College of Europe
Collège d'Europe

Brugge

Natolin

An Economic Analysis of Liability of Hosting Services: Uncertainty and Incentives Online

Joanna HORNIK and Carmen VILLA LLERA

DEPARTMENT OF
EUROPEAN ECONOMIC STUDIES

Bruges European Economic Research Papers 37 / 2017

Abstract

In this paper we study the uncertainty in the liability provisions under the E-Commerce Directive from an economic perspective . Through the combination of economics of cybersecurity and economic theories of deterrence and liability we analyse how the uncertainty in Articles 12-15 of the E-Commerce Directive can affect the incentives that Internet service providers have as regards what level of involvement to have with data uploaded by users. By looking at the costs and benefits of investment in security, we show how the existence of uncertainty in the law can lead to a suboptimal level of investment. Subsequently, we explore the consequences of changing the current liability provisions towards either strict liability or no liability at all. We show how rationally speaking, excessively strict liability could lead to surveillance of all online content, posing a threat to freedom of expression and exchange of information. On the other hand no liability would transfer the responsibility for a safe online space away from hosting services towards public authorities and civil society groups. The paper intends to add economic analysis to the legal debate in pursue for more clarity regarding the interpretation of current rules as well as a better alignment of incentives of hosting service providers and user preferences so as to create a safer and fairer online environment.

Keywords

Liability online, Economic Analysis of Liability, Hosting service providers in the EU, E-Commerce Directive

JEL Codes

K24, K42, K41, L51, D81, D92

Acknowledgements

We would like to thank Professor Phedon Nicolaides, Dr Adina Claici and Luca Di Mauro for their invaluable comments and suggestions in the making of this paper.

Joanna Hornik is an Academic Assistant in the Economics Department at the College of Europe in Bruges, Belgium.

Carmen Villa is a Research Assistant in the Center for Economic Performance at the London School of Economics.

The authors assume full responsibility for the views presented in this paper. They do not necessarily reflect the views of the institutions of which they are part.

1 Introduction

As much as the Internet is an asset for exchanging information, it can also be used as a resource for illegal and even criminal behaviour, such as the exchange of content protected by intellectual property (IP) rights, child pornography, racist and xenophobic content, defamation, incitements to terrorism, illegal gambling or fake banking services among many other unlawful behaviours [European Commission, 2012]. With more than 3.2 billion users of the Internet [Internet-Live-Statistics, 2016], the monitoring and control of all uploads on the Web is economically and practically impossible; however, some degree of active control and removal of illegal information is necessary. Given the ubiquitous presence of the Internet in all aspects of life, an appropriate regulatory framework should aim to achieve an optimal balance between privacy protection, security assurance, provision of high quality online services, and freedom of expression.

One of the key issues in achieving this balance concerns liability online, which is particularly pertinent for information service providers (ISP) who do not generate online content but provide platforms for exchange of information among users. Information society services are defined in EU law as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" [E-Commerce Directive, 2000]. In the European Union, the liability of such online intermediaries is regulated by the E-Commerce Directive (ECD). The Directive was approved in the context of comprehension of the essential role that such services would play in modern economy, with the objective of allowing online intermediaries to become drivers of economic growth. At its conception, the ECD aimed at aligning regulatory regimes in the European online space, so as to increase consumers' trust in online markets and provide companies with legal certainty that would allow them to operate in the Single Market [European Commission, 1998]. However, while the objective was noble, there are several issues in the liability provisions which, given their vague wording, have left stakeholders with a certain degree of uncertainty over the application and limits of the ECD.

Such uncertainty presents a problem for ISPs and other stakeholders because it limits the extent to which an ISP should be involved in monitoring the data uploaded by users. This in turn leaves ISPs with contradictory

incentives as to what role to play in achieving a secure Internet in the European Union. Some have argued that it is desirable for ISPs to play an important role in the fight against criminality online - for instance, David Cameron stated in 2013 that some services have a "moral duty" to fight illegal behavior online [Watts, 2013]. At the same time, it seems that the E-Commerce Directive has not succeeded in achieving the balance that would both allow ISPs to operate and incentivise them to play an important role in preventing illegal materials online.

