Philos. Technol. (2011) 24:419–436
DOI 10.1007/s13347-011-0031-x

SPECIAL ISSUE

ISPs & Rowdy Web Sites Before the Law: Should We Change Today's Safe Harbour Clauses?

Ugo Pagallo

Received: 12 March 2011 / Accepted: 6 May 2011 / Published online: 20 May 2011
© Springer-Verlag 2011

Abstract The paper examines today's debate on the new responsibilities of Internet service providers (ISPs) in connection with legal problems concerning jurisdiction, data processing, people's privacy and education. The focus is foremost on the default rules and safe harbour clauses for ISPs liability, set up by the US and European legal systems. This framework is deepened in light of the different functions of the services provided on the Internet so as to highlight multiple levels of control over information and, correspondingly, different types of liability. The new responsibilities of ISPs concern the original "end-to-end" architecture of the medium and policies on design rather than responsibility for user content and individual messages.

Keywords Copyright · Data protection · Internet service providers · Jurisdiction · Privacy by design · Responsibility · Safe harbour clauses · Self-enforcement technologies

1 Introduction

Current provisions on legal responsibility of Internet service providers (ISPs) can be summed up with a default rule and a factual condition. On one hand, the default rule concerns the clause of legal immunity that has been granted by both the US and EU lawmakers so as to strengthen the flow of information on the Internet. It suffices to mention section 230 of the US *Communication Decency Act* from 1996, section 512 (c) of the US *Digital Millennium Copyright Act* (DMCA) from 1998, and the responsibility regime set up by the EU Directive 2000/31/EC on e-commerce. According to article 15 of this latter directive, there is "no general obligation to monitor the information which [ISPs] transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity".

U. Pagallo (✉)
Law School, University of Torino, via s. Ottavio 54, 10124 Turin, Italy
e-mail: ugo.pagallo@unito.it

On the other hand, such a status of immunity ends when ISPs fail stopping an illegal activity undertaken by recipients of the service once they are informed about such activity or when they are asked to intervene. In the wording of article 15 D-2000/31/EC, "Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements".

There are a number of reasons why inventors, lawmakers and judges alike have deemed the default rules of ISP legal irresponsibility to be "good". On the side of the scientists, for example, Tim Berners-Lee, the inventor of the Web, reckons it was crucial, both for philosophical and technical reasons, to develop a net "out of control" (Berners-Lee 1999). Similarly, an Internet pioneer, Vinton Cerf, has declared that "by placing intelligence at the edges rather than control in the middle of the network, the Internet has created a platform for innovation. This has led to an explosion of offerings that might never have evolved had central control of the network been required by design" (Cerf 2007). Likewise, it is remarkable that on the side of the lawmakers, the Judiciary Report of the US Senate Committee, when discussing the aforementioned "safe harbour" clause of the *Digital Millennium Copyright Act* (DMCA), insisted on this very point: "In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand" (S. Rep. No. 105-190, p. 8). This "good balancing" of interests and rights involving ISP liability is also stressed by rulings: in the phrasing of *Zeran v. American Online*, "section 230 [of the *Communications Decency Act*] was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the *medium* to a minimum" (129F.3d 327, 330, 4th Circuit 1997).

However, some argue that today's legal balance is not "good enough". The use of generative technologies such as personal computers not only leads to an explosion of offerings and creativity on the Internet but also induces a new generation of offences as identity thefts and spamming in the field of computer crimes as well as activities of "rowdy web sites" like VampireFreaks.com on today's Web (Cohen-Almagor 2010). Moreover, in the 2010 Report on the "Application of D-2004/48/EC," that is, the EU Copyright Directive, the European Commission affirms that "despite an overall improvement of enforcement procedures, the sheer volume and financial value of IP rights infringements are alarming. One reason is the unprecedented increase in opportunities to infringe IP rights offered by the internet" (SEC-2010-1589 final). In order to stop such illegal activities, the European co-legislators have therefore suggested to overturn today's safe harbours of the law by adopting a set of provisions that severely impact on current obligations of ISPs. Consider the proposal of obliging ISPs to install "a system for filtering all electronic communications" and, especially, peer-to-peer (P2P) applications. Besides, the EU Commission is supporting a new generation of injunctions that should be taken against Internet intermediaries, *regardless of their liability*, with the aim to prevent "further infringements" even in the hypothesis of extraterritorial effects.

In light of today's polarization of the debate, the paper examines whether we should increase the set of current obligations of ISPs so as to integrate (or to overrule) the safe harbours of the law. In Section 2, I suggest three ideal-typical conditions in which individuals as well as corporations find themselves confronted with legal rules on liability. In Section 3, I consider different kinds of ISPs such as mere conduits, information distributors and financial mediators to emphasize the importance of these distinctions when discussing legal responsibilities and obligations of Internet intermediaries. The final section of the paper provides an assessment of what new responsibilities ISPs should have in connection with the information revolution and legal problems concerning the delimitation of jurisdictions, data processing, people's privacy and education. The aim was to show that the new responsibilities of ISPs follow from the original "end-to-end" architecture of the medium and policies on design rather than responsibility for user content and individual messages.

2 On Law and Responsibility

In order to examine the most relevant legal issues concerning the liability of ISPs, let me focus on three ideal-typical situations where corporations, as well as individuals, find themselves confronted with legal responsibility: (1) immunity, (2) faultless or strict liability, (3) responsibility that depends on individual "fault". A classical text such as Thomas Hobbes' *Leviathan* (1651) helps clarify some relevant facets of the distinction. As far as the first ideal-typical form of responsibility is concerned, immunity is grounded on the idea that "everything which is not prohibited is allowed". As remarked in Chapter 26 of *Leviathan*, once we assume that "the law is a command, and a command consisteth in declaration or manifestation of the will of him that commandeth", it follows that that command *must* be expressed "by voice, writing, or some other sufficient argument of the same". In criminal law, the principle corresponds to the clause of legal irresponsibility which is summed up, in Continental Europe, with the formula of the "principle of legality", i.e. "no crime, no punishment without a criminal law" (*nullum crimen nulla poena sine lege*). In civil law, most of the time, the principle is connected to clauses of contracts and obligations, where the condition of immunity is traditionally summed up with the Latin saying *ad impossibilia nemo tenetur*, that is, "no one is held to what is impossible". Likewise, lawmakers can establish forms of immunity through statutes. An example has been given with Section 230 of the *Communications Decency Act*: "No provider (…) shall be treated as the publisher or speaker of any information provided by another content provider".

