data are, therefore, key issues for freedom online.

### 7.1 Background

Challenges to privacy in European society exist on many levels, for instance, in the relationship between businesses and consumers, citizens and government and between Internet users. In this chapter, we examine some key issues for privacy online. But first it is important to explore the right to privacy more in depth.

---

<sup>88</sup> Dutch Notice and Takedown Code of Conduct (2008).

### 7.1.1 The right to privacy

The need for privacy is probably as old as mankind itself. Virtually all societies, both primitive and modern, have techniques for setting distances and avoiding contact in order to give members a measure of privacy.<sup>89</sup> Before the rise of modern technology, physical boundaries, combined with rules, customs and taboos, created a distinction between the public and the private. But as technology progressed, physical barriers became less effective, making legal protection more important. The first explicit mention of a right to privacy was in an article by the United States Supreme Court justices Warren and Brandeis in 1890. They defined the right to privacy as the 'right to be let alone'.<sup>90</sup> Since then, the right to privacy has been recognised as an important human right and codified in international treaties and the constitutions of many states, including Article 8, Paragraph 1 of the *European Convention on Human Rights*: 'Everyone has the right to respect for his private and family life, his home and his correspondence.'

While the right to privacy states that we must respect the 'private sphere', it is not clear what constitutes the private sphere and when the right to privacy can be invoked. Privacy is not a static object, but is a concept that is always context related, making it impossible to define it without referring to a complex set of social, cultural, religious and historical parameters from which it derives its meaning.<sup>91</sup>

---

<sup>89</sup> J. Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, (Ithaca: Cornell University Press, 1997): 12.

<sup>90</sup> S.D. Warren and L.D. Brandeis, 'The right to privacy: the implicit made explicit', *Harvard Law Review* 4 (5) (1890): 193–220.

<sup>91</sup> S. Gutwirth, *Privacyvrijheid! De vrijheid om zichzelf te zijn* (Amsterdam: Otto Cramwinckel Uitgevers, 1998): 40 (in Dutch).

Law professor Daniel Solove has argued convincingly that no single definition of privacy exists. He draws upon Ludwig Wittgenstein's notion of 'family resemblances' in outlining how different notions of privacy have no particular thing in common, but are related to one another in many different ways.<sup>92</sup> Instead of trying to conceptualise privacy, therefore, we should take a more pragmatic approach and focus on understanding privacy in specific contextual situations. That makes abstract discussions about privacy more concrete, enabling effective policymaking.

When we look at the right to privacy in different contexts, we can see that it is aimed at protecting underlying interests. In other words, the right to privacy is often a means, rather than an end in itself, with the important functions of maintaining personal autonomy, enabling audience separation and minimising burden. The underlying interests protected are human dignity and freedom.

### 7.1.2 Informational privacy and data protection

The private sphere traditionally comprises the home, family life and correspondence.<sup>93</sup> Within those domains, individuals are free to live their lives as they see fit. Since the right to privacy allows us to shield certain parts of ourselves, it seems an ideal vehicle for curbing the spread of personal data. Over the past few decades, the private sphere has

---

<sup>92</sup> D.J. Solove, 'Conceptualizing privacy', *California Law Review* 90 (2002): 1096.

<sup>93</sup> P. Blok, *Het Recht op Privacy* (Den Haag: Boom Juridische uitgevers, 2002): 323 (in Dutch).

grown to include personal data, giving rise to a new type of privacy: informational privacy. Westin defined informational privacy as ‘the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated.’<sup>94</sup>

The OECD outlined principles for the protection of personal data as early as 1980.<sup>95</sup> The goal was not only to protect personal privacy but also to ensure that disparities in national laws would not lead to interruptions in the transborder flows of data. The OECD principles formed the basis for the *Personal Data Protection Directive* (1995/46/EC), which was adopted in 1995.

### 7.1.3 The limits of privacy

The privacy granted to an individual is always balanced against society’s need for openness and disclosure. Ideally, individuals should be able to enjoy maximum privacy, but in cases such as public health or security, the legitimate interests of society may outweigh the individual right.<sup>96</sup> To maintain a proper balance between the two, laws place limits on the interferences that may be made by third parties. Article 8 Paragraph 2 of the ECHR states:

---

<sup>94</sup> A.F. Westin, *Privacy and Freedom*, (New York: Atheneum Press, 1967): 7.

<sup>95</sup> OECD Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data (23 September 1980)

<sup>96</sup> A. Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999): 8.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Striking such a balance is the key challenge for regulating privacy, both between businesses and consumers and between citizens and government.

## 7.2 Challenges for Europe

Privacy is a concept in a perpetual state of transformation. As an important human right and a foundation for other rights, protection of privacy is a prerequisite for a democratic society. The Internet poses significant challenges to privacy, some of which we discuss below.

### 7.2.1 Persistence and reputation

The persistence of information online is the first such challenge. Once information has been published, it can be very hard to remove. In the offline world people gradually forget what they have seen, but online information remains visible almost indefinitely. So when personal information is put online, the infringement of the private sphere is often more extensive.

That is a particular issue when the information is of a very private nature, for instance images of one's sexual life, or when the information is inaccurate or slanderous. In such cases, a person's reputation can be significantly harmed. Although celebrities, politicians and other prominent figures regularly must deal with such invasions, average citizens can also be affected. About 4% of adults say they have suffered from having embarrassing or inaccurate information posted about them online. Despite such incidents, only 33% of Internet users say they worry about their online identity.<sup>97</sup>

### 7.2.2 Context and audience separation

Closely related to online reputation is the issue of context and audience separation: how people present themselves and what information they divulge is dependent on their audience and the context. How one behaves at a party with friends, for instance, is different from how one behaves at work. In a sense, people have different identities that match the context they are in. However, on the Internet, information recorded in one context may easily be transported to another, where data may be misinterpreted.

---

<sup>97</sup> M. Madden and A. Smith, 'Reputation management and social media: how people monitor and maintain their identity through search and social media', PEW Internet, May 2010, <http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx>.