The paper is structured in the following way: Section 2 outlines the content of the ECD with regard to liability for online actors and introduces the notion of uncertainty surrounding these liability provisions. In Section 3 we review the literature related to the law and economics of liability. In Section 4 we develop an economic model on how uncertainty about liability affects the incentives for hosting platforms to invest in prevention mechanisms. We outline the practical implications of our model and the resulting debate in Section 5 and finish with conclusions.

2 Liability of Hosting Services Online

2.1 The liability exemption

The provisions in Articles 12-15 (Section 4) of the ECD define the scope of the exemption from liability for intermediary service providers, making a distinction between three types of services: mere conduit (art. 12), caching (art. 13) and hosting (art. 14). The liability exemption in the ECD applies only to activities of "mere technical, automatic and passive nature" where the information society service providers have "neither knowledge (...) nor control" over content transmitted through or stored on their site. The conditions for what constitutes a passive service provider are outlined in Articles 12 and 13 of the ECD. Article 12 refers to the exemption for 'mere conduit' that ensure no liability for the: "Information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (b) does not select or modify the information contained in the transmission.".

Article 13 adds an exemption for 'caching' that obliges Member States to ensure that: "The service provider is not liable for the automatic, intermediate and temporary storage of (...) information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request." Provided the information is not modified, access to it and updating is regulated, the technology to obtain data is used lawfully and any illegal content is removed swiftly, the ISP is exempt from liability for caching.

Article 14, in turn, regulates hosting services, which are information society services that store information provided by a recipient of the service [European Commission, 2003]. The Article states that a hosting service provider is not liable for the "Information stored at the request of a recipient of the service, on condition that (a) the provider does not have actual knowledge of illegal activity [...] or (b) the provider upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

In other words, the hosting service is not responsible for illegal content uploaded on its site as long as it is not aware of the existence of such content and that as soon as the company obtains knowledge of unlawful material, it removes it rapidly from the platform. Finally, Article 15 contains a provision of "no general obligation to monitor" to be imposed by Member States on intermediary service providers, allowing however for obligations to inform authorities of any illegal activities "promptly".

2.2 Uncertainty in the interpretation of liability provisions

Through the Directive and specifically in Article 14, hosting service providers are given a 'safe harbour' from liability which allows them to function without the need to supervise or monitor all the content uploaded onto their sites. However, failing to remove the illegal content "expeditiously" can transform the hosting service into a publisher or deem it to have facilitated the availability of the disruptive information; hence the hosting service does still have certain responsibility.

The liability provisions in the ECD have been considered as an invitation

to self-regulation [European Commission, 2003], as by removing strict obligation to monitor while leaving room for liability, they incentivise hosting services to impose a measure of control upon content uploaded online. Yet this leaves hosting services with an essential decision to make on how 'involved' they want to be with data on their platforms which, as we will explore in Section 5 may not always be aligned with societal security concerns.

The dilemma stems from the fact that there is a degree of uncertainty about the liability regime for intermediary service providers. At the heart of this uncertainty, there is the ambiguous distinction arising from the case law which defines 'active' and 'passive' services. In the concluding statements of paragraph 120 in the *Google v Louis Vuitton* judgment, the Court of Justice of the EU specifies that within the meaning of Art.14 of the ECD, the liability exemption applies to "an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored". Thus it appears that knowledge or control over data stored by hosting platforms is crucial to making the distinction between active and passive intermediary service providers [1].

The case law on what constitutes an 'active' service provider remains ambiguous. For instance, Myspace, the American social networking platform, was found guilty by the Court of Paris of not removing the videos of Mr. Jean-Yves Lafesse that were posted without his consent. Myspace was qualified to be an editor of online content due to the pre-defined structure of the personal pages of users as well as to the presence of profit-generating adverts on the website. A similar interpretation of the liability rules was reached in a case involving the video-hosting platform IOL under Italian jurisdiction. IOL was believed to have "actual knowledge" of the illegal content because it indexed the information uploaded and allowed users to find videos through a "related search" service [Benjumea Moreno, 2012]. At the same time, a French video platform Dailymotion was qualified as a passive hosting service provider because its involvement with online content (such as re-encoding, formatting and organising) was purely technical rather than editorial [Court of Cassation, 2011].