Vice versa, the responsibility of traditional publishers clarifies the hypothesis of faultless liability or strict liability, i.e. the second ideal-typical form of responsibility. Notwithstanding eventual illicit or culpable behaviour, editors, publishers and media owners (newspapers, TV channels, radio, etc.) are liable for damages caused by their employees, e.g. pre-digital media's journalists or writers. This mechanism is at work in many other cases where law imposes liability regardless of the person's intention, as it occurs with people's responsibility for the behaviour of their pets and, in most legal systems, of their children. Whilst the *rationale* of the strict liability rule for

traditional publishers hinges on the "one-to-many" architecture of pre-digital medias, it is debatable whether this mechanism of distributing risk should be applied to current ISPs, given the "end-to-end" architecture of the Internet (Lessig 1999; Zittrain 2008). The difference can be illustrated with a case from May 2002, when a section of the Tribunal in Milan, Italy, likened the responsibilities of e-publishers to those of traditional editors pursuant to art. 1 of the Italian statute no. 62 from March 7, 2001. The provisions of the National Parliament made indeed no distinction between electronic and traditional publishing such as in newspapers, radio or television. What the ruling no. 6127 of the third civil section in Milan missed, however, is the specific purpose of this equalization, i.e. to make property assets transparent and to set the conditions for public supply. In other words, the Italian statute no. 62 from 2001 has not modified the general framework of art. 57 of the Italian criminal code in that *only* press editors and vice editors can be held strictly liable for crimes committed through their newspapers. This is what the Italian *Court of Cassation* confirmed in the decision no. 35511 from July 16, 2010. Either the Italian lawmakers change the rule or it would be illegal to apply the strict liability provision of the Italian criminal code's art. 57 to electronic publishing of ISPs such as in user-generated content (UGC) platforms, social network services (SNS) and the like.

Yet, most of the time, matters of liability are not only defined a priori, that is, by establishing them ex ante (strict liability rules) or excluding them overall (general legal irresponsibility). People are in fact liable for what they voluntarily agree upon through strict contractual obligations and, moreover, for obligations that are imposed by the government to compensate damage done by wrongdoing. Whilst there is liability for intentional torts when a person has voluntarily performed the wrongful action prohibited by the law, legal systems provide for liability based on lack of due care when the "reasonable" person fails to guard against "foreseeable" harm. This kind of liability is therefore grounded on the circumstances of the case, as the wording of the aforementioned Section 512(c) of DMCA clarifies: "a service provider shall not be liable for monetary relief (…) *if* the service provider does not have actual knowledge that the material or an activity using the material on the system is infringing".

Furthermore, this kind of responsibility grounded on our own "fault" is entwined with the general clauses of immunity previously discussed. For instance, in the 2009 Opinion on social networks, the European privacy commissioners, that is, the EU Working Party art. 29 D-95/46/EC, affirmed that ISPs as well as SNS should provide information and adequate warning to users about privacy risks when uploading data: "users should be advised by SNS that pictures or information about other individuals, should only be uploaded with the individual's consent" (WP 29 2009a). Suggesting some convergences with the legal framework established by Section 512 of DMCA, this means that ISPs and SNS have no general obligation to monitor the information they transmit or store, although ISPs and SNS should inform users that they are personally liable for their behaviour online (as confirmed by cases of defamation and copyright or privacy infringements). Besides, "many-to-many" services such as SNS and UGC platforms are liable when they fail to remove illegitimate content after having actual knowledge of facts or circumstances indicating illegal activity or been asked to remove that content by a judicial authority.

However, some argue that this legal balance is not "good enough", in that ISP liability should not be understood with the "end-to-end" metaphor of telephone carriers (or road network managers), with which safe harbour clauses are traditionally entwined. Rather, we should grasp ISP responsibility with the metaphor of bookstores and libraries where people are liable for the volumes they select and place on their shelves: "in both kinds of store, store owners would like to keep the business going. They will listen to alerts about the illegality of certain books" (Cohen-Almagor 2010). As a consequence, *if* we admit that current default rules on ISP irresponsibility should be abandoned, *then* one option is to go back to the aforementioned strict liability rule of traditional publishers and editors. In both cases, people should be held liable regardless of any eventual illicit or culpable behaviour because it is their "one-to-many" responsibility to preventively control the information transmitted by TV channels, radios, newspapers and—why not?—bookstores, libraries and ISP services. ISPs should indeed monitor the information they transmit or store so as to actively seek for facts or circumstances indicating illegal activity (*pace* Article 15 of the EU Directive 2000/31 on e-commerce). Moreover, some forms of speech should be restricted by forcing people to sign up for reading and viewing "some problematic material" whilst "providing some details about their identity and why they wish to read this particular piece of information" (Cohen-Almagor 2010).

Leaving aside the problematical definition of "some problematic material", it is nonetheless unclear why ISPs "*should* aspire to take responsibility for content" (*ibid*). There are many reasons why the default rule of ISP legal immunity plays an irreplaceable role in the development and enrichment of the "properties" of the Internet: it is more than likely that applying the "one-to-many" *rationale* of strict liability rules to the "many-to-many" nature of most services on the Internet would have perverse effects for the flourishing of the "infosphere" and its informational objects (Floridi 2003). All in all, such a "one-to-many" policy risks to "stop the future of the Internet" (Zittrain 2008), and new ways of providing services, e.g., Apple's mosaic of i-services and Facebook's "digital walls," have suggested *Wired*, a popular magazine, to provocatively announce, in September 2010, that "The Web is dead" (Anderson 2010; Wolff 2010).