### 7.2.3 Privacy, dignity and personal autonomy

Democratic societies have a fundamental belief in the uniqueness of the individual, his basic dignity, and his worth as a human being.<sup>98</sup> To safeguard personal autonomy and individuality, one must be allowed a private space free from outside influences. In this ‘inner sanctum of the self’, a person can be alone with his deepest thoughts and feelings. Were it not for the psychological barrier raised by privacy, a person would be open at any time to outside scrutiny and judgment. Such things as unwanted body searches, the display of intimate behaviour or peculiarities to the world and intrusions into our homes all encroach upon our sense of human dignity.<sup>99</sup> Privacy shields a person from the inquisitive gaze of third parties. When his core self can be invaded without permission, or even without knowledge, dignity is diminished.<sup>100</sup> An important aspect of human dignity is the right to individual liberty. The more we know about a person, the greater the degree of control we exercise over him. Privacy limits what the state and other parties can and may know about us by creating an impregnable personal sphere. In that regard, privacy acts as a limit to the power that can be exercised over us by third parties, most importantly government. Privacy can thus be seen as a countervailing force against power and control.

---

<sup>98</sup> Westin, *Privacy and Freedom*, 7 and 33.

<sup>99</sup> E.J. Bloustein, ‘Privacy as an aspect of human dignity: an answer to Dean Prosser’, in F.D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984): 156–202.

<sup>100</sup> G.T. Marx, ‘Murky conceptual waters: the public and the private’, *Ethics and Information Technology* 3 (3) (2001): 157–69.

As mentioned earlier, however, criminals and terrorists have learned to use the Internet to their benefit, giving rise to a need for new standards in law enforcement for the fight against cybercrime and terrorism. In that area, the right to privacy regularly clashes with the interests of law enforcement.

### 7.2.4 Digital footsteps

New technologies have led to changing notions of privacy. While technology is neutral in its approach, our current *Data Protection Directive* betrays its age.<sup>101</sup> In particular, the notion of personal data, central to the application of the directive, is increasingly difficult to apply in the Internet age.

Personal data is any information relating to an identified or identifiable natural person, or data subject. It is clear that that a name and a surname are personal data, but it is less clear that information that cannot directly be linked to a person should be considered personal data. We leave digital footsteps in many places, and although they might not be considered personal data, they can influence individuals nevertheless. In the case of behavioural targeting, for instance, individualisation is enough for it to be effective, identification of a person is not necessary.<sup>102</sup>

---

<sup>101</sup> A revision process of the Data Protection Directive is currently taking place in Europe.

<sup>102</sup> Behavioural targeting is a marketing technique whereby consumer behaviour (for instance, web browsing) is monitored in order to determine consumers' interests.

## 7.2.5 Globalisation of privacy issues

The *Personal Data Protection Directive* aims to provide a uniform level of protection throughout Europe. It also applies to data on European citizens that is transported abroad. Organisations wanting to export personal data have to prove that the destination country has a level of protection equal to European standards. But the Internet, as we have noted, does not play by territorial rules. In particular the advent of cloud computing, in which it is often unclear where data is stored at any point, makes enforcing European rules more difficult. It also creates economic problems because Europe's fragmented privacy laws put us at a competitive disadvantage with other countries.

## 7.3 Possible solutions

While the challenges to privacy are significant, there are ways to mitigate the risks such challenges pose.

### 7.3.1 Awareness

Europeans are worried more about privacy on the Internet than about their online reputations. A large majority feels that data transmission is not secure enough (82%).<sup>103</sup> Confidence

---

<sup>103</sup> Eurobarometer, *Data Protection in the EU: Citizens' Perceptions*, Survey conducted by the Gallup Organization Hungary upon the request of Directorate- General Justice, Freedom and Security, Flash Eurobarometer Series 225, February 2008, 40; available at [http://ec.europa.eu/public\\_opinion/flash/fl\\_225\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf).

in transmitting data decreases with the age of respondents and increases with education level.<sup>104</sup> Despite their fears, data subjects know relatively little about the misuse and abuse of personal data, their rights as data subjects and ways to avoid or limit risk. Awareness, therefore, is critical.

### 7.3.2 Transparency and control

In 2009 Commissioner Reding released a statement that European citizens need to gain more control over the use of their personal information.<sup>105</sup> If they are to do that, they must be made aware of how the data is processed, and to that end, the transparency of processing must be heightened. The recently adopted *Telecoms Package*, directive 2009/136/EC, stipulates that third parties wanting to store information on or obtain data from a user's computer, via cookies, for instance, must provide the user with clear and comprehensive information about activity to achieve those goals. At the same time, it recognises that security breaches involving personal data may result in economic loss and social harm, including identity theft or fraud, physical harm, humiliation or damage to reputation. As a result, providers are required to notify the affected individuals without delay to allow them to take any necessary precautions.<sup>106</sup>

---

<sup>104</sup> Ibid. 41.

<sup>105</sup> Press Release 'Citizens' privacy must become priority in digital age, says EU Commissioner Reding', IP/09/571, Brussels, 14 April 2009.

<sup>106</sup> Recitals 61 and 66, Article 2, Paragraphs 4 and 5 of Directive 2009/136/EC.

As well as becoming aware of how their personal information is used, data subjects must have the means to exercise their rights, and tools that help them do that can aid in putting the user back in control. The EU could play a role in developing and stimulating the use of such tools.

### 7.3.3 Accountability and enforcement

Privacy plays an important role in the trust people develop in companies and administrative bodies, so both the private and the public sector tend to use personal data responsibly. Still, there are organisations that do not, emphasizing the need for accountability and effective enforcement to weed out the bad seeds.

For the private sector, better oversight by national authorities could help strengthen privacy. An alternative would be to strengthen the rights of individuals, possibly by giving them the opportunity to seek damages from organisations that violate their rights.

For law enforcement and government use of personal data, there must be strong oversight by governments and the EU, for instance through the European Parliament. Laws should contain necessary checks and balances and sunset clauses where possible.