[1] This position of the ECJ has been further confirmed in the Google Adwords judgment from March 23, 2010

Higher involvement or care towards data uploaded can convert a host into an "active" host and higher monitoring could be considered a determinant of "actual knowledge" of illegal content, which could suggest that it is optimal for a hosting service provider to take no preventive action. However, too little involvement leading to failure to remove content "expeditiously" can make a hosting service provider liable as well. In turn, the technicalities in automaticity of engagement with data by hosts and the sheer number of possible infringements make the issue even more complex and leave room for misinterpretations of the law.

In this paper, we examine whether such a distinction between passive and active hosting services corresponds to the economic theories of investment in cybersecurity. We create a theoretical model of economic analysis of law to explain the contradictory incentives for hosting service providers created by legal uncertainty surrounding liability. Our analysis is based on several key findings from economics of cybersecurity and theories of liability which are discussed in the following section.

3 Law and Economics of Liability Online

Uncertainty about liability under the E-Commerce Directive is both a legal and an economic matter and therefore, we combine theories from both disciplines to understand the issue.

First of all, we build our model on insights from economics of cybersecurity and in particular the Gordon and Loeb (GL) model, which is the most important theory in this field to date. The model sets off to examine what is the optimal level of investment companies should undertake in order to protect their assets on the web from cybercrime, focusing largely on information losses. In their model, Gordon and Loeb present the optimal amount to invest in information security by analysing under a set of assumptions the relationship between vulnerability and productivity of investment. The model is a one-period model accounting for monetary loss by breach of security of the information set, probability of an attempted breach, threat probability, investment in security and vulnerability. While the GL model talks generally

about "information security in a computer-based environment" [Gordon and Loeb, 2002], we extrapolate its logic to analyse the behaviour of hosting services with respect to illegal content entering their platforms.

In section 4 we adapt the variables and economic logic used by Gordon and Loeb and derive, in a similar way, the optimal point of investment in prevention mechanisms, which is "at the point where marginal investment costs equal the expected marginal benefits derived from the investment" [Gordon and Loeb, 2002]. Aside from adapting the variables, we adapt as well some of the assumptions underlying the model so as to better fit the problem of uncertainty as regards liability. In turn, while Gordon and Loeb's model aims at preventing theft of information, ours is related to the hosting service's decision as regards preventing illegal material from being uploaded.

Other very relevant theories influencing our work are deterrence, liability, and cost-allocation theories. In deterrence theory, an actor's expected utility derived from committing a certain action can be monetised into a total monetary utility and there is also a monetary equivalent of a punishment and the subject's probability of conviction [Becker et al., 1974]. An actor will thus decide whether to engage in an (illegal) activity by weighing the benefits of performing such activity with the costs of doing so [Beccaria, 1767] [Bentham, 1843]. In the context of uncertainty, assuming hosting service providers are rational actors, they will decide on their degree of care and involvement towards data by making an utilitarian cost-benefit analysis, in a similar way that deterrence theory explains the motivation for a criminal to engage in an illegal activity.

In theories of liability, economists and lawyers analyse the agency dilemma, referring to situations in which one person's actions (agent) impact another person (principal). In these cases, the principal has an incentive to take control over the agent's actions [Shavell, 1980] which in our situation translates into hosting service providers having an incentive to control their users' behaviour. Many of these theories also account for a probability of an accident occurring [Polinsky and Shavell, 2007], which in our context means the probability of a party being harmed by illegal content being available on a platform. As has been shown by Shavell [Shavell, 2009], the probability of an accident is negatively related to the level of care and the optimal level of care occurs when potential losses are minimized at a minimal cost, given

the risk of an accident. This translate in our model into the assumption of rational investment where a higher level of care towards online content decreases probability of illegal content appearing on the platform.

Our model is also largely influenced by the work of Johnston, who develops an analysis on how uncertainty can impact the incentives in principal-agent relations [Johnston, 1990]. Johnston introduces in his model a variable accounting for effort or precaution level (exercised by the principal or party in control) that is influenced by random circumstances determining realised probability of harm and random circumstances determining realised cost of effort or precautions. While Johnston rationalises the conditions for an actor to exercise a high level of care from the point of view of the desirability of uncertainty in a rule of law, we focus on the incentives for the principal (i.e. the hosting platform) to invest in care towards data.