Still, apart from strict liability rules and clauses for legal irresponsibility, i.e. safe harbours, there is a third way to interpret the new responsibilities of ISPs, namely, in accordance with the type of liability grounded in "fault" or individual "culpa". When scholars claim that "ISPs and web-hosting companies should aspire to take responsibility for content" and behaviour of the users (Cohen-Almagor 2010), it is not necessary to establish a new strict liability rule. As a matter of legal fact, it would be enough to increase the set of current obligations of ISPs in order to integrate, and not overrule, current default rules of immunity. Even in such a case, however, we should further distinguish between contractual and extra-contractual obligations of *different types* of ISPs. In the case of contractual obligations, fault is strictly related to the clauses we have voluntarily agreed upon through pacts: most of the time, issues concern the alleged rights of the ISP involved, e.g. property rights over personal data of users rather than ISPs' responsibility for individual conduct or user-generated content. Vice versa, in the case of extra-contractual responsibility, legal claims tend to converge on the notion of "unjust damages" that, nevertheless, would

require to differentiate the multiple services ISPs provide, e.g. connectivity to the Internet and tools for publishing and retrieving information online. Whilst levels of control over information impact differently on the flourishing of the Internet, it is urgent to find an agreement on a common categorization of ISPs so as to determine what type of new obligations should set their liability.

3 Classes of ISPs

The new generation of legal problems induced by the information revolution mainly concern matters of access and control over information in digital environments. This is the typical case of privacy and data protection, copyright and, of course, ISP responsibilities. More particularly, these latter responsibilities have to do with people's *access* to the net and the archipelago of its services, as well as how ISPs *control* (or how they should run) this information fairly. Legal responsibilities of ISPs ultimately depend on the panoply of functions and services they provide on the Internet, where levels of control over information affect how this information is shared by individuals. In order to clarify different levels of legal responsibilities, let me mention two examples of how ISPs' activities have been categorized.

First, we have the distinction made by the US and EU provisions on ISP limited liability. In the USA, the DMCA "safe harbour" clause refers to intermediates' routine activities so as to distinguish the responsibilities of ISPs when they act as a *conduit* of Internet communications, as a *cache* of material, as a *host* of user-generated content or as a *provider* of information *location tools* and *search engines* (17 U.S.C. Section 512). In Europe, Directive 2000/31 on e-commerce similarly differentiates ISPs acting as a "mere conduit" (art. 12), "caching" (art. 13) or "hosting" information (art. 14). On this basis, legal systems provide for different kinds of legal immunity depending on the ways ISPs transmit or distribute information. In the EU legal system, for example, there are three different "safe harbours":

1. A mere conduit is not liable if the provider does not initiate the transmission or select receivers of the transmission or modify the information contained in the transmission itself;
2. In the case of caching, the provider is not liable if, and only if, it complies with conditions and rules on accessing or updating information and does not interfere with "the lawful use of technology";
3. Finally, when services consist in "hosting", i.e. storing information provided by a recipient of the service, the immunity rule requires that "the provider does not have actual knowledge of illegal activity or information" and, once obtained, "such knowledge or awareness, acts expeditiously to remove or to disable access to the information" (art. 14.1 a-b of D-2000/31/EC).

A second typology has been offered by the Civil Society Information Society Advisory Council (CSISAC 2009). Here, the classification hinges on the *architecture* through which services and tools are provided so that we should differentiate ISPs that act as mere conduits by providing connectivity to the Internet, information distributors such as search engines, hosting providers or social network sites and, finally, intermediaries that facilitate e-commerce and online activity such

as financial intermediation. The CSISAC document stresses the different *levels of control ISPs have over the information transmitted and shared through their services*. Such a level of control is critical when determining the legal responsibilities of ISPs: "Legal rules for imposition of liability must take into account the level of control (if any) that an Internet intermediary exercises over user conduct and unlawful material, but this consideration should not be mistaken with a mandate to redesign the service or product. Rules must be based on actual ability to control, and not the mere assertion of an obligation to control" (CSISAC 2009). So, different "levels of control" related to the services, functions and architecture of ISPs allow us to re-examine matters of responsibility and immunity by distinguishing ISPs in two classes, that is, *transmission intermediaries* and *information distributors*.

In the case of transmission intermediaries, responsibility depends on the nature, role and functions of "mere conduits", i.e. services that "consist of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network" (art. 12 of the EU Directive on e-commerce). Leaving aside parallelisms with librarians and booksellers (Cohen-Almagor 2010), the similarity with the responsibility of managers and administrators of highways seems particularly instructive. Providers of transmission intermediary services should not have any responsibility for what people do once individuals access digital and traditional freeways: in both cases, the architecture of the system suggests the similar balancing in that it is people's responsibility to drive safely and prevent accidents on the highways, just like it is the responsibility of the "end-to-end" and "many-to-many" intermediaries of digital and traditional highways to keep their services functioning even after an accident. Today's clauses determining the immunity of the type of ISP that functions as transmission intermediary should be considered to be appropriate for this end. Such clauses have been determinant in the flourishing of the Internet and its services. Moreover, the alternative could be illustrated with the example of road network managers with police functions in totalitarian regimes, e.g. militarized highways in ex DDR.

Needless to recall the regime of liability for the "one-to-many" road network managers in ex DDR, to understand what is wrong when some Western states treat ISPs as a sort of "digital sheriff" (Pagallo 2008). Notwithstanding clauses of legal irresponsibility, this is what occurred in the USA when a general obligation has been imposed on transmission intermediaries to track people's behaviour on the Internet. The lawsuit opposing an American ISP, Verizon, and the Recording Industry Association of America (RIAA) is an illustration of how people's rights on the Internet are "threatened under certain interpretations of the Digital Millennium Copyright Act (DMCA) in the United States [as] a new form of 'panoptic surveillance' that can be carried out by organizations such as the RIAA" (Grodzinsky and Tavani 2005). Likewise, copyright crusades have spread throughout Europe: on October 22, 2009, the French Parliament passed a law establishing the *Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet*, i.e. the HADOPI law. Following the "three strikes" doctrine of the statute, French transmission intermediaries have been sending the first e-mails of the *Haute Autorité* in October 2010 as a part of the graduated system that ultimately leads to the disconnection of the user after three warnings. Although it is not possible to examine all the details of the HADOPI law and similar statutes, e.g. the South Korean

copyright law, it suffices to stress why a general obligation imposed on transmission intermediaries making them monitor the net seems legally flawed.