### 7.3.4 Privacy by design

Privacy by design incorporates privacy rules into the design of an information system. By hardwiring the rules into the technology—through anonymisation, authentication, and selective disclosure—breaches of privacy are prevented. Privacy by design is more effective than legal protection; rules can be broken or changed, but the design of an information system is a fixed reality.

### 7.3.5 Rethinking privacy

We need to keep rethinking privacy and its protection. The current approach is focused on processing data, rather than data's uses and the consequences for data subjects. To overcome challenges to privacy, we need to think in terms of possible harm and managing identities in different contexts.<sup>107</sup> The European Data Protection Directive is still geographically oriented although privacy issues are global. It is timely that the directive is under review.

Another approach is to view privacy as a collective interest. Privacy is currently conceptualised as an individual right, but the interests it aims to protect are also collective: autonomy, social cohesion and equal treatment. If we see privacy as a prerequisite for a stable, democratic and free society, we can avoid pitting individual privacy rights against the security of society as a whole.

---

<sup>107</sup> J. Van den Hoven, 'Information technology, privacy and the protection of personal data', in J. Van den Hoven and J. Weckert (eds.), *Information Technology and Moral Philosophy* (Cambridge: Cambridge University Press, 2008).

## 8 Intellectual property and the Internet

Digitisation and the Internet have radically altered the landscape for the creation and distribution of content. Movies, music, games, software and e-books can be copied and distributed at minimal cost and without a loss in quality. That has created new opportunities for business and new services for consumers, but it has also meant that intellectual property infringement now takes place on a massive scale.

How we should deal with intellectual property in the digital age has been fiercely debated for more than a decade, with the argument going back and forth between the online communities' dedication to the free flow of information and the role of intellectual property in stimulating creativity.

In this chapter we explore the dilemma and examine the different positions.

### 8.1 Background

Intellectual property (IP) is a legal construct aimed at striking a balance between the free flow of information, knowledge and culture and the protection of the people and institutions that produce creative works. The concept of intellectual property naturally has its roots in the more general concept of property. Political philosopher John Locke argued that property extends to the products of one's labour: 'Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his labor with,

and joined it to something that is his own, and thereby makes it his property.<sup>108</sup>

The most important feature of any kind of property is exclusivity, meaning that use of the property requires the owner's authorisation. The same goes for intellectual property, subject to the legal rights and interests of others. The exclusive right to property is recognised in article 17 of the *European Convention on Human Rights*, which also states that intellectual property shall be protected (article 17, paragraph 2). Information, however, is a public good. It is non-rivalrous, meaning that consumption of the good by one does not reduce its availability to others, and it is non-excludable, meaning that no one can be excluded from consuming it. Exclusivity is not a characteristic of information without additional protection. Copyright is aimed at providing that protection by taking away the public-good character of information. In order for that to be effective, it must be enforced, and enforcement in the digital era is problematic. Copyright holders are finding it increasingly difficult to protect the exclusive nature of their right. IP is divided into two categories: industrial property, which includes inventions and their patents, trademarks, industrial designs and geographic indications of source; and copyright, which includes literature, films, musical works, visual art and architectural designs. Rights related to copyright include those of performing artists for their performances, producers of phonograms for their recordings and broadcasters for their radio and television programs.<sup>109</sup>

---

<sup>108</sup> J. Locke, J. (1690). *The Second Treatise of Government and a Letter Concerning Toleration*, republished in 1981 (ed. Gough, J.W.), New York: Dover Publications, § 27, at 19

<sup>109</sup> World Intellectual Property Organisation, 'What is intellectual property?', [www.wipo.int/about-ip/en/](http://www.wipo.int/about-ip/en/).

## 8.2 Challenges

For a knowledge-based economy such as Europe's, the creation and free flow of information is vital. We must create an environment that stimulates the creation and consumption of content. To build such an ecosystem online posits the protection of intellectual property and the free flow of information. Specific aspects of intellectual property warrant discussion in relation to the online world, primarily copyright and illegal file sharing. Another prominent concern deals with the copyright-related aspects of Web 2.0: user-generated content, Wikinomics, crowdsourcing and co-creation.<sup>110</sup>

### 8.2.1 (Illegal) file sharing and copyright

Digitisation has made possible the creation of exact copies of copyrighted works at virtually no cost. They can subsequently be distributed over the Internet. File sharing has grown immensely popular as a result of growing broadband penetration and the introduction of easy to use peer-to-peer (p2p) file-sharing services. P2p file sharing accounts for a substantial percentage of worldwide Internet traffic,<sup>111</sup> and most people agree that the majority of shared files are infringing.

The massive scale at which copyrighted files are illegally shared has sparked a battle between authors, artists, the

---

<sup>110</sup> In this chapter we limit ourselves to discussing copyright and do not go into issues of patent law, trademark infringements, etc.

<sup>111</sup> Cisco Systems, 'Cisco visual networking index'.

entertainment industry and pro-copyright groups on one side, and pirates, advocates of free culture and consumer rights groups on the other. The differing views have their roots in differing opinions on the moral basis and economic utility of intellectual property rights.

Proponents of copyright support it as a necessary moral and economic protection for the creator. They argue that because a work is the fruit of his labour, the creator has the right to dispose of it as he sees fit. The author thus has the 'moral right' (*droit moral*) to his output. That right protects the personal and reputational value of the artist and his work, and plays a role in the economic utility of copyright. Without copyright, its proponents argue, creators will be unable to recoup the investments they have made in time, money and effort, and the stimulus to create new works will be reduced, investment in creativity will decline and society as a whole will be hurt.

Opponents of copyright point out that while the author has certain moral rights, in particular the personal and the reputational, they are by no means absolute. It is up to society, they argue, to decide how a work should be used once it is made public, after which an author can stake no claim to exclusivity. That idea is also reflected in their theory of the utility of copyright. Opponents feel that while creators might deserve recognition, their work should benefit society as a whole. They argue that copyright creates an artificial scarcity, hindering innovation and reducing its overall utility for society. By removing intellectual property rights, everyone can benefit from the work, either by consuming it or by creating new works based on the original.