On one hand, against the "three strikes" doctrine, there is the *literal* meaning of safe harbour clauses such as art. 15 of D-2000/31/EC: there is indeed "no general obligation to monitor the information…". Even in the *Vividown case*, where some Google's executives were held responsible for an "illicit treatment of personal data" pursuant to article 167 of the Italian Data Protection Code, the Tribunal of Milan, Italy, carefully stressed that no such a "general obligation to monitor the information" exists (decision 1972 from February 24, 2010). On the other hand, further decisions on data protection and the principle of proportionality seem to confirm the view. Let me only mention the case before the European Court of Justice on January 29, 2008 (C-275/06), in the lawsuit opposing another ISP, *Telefónica de España*, and the recording industry association of Spain, *Promusicae*. On that occasion, Justices in Luxembourg affirmed that the EU law does *not* require Member States to lay down "an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings" (Section 70 of the decision).

What all these cases suggest is to grasp legal responsibilities of transmission intermediaries on the Internet with the metaphor of traditional immunity of road network managers. The analogy is confirmed by simply substituting the word "transmission" of art. 12 and 15 of the EU Directive on e-commerce, with the word "car". The general provision of the directive setting up "no general obligation to monitor the information which ISPs transmit or store" accordingly states "no general obligation to monitor the information which the car transmits or stores while using the highway, no a general obligation actively to seek facts or circumstances indicating illegal activity" in that speedway. The principle that reasonably applies to road network managers should comprehend transmission intermediaries as well. But how about the second "level of control" and the corresponding liability of ISPs as information distributors? Does the immunity clause applicable to the kind of ISPs that provide transmission intermediation extend to ISPs that distribute information?

In connection with clauses on hosting in Section 512 of the US Code and art. 14 of D-2000/31/EC, we should assess the responsibilities of ISPs by distinguishing illegal material on web sites, people's conduct and, foremost, data protection. Services of information distribution and hosting of user content and personal data have in fact induced lawmakers and scholars to support a *stronger* responsibility of these ISPs because levels of control in distributing information have a greater impact on individuals looking for sites and information through search engines, posting on hosting providers, interacting via social networks, purchasing on video and auctions platforms, or simply blogging. In accordance with the context-dependent approach put forward by Helen Nissenbaum, I agree that this greater level of control is legitimate and "integral to the transaction between a merchant and a customer that the merchant would get to know what a customer purchased. (…) Although the online bookseller Amazon.com maintains and analyses customer records electronically, using this information as a basis for marketing to those same customers seems not to be a significant departure from entrenched norms of appropriateness and flow" of information (Nissenbaum 2004). Yet, there are more critical cases.

Greater levels of control are at stake when user behaviour is electronically processed by, say, Facebook's headquarters or when Google processes personal data

through the mosaic of its services. Different levels of control have suggested lawmakers in the USA and Europe to reinforce obligations and responsibilities for information distributors: for example, in the Opinion of the EU Working Party art. 29 on social networks, the European privacy commissioners propose that SNS should be held responsible for providing information and adequate warning to users about privacy risks when uploading data, e.g. SNS should "advise" users to request people's consent when uploading pictures or information about other individuals (WP 29 2009a). However, this stronger form of responsibility of information distributors in "advising" SNS users does not mean these ISPs have to look after the conduct of users, as if they were pupils in schools and the ISPs the teachers. By increasing the list of obligations that define ISP liability, it does not follow that we should change today's "golden rule" that information distributors are literally *irresponsible* for what people say and how they behave on the Internet, lest they start "modifying the information" of the users (as Section 1a of art. 13 of the EU Directive on e-commerce states). Until ISPs host information and do not judge or assume responsibility for content by selecting it, the only duty of SNS like Facebook or UGC platforms like YouTube is to remove or to disable access to the information they have stored once they obtain knowledge of illegal activity, and as far as claims for damages are concerned, these ISPs are not aware of circumstances making the illegal activity or information apparent. This safe harbour clause should be kept as it is (Sartor and Viola 2010).

Still, it would be naive to think that gigantic information distributors like Apple, Google or Facebook do not "modify the information" of the users. It is not only an open question whether methods of automated filtering of information are compatible with the "neutrality" of ISPs in sectors as keyword advertising, trademarks, search engines, social networks and the like. In fact, matters of trust and privacy on the Internet are suggesting private companies and some hundred million people to opt for more reliable, yet sterile, appliances: mobile phones, e-books and video games consoles are creating a set of digital walls as Facebook's closed e-mail system or Apple's model of services and mobile devices. Confronted with the previous generation of information distributors, these new ISPs not only control the architecture of the system with its apps, e.g. 250.000 only for i-Phones, but determine control over the content of the communication as well, e.g. Facebook's terms of service, so that the ISP has the right to unilaterally disconnect user groups or block discussion pages.

Whether or not you agree that restrictions for freedom of speech are necessary (Waldron 2010), the "neutrality" of the service, on which the responsibility of both new and old ISPs depends, is legally recast by the evolution of automated systems for the processing and filtering of huge amounts of data through search engines, data mining or cloud computing. The information revolution is indeed blurring key legal distinctions such as the difference between "controllers" and "processors" of data (WP 29 2010); it is also radically changing how information distributors *do* "modify the information" of the users. Whereas work on AI, ontologies and design theory applied to legal systems are shedding further light on how the new responsibilities of ISPs can be addressed, development on the Internet of the things, smart environments and the "semantic Web" (Breuker et al. 2009) force us to *rethink* ISPs with their responsibility and immunity clauses.

4 New Responsibilities of ISPs

Current debate on the new responsibilities of ISPs may be summarized in light of a polarization. On one hand, some stress that ISPs should be responsible for user content on their web sites so as to control or avert illegal activities such as child pornography, defamations and so forth: "the issue is not the neutrality of the Net, but whether we should be neutral regarding this kind of content. Morally speaking (…) we cannot be neutral regarding such alarming speech" (Cohen-Almagor 2010). On the other hand, privacy commissioners and data protection authorities deem ISPs responsible for the design of their services rather than content of users' messages. In the 2009 document on "The Future of Privacy", for example, the EU Working Party art. 29 has proposed that global issues of data protection have to be approached by "incorporating technological protection safeguards in information and communication technologies". In other words, the principle of privacy by design "*should be binding* for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT" (WP 29 2009b).

Significantly, both approaches to the new responsibilities of ISPs, e.g. liability for user content and liability for the design of ISP services, converge on matters of jurisdiction and the regulative effects of technology. Regardless of the ways ISPs transmit, store or distribute information, most of today's troubles with law enforcement depend, in fact, on the architecture of the Internet and how ISPs can alternatively be obliged to employ different design mechanisms. Next, in Section 4.1, I will focus on the impact of technology on current issues of jurisdiction through the employment of digital right management (DRM) devices. After the design and use of alleged self-enforcement technologies, Section 4.2 dwells on further goals design may aim at, such as limiting the "informational entropy" of the system or encouraging the change in people's behaviour. In Section 4.3, finally, I focus on the educational aspects of designing information and communications technology (ICT) and other types of technology, with the aim to decrease the impact of harm-generating conducts and to guarantee people's rights by widening the range of their choices. In order to proceed with the analysis of the new responsibilities of ISPs and whether we should change the safe harbours of the law, let me then start with the power to "speak the law" (*dicere ius*), that is, juris-diction.

4.1 Jurisdiction

International conflicts of law and the traditional criteria of "pertinence to the territory" used in legal systems are notoriously a nightmare for scholars. Part of the problem hinges on the limits of both international private and public law which, even in cases such as defining individual citizenship regime, have turned out to be "a recipe for chaos" (Bauböck 1994). In the case of ISPs' responsibilities, most of the problem revolves around the Internet and the fact that no clear legal boundaries exist in digital environments. State action is often ineffective due to the ubiquitous nature of information processed by transmission intermediaries or information distributors. Whilst citizens of nation states are often affected by conduct that the state is unable to regulate (e.g. spamming), this situation may also lead to the illegitimate condition where a state claims to regulate extraterritorial

conduct by imposing norms on individuals who have no say in the decisions affecting them (Post 2009).

In addition, the ineffectiveness of state action depends on how ICT allows information to transcend traditional legal borders, questioning the notion of the law as made up of commands enforced through physical sanctions. Spamming is again a good example for it is *par excellence transnational* and does not diminish despite harsh punishment (as the *CAN-SPAM Act* approved by the US Congress in 2003). Since the mid-1990s, consequently, companies and big business have tried to find a remedy for the apparent inefficacy of state action in protecting private rights. Whilst lobbying national and international lawmakers in the field of copyright, some of the most important companies focused on how to enforce their (alleged) exclusive rights through the development of self-enforcement technologies such as DRM. By enabling right holders to monitor and regulate the use of their copyright-protected works, companies would have prevented unsolvable problems involving the enforceability of national laws and conflicts of law at the international level.

Yet, attention should be drawn to the difficulties of achieving such total control. Doubts cast by "a rich body of scholarship concerning the theory and practice of 'traditional' rule-based regulation bear witness of the impossibility of designing regulatory standards in the form of legal rules that will hit their target with perfect accuracy" (Yeung 2007). As Steve Jobs concedes in his *Thoughts on Music* (2007), DRM-compliant systems raise severe problems of interoperability and, hence, antitrust-related issues. Moreover, the use of DRM techniques involves strong responsibilities of ISPs because a kind of infallible self-enforcement technology not only collapses "the public understanding of law with its application eliminating a useful interface between the law's terms and its application" (Zittrain 2007). What is more, as a response to the inefficacy of state action, the use of DRM technology risks to severely curtail freedom and individual autonomy since people's behaviour would unilaterally be determined on the basis of technology rather than by choices of the relevant political institutions.

Another problem concerning the ineffectiveness of state action is admitted by lawmakers and privacy commissioners in Europe: they stress the *impossibility* to protect people's fundamental rights *without* the cooperation of private corporations. In the Opinion from July 25, 2007, the European Data Protection Supervisor, Peter Hustinx, significantly affirmed that the challenge to protect personal data at the international level "will be to find practical solutions" through typical *transnational measures* such as "the use of binding corporate rules by multinational companies" and the promotion of "private enforcement of data protection principles through self-regulation and competition". The reason hinges on the peculiarity of "this system, a logical and necessary consequence of the territorial limitations of the European Union, [that] will not provide full protection to the European data subject in a networked society where physical borders lose importance (…): the information on the Internet has an ubiquitous nature, but the jurisdiction of the European legislator is not ubiquitous" (Hustinx 2007).

Although most *transnational* measures apparently concern ISPs' "good will" to be compliant with law enforcement, what data protection authorities and privacy commissioners are really suggesting is a stronger *legal* responsibility. As previously said, the EU Working Party art. 29 has declared that global problems of enforcing

people's rights should be approached by embedding data protection safeguards in ICT so that the principle of privacy by design should be binding for ISPs (WP 29 2009b). Ever since the first European directive on data protection, lawmakers declared that their intention was to embed "appropriate measures" in ICTs "both at the time of the design of the processing system and at the time of the processing itself" (according to the phrasing of the recital 46 of D-95/46/EC).

However, the impact of design on social relationships and on the functioning of legal systems has to do with a number of relevant issues: not only privacy and data protection but also universal usability, informed consent, crime control, social justice and more. Due to the panoply of possible applications, it is thus important to pay attention to the different goals design may aim at. After all, a new responsibility of ISPs for the design of their services, e.g. the 2009 Working Party's proposal on the principle of privacy by design, ultimately depends on the multiple and even opposite goals design may pursue.

4.2 Design

In their work on *The Design with Intent Method*, Lockton et al. (2010) describe 101 ways in which products can influence the behaviour of their users: in this context, dealing with the new responsibilities of ISPs, it suffices to insist on three aims of design (Yeung 2007). In fact, by embedding legal rules in information technology, (1) Design may encourage the change of social behaviour; (2) It may aim to decrease the impact of harm-generating conducts; (3) Design may finally prevent harm-generating behaviour from even occurring.

In order to illustrate the first modality of design, consider the case of the free-riding phenomenon in P2P networks where most peers tend to use these applications to find information and download their favourite files without contributing to the performance of the system. Whilst this selfish behaviour is triggered by many properties of P2P applications like anonymity and hard traceability of the nodes, designers have proposed ways to tackle the issue through incentives based on trust (e.g. reputation mechanisms) and trade (e.g. services in return). The idea is to encourage the change of people's behaviour and enrich the flow of information in P2P systems so that "the receiver can recompense the provider immediately, during or after the service provision, or she can promise a service in return" (Glorioso et al. 2010). This kind of design mechanism seems ultimately fruitful since the aim is by definition to widen the range of people's choices rather than imposing social conduct by design.