A third group also takes part in the debate. It does not question the importance of copyright and its role in protecting creators and rights holders, but is critical about copyright in practice. Its members believe that copyright stifles innovation by being used too defensively, particularly by the entertainment industry. They argue that copyright is too often used to protect aging business models and to maximise profits. The third group is more concerned with the influence of copyright on the functioning of the digital market.

In the midst of that discussion, a thriving market for illegal file sharing has emerged, undermining copyright and creating a lucrative black market where pirates can earn a lot of money with direct copyright infringement or by facilitating copyright infringement.

### 8.2.2 Enforcing copyright in a digital environment

The copyright debate is highly polarised, in part because Internet users fear that effective enforcement will encroach on their civil liberties. Users who infringe copyright, for instance, may have to relinquish their anonymity so that rights holders can commence legal action. Furthermore, technical measures such as monitoring, filtering, throttling or blocking of Internet traffic might be at odds with freedom of expression and the right to privacy.

There are two distinct approaches to the enforcement of copyright: disrupting supply and discouraging demand. Both are in use with varying degrees of vigour and success. While

effective strategies to enforce copyright online will likely require elements of both, regulators need to choose which option to emphasise.

## Disruption of the supply side

Publishing a work of literature, science or art is the exclusive right of the author. Sharing of a work online is regarded as publication. So, uploading a copyrighted work to a p2p file-sharing network, Usenet, a website, or a video platform such as YouTube is an infringement of copyright, unless it is done by the author or rights holder.

Anti-piracy organisations such as BREIN in The Netherlands or the GVG in Germany direct their efforts at Internet sites and file-sharing platforms that play a key role in the distribution of infringing content. The biggest advantage of disrupting supply is that it has a huge impact. Most illicit file sharing takes place through only a small number of platforms, such as The Pirate Bay, BTJunkie and Torrentz.com. A second advantage is that users are not targeted. The drawback is that the sites are notoriously hard to take down. Many file-sharing platforms are located in countries with which mutual legal assistance is a time-consuming matter. A case in point is the continuous legal struggle against The Pirate Bay, currently the world's largest file-sharing portal. Even though the site's owners have been convicted and the site's hosts receive regular takedown orders, the site remains online by moving to a different host when necessary. Anti-piracy organisations can also request ISPs to block access to sites offering infringing content. While the *E-Commerce Directive* does allow such actions, blocking sites is highly controversial because non-infringing content can also be blocked, a possible infringement of freedom of expression.

## Interventions on the demand side

As long as demand for free consumption of copyrighted content remains high, so does the incentive to supply it. The rationale for cracking down on demand is to add the costs of piracy to the price users pay when they access pirated content, producing an unfavourable cost-benefit ratio. In most European countries, downloading of copyrighted content is prohibited, but without meaningful enforcement, a ban is ineffective at best. As a result, new strategies, such as graduated response and filtering, are being considered, and in some cases used.

Significant drawbacks to enforcing copyright exist on the demand side. Punishing those who habitually infringe copyright may require tactics that invade the privacy of alleged file-sharers. In order to prove that someone is consuming copyrighted works without permission, either the Internet use or the computer of the alleged offender must be examined. Techniques such as Deep Packet Inspection can identify different types of traffic, but permanent monitoring of Internet use may conflict with society's interest in preserving the civil liberties of its citizens.

Another consequence of cracking down on demand is that it makes rights holders look like big, faceless companies targeting ordinary people with unfair sanctions. The resulting negative public image has moved rights holders to favour disrupting supply.

### 8.2.3 Digital Rights Management

Many rights holders try to limit piracy through Digital Rights Management methods. Using anti-copying technology on data carriers or files makes it more difficult to use them in unapproved hardware or prevents copying.

While DRM can protect intellectual property and permit a fine-grained mechanism for rights management and payment, it has drawbacks. Products with DRM often reduce users' utility, possibly limiting their rights under existing copyright exceptions. Users may not be able to play movies or make back-up copies. DRM may also lead to 'consumer lock-in' if content cannot be played on different devices. A final issue is that DRM targets legitimate consumers of a product, the people willing to pay for it. Critics believe that by using DRM, the entertainment industry antagonises paying fans.

### 8.2.4 Slow emergence of new business models

One of the major criticisms that the anti-copyright and file-sharing community has against the entertainment industry is that it has failed to change its business models to keep up with the evolving technical reality of the Internet. They argue that a lack of new business models is the primary reason people turn to illegal alternatives, and that changing the business models is the easiest and most effective way to deal with illegal file sharing. But the proposed fix is not as straightforward as the anti-copyright and file-sharing community makes it seem.

The playing field is not level between legal and illegal services. Legitimate businesses are bound by market rules and realities. They must be profitable, are subject to taxation, must comply with all relevant legislation, need payment mechanisms and must offer a high level of quality. Legitimate businesses are also situated in a complex value chain composed of various players—authors, producers, distributors, hardware vendors etc.—each with their own specific set of interests. Experimenting with new business models might affect the value chain, leading to friction and a loss of profit and goodwill. The deeply embedded culture of release windows in the movie industry provides a good illustration. Investments in movies are recouped in different stages, separated in time. Theatrical release is followed by DVD release, which is followed by a release for TV broadcasting. That tiered system of windows is the result of a careful balance of the interests of various economic actors, which rely on each other for profitability. Upsetting the balance forces the various parties to respond, trying to restore the status quo. When Disney, for instance, wanted to narrow the window for theatrical release for *Alice in Wonderland* from 17 to 12 weeks, theatres responded with a boycott of the movie.<sup>112</sup> Given the importance of a theatrical release, studios are reluctant to abandon the window system in favour of new all digital business models.

---

<sup>112</sup> J. Malvern, 'Cinema boycott could send *Alice in Wonderland* down the rabbit hole', *The Times*, 22 February 2010; available at <http://www.timesonline.co.uk/tol/news/uk/article7035592.ece>.

## 8.2.5 User generated content

The advent of Web 2.0 has led to a huge boom in user-generated content. Thanks to cheap and easy to use production tools, and publishing platforms such as YouTube, Vimeo, Picasa and Facebook, every consumer is now also a potential producer. The new cult of the amateur, where ‘prosumers’ can participate in the creation of content, is a great benefit to society and a significant addition to professionally produced content. By unlocking the wisdom of the crowd through crowdsourcing and co-creation, hitherto untapped resources can be used to create new content—Wikipedia is an example—and even solve social issues.

Several legal issues, however, attach themselves to user-generated content, crowdsourcing and co-creation, many related to intellectual property. Prosumers, for instance, often base their created content on existing copyrighted works, or use copyrighted material in their own productions, using a copyrighted song as a sound track in a home video, for instance. That creates questions about how traditional notions of copyright exceptions and fair use apply. Another issue is that prosumers are often unaware of their rights as creators and fail to protect their works or realise their monetary value. Crowdsourcing and co-creation also pose legal challenges to those taking part. Given that many parties are involved in developing an artistic work or service, it is often unclear who owns the final product and who may make changes to it. Legal uncertainty hampers the future development of user-generated content, crowdsourcing and co-creation.

## 8.3 Possible solutions

When we look at the arguments of copyright proponents, opponents and critics, we see that all sides want an environment that provides maximum utility for society. How to create that environment is where they disagree. The challenge is to find a regulatory regime that reconciles the differing opinions.

### 8.3.1 Stimulating new business models

Creative industries have long struggled to find new and viable models for using the Internet to distribute content in Europe. Their difficulties result from an abundant supply of pirated content, issues within the value chain, fragmented markets and the inability and/or unwillingness of the entertainment industry to adapt to a changing digital environment. The market for online content is there, however. Though unauthorised access is a significant problem, surveys suggest that people are willing to pay for online content.<sup>113</sup> Even habitual file sharers are not averse to spending money on music, movies or games.

Creating new business models should be left to the market, but government can facilitate their emergence by removing market barriers and curbing piracy.

---

<sup>113</sup> See for instance: Huygen, A., N. Helberger, J. Poort, P. Rutten, N. van Eijk, Ups and Downs; Economic and Cultural Effects of File Sharing on Music, Film and Games, TNO/SEO/IVIR 2009

### 8.3.2 A single digital market

For new business models to succeed, a single digital market is vital. Commissioner Kroes and her predecessor, Commissioner Reding, have both indicated that a single, internal digital market is a key goal of the ‘Digital agenda’. The aim is to create a clear framework that allows consumers and companies to partake more easily in the digital market. An important element in the strategy is for copyright to be harmonised across the EU.

In fact, copyright itself has been harmonised, but the same is not true of exceptions such as the home-copying exception, licensing and collective management of rights. A harmonised exceptions system is needed to clarify the position of consumers, intermediaries and content providers. A clear and uniform means for acquiring and managing licences is necessary so that entrepreneurs can more easily extend their services to other countries, and rights holders are reimbursed in a fair and simple way. To this end the Commission has proposed a cross-border, pan-European licensing scheme as well as improved governance and transparency for collective rights management.<sup>114</sup>

### 8.3.3 Enforcement of intellectual property

For new business models to flourish, intellectual property must be protected and pirates who profit from copyright

---

<sup>114</sup> European Commission, ‘A digital agenda’, 9.

infringement stopped.<sup>115</sup> The only way to do that is through effective enforcement. But we also have to take into account how enforcement may affect the freedom and rights of citizens, balancing the right to property with the right to privacy and freedom of expression. And intellectual property and its enforcement should not provide undue protection to ageing business models. Three different regulatory approaches exist: state regulation, self-regulation and co-regulation, and regulation through architecture.

### **State regulation**

A first approach to protecting intellectual property is to strengthen traditional law enforcement, paying particular attention to international cooperation. A strategy aimed at the supply side, prosecuting pirates, rather than the demand side likely would be most effective. While international cooperation is necessary, we must ensure that individual rights and liberties are respected. The most important initiative in international cooperation, the *Anti-Counterfeiting Trade Agreement (ACTA)*, has attracted critics who fear it will give law enforcement agencies and customs organisations sweeping authority offline as well as online. The fact that the ACTA negotiations were conducted in secret adds fuel to their suspicions.

### **Self-regulation and co-regulation**

The state-oriented approach could be replaced or augmented by a self-regulatory scheme, including notice and takedown

---

<sup>115</sup> See European Parliament, Committee on Legal Affairs, 'On enforcement of intellectual property rights in the internal market', Report, 3 June 2010; available at <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2010-0175&language=EN>.

systems and graduated response mechanisms. That would require cooperation between the content producers and the distributors, the ISPs. In any self-regulatory scheme, ISPs play an important role, given that they manage Internet traffic and hold the key to contacting users. ISPs are reluctant to cooperate with rights holder, however, as they do not want to be responsible for regulation, and cooperation with rights holders may damage their business model and their relationship with their customers.

The *E-Commerce Directive* states that ISPs are not responsible for copyright infringements perpetrated over their networks if they have no prior knowledge of them (articles 12 through 14). Article 15 states that ISPs are under no obligation to monitor Internet traffic proactively. These safe harbour provisions protect ISPs and other service providers against claims from third parties. The idea is that an ISP, as an intermediary, should not be held responsible for the actions of the end user. Only under specific circumstances can this protection be lifted. Still, it must also be noted that ISPs may indirectly benefit from copyright infringement. As file sharing raises the utility of users' Internet connections, it also increases their willingness to pay for broadband connections, creating economic incentives for ISPs.<sup>116</sup> By shifting this incentive away from illegal file sharing towards legal file sharing, in which ISPs have a share, we may heighten the potential for successful cooperation between rights holders and ISPs.