The second modality is represented by efforts in deploying security measures (von Ahn et al. 2008), friendly interfaces (Norman 2007) or network approaches to privacy (Pagallo 2010): the goal is to decrease the impact of harmful behaviour rather than changing people's way of behaving. By embedding data protection safeguards in ICT or by designing spaces, processes and products, this sort of "digital air bags" prevents the informational entropy of the "infosphere" (Floridi 2003). For instance, it is feasible to program video surveillance systems in such a way that faces of individuals cannot be recognized. Furthermore, such design techniques apply to the realm of ISPs as well, as Facebook's issues with data protection laws confirmed on May 26, 2010. On that occasion, the social network

announced to have "drastically simplified and improved its privacy controls" which previously amounted to 170 different options under 50 data protection-related settings. Leaving aside Facebook's problems with data protection, it is clear that this type of design mechanism can decrease the impact of harm-generating behaviour by setting the default configuration of the system so as to ensure minimization and quality of personal data.

The final mechanism of design pertains to the goal of preventing harm-generating behaviour from occurring. Besides DRM techniques, some claim that this mechanism entails new ISP responsibilities in the field of privacy by design (Cavoukian 2010). The Ontario's Privacy Commissioner, in fact, is convinced that the full functionality of the principle allows a "positive sum" or "win–win" game, making trade-offs between privacy and business, or privacy and security, unnecessary. Personal data should be *automatically* protected in every IT system as the *default* rule and according to a cradle-to-grave, start-to-finish or end-to-end life cycle protection approach so that privacy safeguards would be at work even before a single bit of information has been collected (Cavoukian 2010). Contrarily to the previous approaches to design, however, the idea of designing legal systems and ISPs to *automatically* prevent "illegal activities" seems highly problematic. Unlike, say, efforts in security measures or reputation mechanisms, the idea of obliging ISPs to install "a system for filtering *all* electronic communications," as the European Commission suggested in the aforementioned 2010 Report on the copyright directive (SEC-2010-1589-final), would neither be desirable nor feasible for three reasons.

First, there is the technical difficulty of applying to a machine concepts traditionally employed by lawyers through the formalization of norms, rights or duties. Informational protection safeguards not only include top normative concepts such as notions of validity, obligation and prohibition but also present highly context-dependent notions as personal data, security measures and data controllers. These notions raise a number of relevant problems when reducing the informational complexity of a legal system where concepts and relations are subject to evolution (Casanovas et al. 2010). Whilst issues of jurisdiction considered in the previous section can hardly be reduced to a software engineering debate, *10 years of efforts* on platforms for privacy preferences show that "the P3P specification is not yet mature enough in terms of element definitions to handle many legal subtleties cleanly" (Jutla 2010). To the best of my knowledge, it would be impossible to program software so as to prevent forms of harm-generating behaviour as simple as defamations: such constraints emphasize critical facets of design ethics which lie behind the use of allegedly perfect self-enforcement technologies (Pagallo 2009).

Second, design approaches to privacy as "automatic control" appear even more problematic than the use of DRM technology for the protection and enforcement of digital copyright because data protection does not represent an automatic zero sum game between multiple instances and options of access and control over information in digital environments. Personal choices indeed play the main role when individuals modulate different levels of access and control, depending on the context and its circumstances (Nissenbaum 2004). Moreover, people may enjoy privacy in the midst of a crowd and without having total control over their personal data, whereas total control over that data does not necessarily entail any guarantee of privacy (Tavani 2007). As a result, the use of self-enforcement technology updates traditional forms

of paternalism since people's behaviour would unilaterally be determined on the basis of automatic techniques rather than by individual choices on levels of access and control over information: "the controls over access to content will not be controls that are ratified by courts; the controls over access to content will be controls that are coded by programmers" (Lessig 2004).

Third, there is evidence that "some technical artefacts bear directly and systematically on the realization, or suppression, of particular configurations of social, ethical, and political values" (Flanagan et al. 2008). Whilst specific design choices may result in conflicts between values, vice versa, conflicts between values may impact on the features of design. Although legal systems help us overcome a number of conflicts between values (Flanagan et al. 2008), it is likely that the use of alleged self-enforcement technologies in fields as, say, data protection, would worsen conflicts between values due to specific design choices, e.g. the opt-in vs. opt-out diatribe over the setting for users of information systems. We should instead adopt a stricter version of the principle that both transmission intermediaries and information distributors should be held responsible for "the acquisition and use of ICT" (WP 29 2009b). It seems fair to add a *new* responsibility of ISPs, i.e. liability for the design of their services if, and only if, the aim is to decrease the impact of harm-generating conducts (e.g. "digital air bags") or to encourage the change of people's behaviour (e.g. incentives and services in return).

Such a stricter approach to design policies brings us back to the polarization between supporters of liability for the design of ISP services and ISP liability for user content. Some scholars affirm that projects for user control like P3P, PeCAN or HCI-related privacy models "implicitly have an educational aspect to them" (Jutla 2010). Moreover, advocates of a stronger responsibility of information distributors argue that under certain circumstances, ISPs even have a responsibility to "advise" their users (WP 29 2009b). After all, the educational aspects of design are a popular topic of work on design ethics (Grodzinsky et al. 2008; Flanagan et al. 2008). Among the new responsibilities of ISPs, let me finally examine how ISPs should "educate" people when using their services. We have to avert a further risk of design mechanisms that encourage individuals to change their conduct.

4.3 User Education

Education represents a further reason why we should be cautious with the use of self-enforcement technologies. By ensuring compliance with regulatory frameworks through design safeguards embedded in ICT, the risk is to end up in sheer paternalism to model individual behaviour according to what the lawmaker or the programmer wants. Not only do the editorials in *The Economist* often stress this threat, but so also scholarly criticisms of the European data protection policies (Kuner 2003). Richard Volkman, for example, claims that the European legal framework "is clearly and deeply flawed as an account of what informational protection is all about" in that "restrictions are so sweeping that many perfectly legitimate business models are de facto outlawed by such a law" (Volkman 2003). Moreover, paternalism seems being conquering the USA too: "The University of Florida has created a software tool called ICARUS that monitors traffic over its network, identifies traffic that appears to be characteristic of peer-to-peer file

sharing, and then suspends network service to the computer generating the traffic for 30 minutes. *Users may regain network access only if they complete a 10-minute interactive presentation of copyright law*" (Cohen-Almagor 2010). In order to prevent misunderstandings, it is crucial to agree upon the meaning of "education" in this context and the difference between education and authoritative imposition.

To start with, even though the new responsibilities of ISPs concern user education, the goal should not be the well-being of citizens by protecting them from any harm: such a claim amounts to paternalism (Kant 1795, ed. 1891). Rather, a stricter focus on the functions and architecture of ISPs is needed so that you are not required to be a supporter of the institutions in Brussels, to follow the EU WP29's proposal that the principle of privacy by design should be implemented in accordance with a bottom-up rather than top-down approach, that is, based on autonomous individual choices via self-regulation and competition among private organizations (WP 29 2009b). Besides, matters of education often depend on people simply ignoring what they are doing when they are, say, connected in P2P, namely, becoming servers and clients at the same time. Education will increasingly be required all the more as technology speeds up this process through the Internet of the things, the semantic web, cloud computing and social networks. Evidence suggests that transmission intermediaries and information distributors can improve the flourishing of the Internet either by decreasing the impact of harmful conducts through "digital air bags" (e.g. security measures and data protection by default settings) or by encouraging the change of user behaviour through design policies (e.g. P2P reputation mechanisms). Therefore, we may deem that ISPs have the responsibility to promote the flourishing of the informational objects in (a certain area of) the "infosphere" (Floridi 2003) by broadening the range of choices available to people through design mechanisms that protect individual rights. Such a meaning of the "educational" role of ISPs is not new in the field of design ethics (Grodzinsky et al. 2008; Flanagan et al. 2008); in fact, it is feasible to embed legal safeguards in products, processes and services so as to prevent claims of paternalism and show how a "win–win" business model is viable (Pagallo and Durante 2009; Glorioso et al. 2010). On this basis, current research in legal architectures, codes and design allows us to restrict the meaning of "education" in three ways:

1. There is no education when self-enforcement technologies are employed, lest users reflect upon what they actually are forced to do;
2. Education does *not* mean to directly *change* people's conduct: in the case of ISPs, the aim should be to limit the effects of harm-generating behaviour or, alternatively, to encourage people's change of behaviour;
3. In this latter case, education may legitimately aim to *encourage* the *change* of individual conduct only when the range of choices available is widened via transparent settings, friendly interfaces and the like.

The legal responsibility of ISPs to "educate" users finds, on this basis, a possible convergence with the EU WP29's claim that "privacy by design" should be legally binding. Once we dismiss the opposite view of automatic control over user content on (rowdy) web sites through self-enforcement technologies, ISPs' responsibility to take care of the design of their services fits like hand in glove to the spirit of today's default rules on legal liability. Instead of worrying about "rowdy websites

entertained by rowdy ISPs" (Cohen-Almagor 2010), we should address "the amount of work and efforts required for a certain kind of agent to obtain, filter and/or block information (also, but not only) about other agents in a given environment" (Floridi 2006). In light of different "degrees of friction" that are required to keep distinctions firm between agents and systems, the impact of design on the ways services are provided on the Internet can be positively oriented to respect the principle of "neutrality" on which current legal clauses on immunity rely. Do we really want to change today's safe harbours of the law?

5 Conclusions

Focusing on the new responsibilities of ISPs, I have stressed the necessity to preliminarily distinguish between the multiple services they provide. Whilst transmission intermediaries propose a parallelism with the responsibility of managers and administrators of speedways, e.g. legal immunity for what people say or do in both digital and traditional highways, ISPs that distribute or host information should arguably have a *stronger* responsibility because services such as search engines, social networks, UGC platforms or auction web sites have a greater level of control over people interacting, looking for sites, posting, blogging and so forth. Over the past years, most (Western) lawmakers have reinforced obligations and responsibilities for this kind of "information distributors" so as to integrate, *without overturning*, default rules of immunity for all ISPs. The aim has been to strengthen people's right to access their data and to oversee how "hosting services" and "providers of information-location tools" comply with provisions on users consent, minimization and quality of the data, transparency of the processing, confidentiality of the communications, down to the user friendliness of information interfaces.

Still, the "neutrality" of the service and the correspondent ISPs' irresponsibility are strictly entwined with the current information revolution and the ways automated systems for the processing and filtering of huge amounts of data are evolving. It is likely that new legal responsibilities of ISPs will emerge as a result: however, it is unclear how the new responsibilities should exactly be disciplined. Some argue that we should change the current safe harbours of the law because information distributors such as SNS, UGC platforms and blogs ought to be responsible for user content and should prevent illegal activities such as child pornography, defamations, copyright infringements and more. Others oppose this view since ISPs' responsibilities would depend on the design of their services rather than individual conduct. At the end of the day, should we follow the bottom-up approach of the Working Party's proposal for design policies or, rather, the plan of the European Commission to amend both copyright and e-commerce directives?

I argue that, *pace* the EU Commission, today's safe harbours of the law should be kept firm. The default rule of irresponsibility for both information distributors and transmission intermediaries represented a crucial condition for the explosion of creativity and offering of services on the Internet. Whether it may be necessary to integrate the list of ISPs' responsibilities and obligations on law enforcement, data protection, take-and-down procedures and so on, it is more than likely that applying the "one-to-many" rationale of strict liability rules to the "many-to-many" services

on the Internet would have perverse effects. By changing the current safe harbours with an obligation to monitor people's information that ISPs transmit, store or distribute, we would transform ISPs into road network managers with police functions, that is, "digital sheriffs". The new responsibilities of ISPs should conversely be conceived in accordance with a stricter approach to design policies. Leaving aside the idea of developing design mechanisms so as to oblige (or permit) ISPs to monitor and control individual conduct via "systems for filtering all electronic communications", according to the goals of the European Commission, what we would expect is that ISPs improve the design of their services by limiting the impact of harmful acting (e.g. security measures) whilst encouraging people to change their conduct by widening the range of their choices (e.g. user-friendly interfaces). The new responsibilities of ISPs, indeed, concern current policies on design and the original "end-to-end" architecture of the medium rather than liability for individual messages and user-generated content: the aim should be to incentive autonomy via self-regulation and competition among private companies. This seems a good balance between clauses of immunity and new forms of liability when providing services on the Internet.