A system under discussion in many countries is graduated response, in which file sharers receive notices from their ISP that they are engaging in copyright infringement. After a

---

<sup>116</sup> O. Bomsel and H. Ranaivoson, 'Decreasing copyright enforcement costs: the scope of a gradual response', *Review of Economic Research on Copyright Issues* 6 (2) (2009): 13–29.

certain number of warnings, usually three, a sanction will follow. Controversy dogs this measure as it does many others. For graduated response to work, a user's Internet traffic must be monitored, a possible infringement of privacy. Also, the ultimate sanction is disconnection, a penalty that is generally considered too harsh.<sup>117</sup> A final matter to be resolved is who will bear the costs of operating the system.

### Technical measures

A third enforcement mechanism is the use of technical measures such as filtering and blocking. They may be effective, but ISPs are even more reluctant to cooperate with these measures than with graduated response. They argue that the measures violate freedom of expression and the right to privacy, and that they will damage their business models, since blocking and filtering run counter to the interests of their customers. Whether self-regulatory schemes using technical measures are feasible, then, is up in the air. Co-regulation, mandated by government, is more likely to be successful, but, once again, we must be cognisant of the risks, most notably to freedom of expression and the right to privacy (see chapters 6 and 7).

### 8.3.4 Alternative compensation mechanisms

The goal of copyright is to protect the creator so he will continue his work for the benefit of society as a whole. Other

---

<sup>117</sup> Alternatives to disconnection might be throttling the connection of a user or denying the user access to infringing sites.

mechanisms to achieve that goal—such as concerts, speaking fees and merchandising—should be explored.

Another way to deal with piracy is to legalise it and reimburse content producers by raising an Internet levy. That may sound attractive, but it also has serious drawbacks. It would provide unfair competition to emerging business models since file sharing would be a legal means of accessing content. If creators and rights holders are denied the option of determining how to distribute and market their content, the free market would cease to function and become dependent on government. In addition, all Internet users would be required to contribute to the levy, regardless of whether they download. In order to create a good repartition key, all downloading traffic needs to be monitored so that popular artists get the share they deserve. Arguments for invasive monitoring are often directed at enforcing copyright, but monitoring would also be required for this alternative. Finally, a download levy would support pirates, since their distribution platforms will no longer be illegal.

### 8.3.5 Unlocking the creative potential of users

The creation and distribution of content is still, for the most part, in the hands of organised conglomerates such as publishers, recording companies and film studios. But with the arrival of Web 2.0, users have started creating and sharing their own content, which could contribute to the future prosperity of Europe, and by unlocking the creative potential of users, provide a boost to our culture and

economy.<sup>118</sup> We need, then, to create a favourable legal climate for user-generated content, and to promote alternatives such as open source, Creative commons and copyleft, or to create a limited copyright exception for user-generated content.

Those mechanisms are the result of legal, more than technical or social, innovation. They are alternatives to traditional intellectual property law, copyright in particular, that allow for greater freedom in the use and reuse of creative work. Creative commons and other soft alternatives allow authors to have an appropriate level of control over their output, from getting credit for it to deciding the conditions under which others can use it. But the models are not a replacement for traditional intellectual property law. In fact, without traditional intellectual property law, these alternative models could not exist.

Yet another option is to create a limited copyright exception for material in user-generated content. To a large extent, the user-generated content culture builds upon existing material, for instance by creating mash-ups. Strict interpretation of current copyright laws means that creative work is often removed from the Internet because some part of it is considered infringing. An exemption for user-generated content could be worthwhile in cases where no substantial infringement has taken place, no commercial gain is possible, the work does not compete with the original and the moral rights of the author are not violated.

---

<sup>118</sup> Organisation for Economic Co-operation and Development, (2007): 32.

## 9 Conclusions

The Internet allows for great freedom. The first users saw it as a new environment where the rules of the physical world did not apply. But as it has become more and more integrated into our physical world and its economy and society, the idea that the Internet should remain free of regulation has given way to the notion that, as with any other aspect of society, some form of regulation is needed.

The modern Internet still allows for great freedom, but with freedom comes responsibility. If we want to keep the Internet an open, safe and vibrant online environment, we must ensure that we take into account and protect the rights and interest of all members of society. Europe's greatest challenge is to ensure maximum freedom for all. That means balancing a range of rights and interests with the general good of society. In that balancing act, we must not play a zero-sum game, whereby values are exchanged for one another, but aim to ensure that values are maximised as much as possible. We must not exchange privacy for security, for instance, but seek an approach that strengthens security while maintaining privacy. In cases where different rights and interests cannot be reconciled, a political choice will have to be made.

In this report, we have described four online categories—innovation, freedom of expression, privacy and intellectual property—in which the different interests of varying social actors feature prominently. Each topic poses specific regulatory challenges, which the nature of the Internet magnifies. Coming up with an effective strategy is complicated by issues such as anonymity online, the

borderless nature of the Internet, technological turbulence and the fact that most of the Internet infrastructure is owned by the private sector.

In regulating the Internet, various regulatory strategies are open to us, including state regulation, self-regulation, co-regulation and regulation through architecture. Each has its own strengths and weaknesses. Self-regulation was the dominant mode when the Internet was in its infancy, but as it has grown in size, scope and importance, the limits of self-regulation have become apparent. State regulation is now the most important, but the Internet's borderless nature and the private ownership of its infrastructure limit state regulation. A third option is co-regulation, in which government sets the legal framework, which is then filled in by the relevant actors, combining aspects of self-regulation and state regulation. Its effectiveness is dependent on the participation of all the actors involved. A final option is regulation through architecture, which forces compliance with rules through limiting users' options technologically. Examples of the code-as-law approach are filtering, blocking and digital rights management. Those methods can be at odds with the rights of individuals, groups and organisations, however, so we have to be aware that regulation through architecture can limit freedom. Nonetheless, the problem remains that traditional means of law enforcement are limited in their effectiveness, and regulation through architecture may be a necessary tool. In designing systems that regulate behaviour we must ensure that legal, moral and ethical principles are taken into account. Value-sensitive design of IT systems is important for the development of the information society. Given the technological turbulence that comes with the high pace of innovation, we must also keep evaluating and re-evaluating both the design of IT systems and the laws that govern their use.