References

Anderson, C. (2010). The Web is dead: Who's to blame—Us. *Wired*, September, pp. 123–127, 164.

Bauböck, R. (1994). *Transnational citizenship: Membership and rights in international migration*. London: Elgar.

Berners-Lee, T. (1999). *Weaving the web*. San Francisco: Harper.

Breuker, J., Casanovas, P., Klein, M., & Francesconi, E. (Eds.). (2009). *Law, ontologies and the semantic web*. Amsterdam: Ios Press.

Casanovas, P., Pagallo, U., Sartor, G., & Ajani, G. (Eds.). (2010). *AI approaches to the complexity of legal systems. Complex systems, the semantic web, ontologies, argumentation, and dialogue*. Berlin: Springer.

Cavoukian, A. (2010). Privacy by design: The definitive workshop. *Identity in the Information Society, 3* (2), 247–251.

Cerf, V. (2007). User-generated content is top threat to media and entertainment industry. Accenture, April 16.

Cohen-Almagor, R. (2010). Responsibility of and trust in ISPs. *Knowledge, Technology & Policy, 23*(3–4), 381–397.

CSISAC (2009). *Comments to OECD on information intermediaries*. The Civil Society Information Society Advisory Council, June 30th, 2009. Retrieved 3rd November 2010 from http://csisac.org/docs/OECD_Intermediary_071409_final.pdf.

Flanagan, M., Howe, D. C., & Nissenbaum, M. (2008). Embodying values in technology: Theory and practice. In J. van den Hoven & J. Weckert (Eds.), *Information technology and moral philosophy* (pp. 322–353). New York: Cambridge University Press.

Floridi, L. (2003). On the intrinsic value of information objects and the infosphere. *Ethics and Information Technology, 4*, 287–304.

Floridi, L. (2006). Information technology and the tragedy of the good will. *Ethics and Information Technology, 8*(4), 253–262.

Glorioso, A., Pagallo, U., & Ruffo, G. (2010). The social impact of P2P systems. In X. Shen, H. Yu, J. Buford, & M. Akon (Eds.), *Handbook of peer-to-peer networking* (pp. 47–70). Heidelberg: Springer.

Grodzinsky, F. S., & Tavani, H. T. (2005). P2P networks and the *Verizon v. RIAA* case: Implications for personal privacy and intellectual property. *Ethics and Information Technology, 7*(4), 243–250.

Grodzinsky, F. S., Miller, K. A., & Wolf, M. J. (2008). The ethics of designing artificial agents. *Ethics and Information Technology, 10*, 115–121.

Hobbes, T. (1651). *Leviathan (1982 edition)*. New York: Penguin.

Hustinx, P. (2007), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. *Official Journal of the European Union*, 2007/C 2551/01, July 25th 2007.

Jobs, S. (2007). *Thoughts on music*. Retrieved 20th April 2009 from http://www.apple.com/hotnews/thoughtsonmusic/.

Jutla, D. N. (2010). Layering privacy on operating systems, social networks, and other platforms by design. *Identity in the Information Society, 3*(2), 319–341.

Kant, I. (1795). *Kant's principles of politics, including his essay on perpetual peace. A contribution to political science* (translated by W. Hastie). Edinburgh, Clark, 1891.

Kuner, Ch. (2003). *European data privacy law and online business*. Oxford: Oxford University Press.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lessig, L. (2004). *Free culture: The nature and future of creativity.* New York: Penguin.

Lockton, D., Harrison, D. J., & Stanton, N. A. (2010). The design with intent method: A design tool for influencing user behaviour. *Applied Ergonomics, 41*(3), 382–392.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

Norman, D. A. (2007). *The design of future things*. New York: Basic Books.

Pagallo, U. (2008). *La tutela della privacy negli USA e in Europa. Modelli Giuridici a Confronto*. Milano: Giuffrè.

Pagallo, U. (2009). Privacy e design. *Informatica e Diritto, 1*, 123–134.

Pagallo, U. (2010). As law goes by: Topology, ontology, evolution. In P. Casanovas et al. (Eds.), *AI approaches to the complexity of legal systems* (pp. 12–26). Berlin: Springer.

Pagallo, U., & Durante, M. (2009). Three roads to P2P systems and their impact on business practices and ethics. *Journal of Business Ethics, 90*(4), 551–564.

Post, D. G. (2009). *In search of Jefferson's moose: Notes on the state of cyberspace*. Oxford: Oxford University Press.

Sartor, G. and Viola de Azevedo Cunha, M. (2010). The Italian Google-case: Privacy, freedom of speech and responsibility of providers for user-generated contents. *International Journal of Law and Information Technology*, forthcoming. Retrieved 19th November 2010 at SSRN from http://ssrn.com/abstract=1604411.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22.

Volkman, R. (2003). Privacy as life, liberty, property. *Ethics and Information Technology, 5*(4), 199–210.

von Ahn, L., Maurer, B., McMillen, C., Abraham, D., & Blum, M. (2008). reCAPTCHA: Human-based character recognition via web security measures. *Science, 321*(5895), 1465–1468.

Waldron, J. (2010). Dignity and defamation: The visibility of hate. *Harvard Law Review, 123*(7), 1596–1657.

Wolff, M. (2010). The web is dead: Who's to blame—Them. *Wired*, September, pp. 123–127, 166.

WP 29 (2009a). EU Working Party art. 29 D-95/46/EC. Online social networking, *01189/09/EN–WP 163*, June 12th, 2009.

WP 29 (2009b). EU Working Party art. 29 D-95/46/EC. The future of privacy. *02356/09/EN–WP 168*, December 1st 2009.

WP 29 (2010). EU Working Party art. 29 D-95/46/EC. The concepts of "controller" and "processor." *02264/10/EN–WP 169*, February 16th 2010.

Yeung, K. (2007). Towards an understanding of regulation by design. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 79–108). London: Hart Publishing.

Zittrain, J. (2007). Perfect enforcement on tomorrow's Internet. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 125–156). London: Hart Publishing.

Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven: Yale University Press.