# 10 Bibliography

## 10.1 Literature

**Anderson, C. and M. Wolf.** 'The Web is dead. Long live the Internet'. *Wired* (online version), 17 August 2010.

**Austin, J.** *The Province of Jurisprudence Determined*. Cambridge: Cambridge University Press, 1832; Cambridge: Cambridge University Press, 1995.

**Ayers, I. and J. Braithwaite.** *Responsive Regulation: Transcending the Deregulation Debate*. Oxford: Oxford University Press, 1992.

**Bain & Company.** 'Next generation competition: driving innovation in telecommunications'. Liberty Global Policy Series, October 2009.

**Barlow, J. P.** 'Declaration of the independence of cyberspace', 8 February 1996; available at <https://projects.eff.org/~barlow/Declaration-Final.html>.

**Berlin, I.** *Two Concepts of Liberty*. 1958. Republished in I. Berlin, Liberty, ed. H. Hardy. Oxford: Oxford University Press, 2002.

**Blok, P.** *Het Recht op privacy*. Den Haag: Boom Juridische Uitgevers, 2002.

**Bloustein, E.J.** 'Privacy as an aspect of human dignity: an answer to Dean Prosser'. In F.D. Schoeman (ed.),

*Philosophical Dimensions of Privacy: An Anthology*. New York: Cambridge University Press, 1984): 156–202.

**Blumenthal, M and D.D. Clark.** ‘Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world’. *ACM Transactions on Internet Technology* 1 (1) (2001): 70–109.

**Body of European Regulators for Electronic Communications.** ‘BEREC Response to the European Commission’s consultation on the open Internet and net neutrality in Europe’. BoR (10) 42, 30 September 2010.

**Bomsel, O. and H. Ranaivoson.** ‘Decreasing copyright enforcement costs: the scope of a gradual response’. *Review of Economic Research on Copyright Issues* 6 (2) (2009): 13–29.

**Cisco Systems** (2010), *Cisco Visual Networking Index 2009–2014*.

**Clark, C.** ‘The copyright environment for the publisher in the digital world’. Proceedings of the Joint ICSU-UNESCO *International Conference on Electronic Publishing in Science*. UNESCO. Paris, 19–23 February 1996.

**Etzioni, A.** *The Limits of Privacy*. New York: Basic Books, 1999.

**Flanagan, M., D.C. Howe and H. Nissenbaum.** ‘Embodying values in technology: theory and practice’. In J. Van den Hoven and J. Weckert (eds.). *Information Technology and Moral Philosophy*. Cambridge: Cambridge University Press, 2008.

**Fornefeld, M., G. Delaunay and D. Elixmann.** *The Impact of Broadband on Growth and Productivity*. Düsseldorf: Micus Consulting, 2008.

**Fuller, L.** *The Morality of Law*. New Haven: Yale University, 1964.

**Grabosky, P. and J. Braithwaite.** *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies*. Melbourne: Oxford University Press, 1986.

**Gutwirth, S.** *Privacyvrijheid! De vrijheid om zichzelf te zijn*. Amsterdam: Otto Cramwinckel Uitgevers, 1998.

**Hobbes, T.** *Leviathan: Or The Matter, Forme, & Power of a Common-Wealth Ecclesiasticall and Civill*. 1651; repr. Harmondsworth: Penguin Classics, 1982.

**Huygen, A., N. Helberger, J. Poort, P. Rutten, N. van Eijk,** Ups and Downs; Economic and Cultural Effects of File Sharing on Music, Film and Games, TNO/SEO/IVIR 2009

**International Telecommunications Union** (2010), *Measuring the Information Society*, version 1.0.1.

**Kelsen, H.** 'The law as a specific social technique'. *The University of Chicago Law Review*, 9(1) (1941): 75–97.

**La Quadrature du Net.** 'Protecting net neutrality in Europe'. 11 November 2009.

**Madden, M. and A. Smith.** 'Reputation management and social media: how people monitor and maintain their identity through search and social media'. PEW Internet, May 2010,

Available at: <http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx>.

**Malvern, J.** 'Cinema boycott could send Alice in Wonderland down the rabbit hole'. *The Times*, 22 February 2010; available at <http://www.timesonline.co.uk/tol/news/uk/article/7035592.ece>.

**Marx, G.T.** 'Murky conceptual waters: the public and the private'. *Ethics and Information Technology* 3 (3) (2001): 157–16.

**McKinsey & Company.** 'Consumers driving the digital uptake: the economic value of online advertising-based services for consumers'. September 2010. Available at: [http://www.iab.net/insights\\_research/947883/consumers\\_driving\\_digital\\_uptake](http://www.iab.net/insights_research/947883/consumers_driving_digital_uptake)

**Mill, J.S.** *Utilitarianism* (1863) and *On Liberty* (1859). These two works have been republished in a single volume edited by M. Warnock (Malden: Blackwell Publishing, 2003).

**Ogus, A.** *Regulation: Economic Theory and Legal Form*. Oxford: Clarendon Press, 1994.

**Organisation for Economic Co-operation and Development.** 'Internet traffic prioritisation: an overview' (6 April 2007).

**Organisation for Economic Co-operation and Development.** *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking* (2007).

**Post, D. G.** 'What Larry doesn't get: code, law, and liberty in Cyberspace'. *Stanford Law Review*, 52 (2000): 1439–58.

**Saltzer, J. H., D.P. Reed and D.D. Clark.** 'End-to-end arguments in system design'. *ACM Transactions on Computer Systems* 2 (4) (1984): 277–88.

**Smart, J., J. Cascio and J. Paffendorf.** 'Metaverse roadmap: pathways to the 3D web'. Acceleration Studies Foundation 9, 2007.

**Solove, D. J.** 'Conceptualizing privacy'. *California Law Review* 90 (2002): 1087–1155.

**Stross, C.** *Halting State*. New York: Ace Books, 2007.

**Tapscott, D. and A.D. Williams.** *Wikinomics: How Mass Collaboration Changes Everything*. New York: Penguin Books, 2006.

**Titch, S.** 'The Internet is not neutral (and no law can make it so)'. Reason Institute. Policy Study 375, May 2009.

**van 't Hof, C., R. van Est and F. Daemen** (eds.). *Check in / Check out: Public Space as an Internet of Things*. Rotterdam: NAI Publishers, 2011.

**Van Buskirk, E.** 'YouTube Blocks Non-Partner Device Syabas as Allegations Fly'. *Wired.com* (online version), 20 November 2009.

**Van den Hoven, J.** 'Information technology, privacy and the protection of personal data'. In J. Van den Hoven and J. Weckert (eds.). *Information Technology and Moral Philosophy*. Cambridge: Cambridge University Press, 2008.

**Van Reenen, J. et al.,** *The Economic Impact of ICT* London:

London School of Economics, 2010.

**Vinge V.** *Rainbow's End*. New York: Tor Books, 2006.

**Volokh, E.** (2003). 'The mechanisms of the slippery slope'. *Harvard Law Review* 116 (4) (2003): 1026–1137.

**Wagner DeCew, J.** *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Ithaca: Cornell University Press, 1997.

**Warren S.D. and L.D. Brandeis.** 'The right to privacy: the implicit made explicit'. *Harvard Law Review* 4 (5) (1890): 193–220.

**Westin, A.F.** *Privacy and Freedom*. New York: Atheneum Press, 1967.

**Wu, T.** 'Network neutrality FAQ'. Available at [http://timwu.org/network\\_neutrality.html](http://timwu.org/network_neutrality.html).

**Wu, T. and C. Yoo.** 'Keeping the Internet neutral: Tim Wu and Christopher Yoo debate'. *Federal Communications Law Journal* 59 (3) (2006): 575–92.

## 10.2 Official publications

**European Commission.** ‘A digital agenda for Europe’. Communication, COM(2010) 245. Brussels, 19 May 2010.  
European Commission. ‘Europe 2020: a strategy for smart, sustainable and inclusive growth’. Communication, COM(2010) 2020. Brussels, 3 March 2010.

**European Commission.** *Modernising ICT Standardisation in the EU – The Way Forward*. White Paper, COM(2009) 324 final. Brussels, 3 July 2009.

**European Commission.** ‘Towards a general policy on the fight against cyber crime’. Communication, COM(2007) 267 final. Brussels, 22 May 2007.

**European Parliament, Committee on Legal Affairs.** ‘On enforcement of intellectual property rights in the internal market’. Report, 3 June 2010; available at: <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2010-0175&language=EN>.

**Council Framework Decision** 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law

## 10.3 Speeches

**Kroes, N.** ‘How to get more interoperability in Europe’ (speech at the Open Forum Europe 2010 Summit, *Openness at the Heart of the EU Digital Agenda*, Brussels, 10 June 2010).

## 11 Appendix: Glossary

|                      |  |
|----------------------|--|
| 3G                   | Third generation fast mobile Internet access                                       |
| Ambient Intelligence | Vision of the future whereby we will be surrounded by an intelligent environment   |
| API                  | Application Programming Interface  |
| Augmented Reality    | Application whereby a layer of information is projected over the physical space    |
| Cloud computing      | Computing paradigm whereby resources are moved to the 'Internet Cloud'             |
| Copyleft             | Using copyright to ensure that a work, and all derivatives, can be shared for free |
| Creative Commons     | System for easy licensing of creative works  |
| Crowdsourcing        | Consulting large groups of users in the process of creation                        |
| Cyberspace           | Popular term to describe the virtual space created by the Internet                 |
| DRM                  | Digital Rights Management  |
| FttC                 | Fibre to the Curb  |

|                    |   |
|--------------------|---|
| FttH               | Fibre to the Home   |
| Internet of Things | Evolution of the Internet whereby physical objects will become networked    |
| IP                 | Internet Protocol   |
| Jitter             | Refers to how variable the latency in a network is                          |
| Latency            | Refers to the time it takes an IP packet to move from source to destination |
| M2M                | Machine-to-Machine  |
| Mission creep      | Expansion of a project or system beyond its original scope                  |
| MMO                | Massive(ly) Multiplayer Online Game   |
| MUVE               | Multi User Virtual Environment  |
| Netizens           | Popular term that generally refers to the first users of the Internet       |
| Nettiquette        | Standard for acceptable behaviour online                                    |
| NFC                | Near Field Communication P2P  |
| Open Source        | System whereby access to the source materials of a work is guaranteed       |
| P2P                | Peer-to-peer  |

|            |   |
|------------|---|
| Prosumer   | Blend word of producer and consumer, i.e., a consumer that also creates content         |
| RFID       | Radio Frequency Identification  |
| TCP/IP     | Transmission Control Protocol / Internet Protocol                                       |
| VoIP       | Voice over IP   |
| Web 2.0    | Popular term describing the evolution of the Web to a participatory medium              |
| Web 3.0    | Popular term describing the next phase in the evolution of the Internet (after Web 2.0) |
| Wikinomics | Economic theory based on sharing, peering and mass collaboration                        |
| WiMax      | Mobile telecommunications protocol for high-speed Internet access                       |

## **Bart W. Schermer, PhD LLM**

Bart W. Schermer is partner and co-founder of Considerati, a research and consultancy firm with a focus on law, policy and technology. In addition, Bart is an assistant professor at eLaw@Leiden, the Centre for law in the Information Society of the University of Leiden, and a fellow at the E.M. Meijers Institute for Legal Studies. He is co-founder and editor of the Dutch Journal of Internet Law (Tijdschrift voor Internetrecht) and a member of the Cybercrime expert group for the Court of Appeal in The Hague.

## **Ton Wagemans, LLM**

Ton Wagemans is partner and co-founder of Considerati. Ton was trained as a lawyer and specialises in policy development, public affairs and public private partnerships. From 2000 to 2004, he worked for the Dutch Electronic Commerce Platform (ECP.NL) and was a member of the European Commission's e-Confidence Core Group. In addition, Ton was a researcher on e-business self-regulation at Oxford University.