Lastly, our analysis also builds on the early theory of social costs developed by Coase. According to Coase, we must take into account the reciprocal character of the economic activity in question and consider who is in a position to internalise the costs associated with the economic exchange. The socially optimal liability regime would thus regulate the market so as to avoid the more seriously harmful effect that is the one associated with a higher social cost [Coase, 1960]. The influence of Coase's theory on analysing the issue of liability online has already been stressed by Lichtman and Posner[Lichtman and Posner, 2006]. The authors defend that ISPs should be strictly liable for the content uploaded onto their platforms as they are in the best position to decrease illegal content online (which we can understand as a negative externality). This in turn defends further the idea that hosting service providers have a responsibility over content uploaded on their platforms and must be incentivised to do so. In our paper it will help us reach conclusions over the desirability of uncertainty in the context of liability online.

These various strains in economic and legal literature about cybersecurity, liability, deterrence and cost internalisation have all contributed to the theoretical model of liability of hosting service providers developed in the next section.

4 Economic Analysis of Liability of Hosting Service Providers

In this section, we adapt the concepts explored in the Gordon and Loeb model to fit the problem of uncertainty about liability of hosting service providers. In the GL model, probability of an attack alters the optimal investment, while for us uncertainty is an element to be considered when making the rational decision with regard to the level of care towards data uploaded by users to a platform/hosting service. We will not enter into exhaustive details regarding the mathematics behind our model as that is not the main focus of this study. A more exhaustive technical specification can be found in the paper by Gordon and Loeb [Gordon and Loeb, 2002].

The optimal level of investment in security or prevention mechanisms by hosting services depends on the costs of investment, effectiveness of investment, and costs of facing liability. Additionally, with ambiguous wording of the liability provisions, the application of the law will be uncertain, which is an element that enters into play in our model as a random variable outside the hosting service provider's control. We have summarised these variables below:

- z : cost of investment in prevention mechanisms. This refers to any investments made by hosting services with the aim of preventing illegal material on a platform from reaching the final user. The most commonly used mechanisms are filtering techniques (for instance Youtube uses a software called Content ID to filter copyright-protected material), monitoring techniques (when resources are deployed for actively searching for possible breaches in the law within a platform) and notice-and-takedown procedures (whenever resources are deployed for content removal done upon notification by a user).

- p : probability of content uploaded by a given user to be illegal and to bypass the security measures in place. Consequently, this variable reflects the likelihood that illegal content appears on the hosting platform and can be accessed by the viewers.

- c_l : this variable comprises any costs incurred by the hosting service if found liable for material on its platform. They can include litigation costs, compensation costs, and reputation costs, among others. It is important to note that these must directly affect the hosting service (i.e. costs borne by a victim of the illegal content do not fall into this category).

- u : random element affecting the probability of a platform being found liable. Since the wording of the liability provisions is vague, this variable captures the various circumstances depending on the interpretation of "actual knowledge", "active service", "passive service", and "expeditiously" from the ECD. By its very nature, the variable's behaviour is unknown, which could affect the expected outcome of a court decision either to the detriment or benefit of the hosting service provider.

The benefits of a higher investment in security are modelled as the decrease in potential losses. Overall, this means the difference between the potential loses of a hosting service provider who does not invest in prevention mechanisms and the potential losses of a hosting service provider who does invest in prevention mechanisms.

Additionally, we include some assumptions in order to draw conclusions from the subsequent derivation. These differ somewhat from the Gordon and Loeb model:

- Assumption 1
  The liability probability function must be between 0 and 1

$$0 < S(z^*, u) < 1$$

- Assumption 2
  For all uncertainty u,

$$S(0, u) = u$$

- Assumption 3
  For $u = 0$ the function $S(z, 0)$ is decreasing and convex

$$\frac{d}{dz}S(z,0) < 0$$

$$\frac{d^2}{dz^2}s(z,0) > 0$$

This means that a higher investment decreases the potential losses by decreasing the probability of illegal material entering the web. This condition is necessary to reflect rationality in the investment decision, for instance prevention mechanisms being effective. This is essential as we are assuming that hosting services are rational actors and therefore the incentive to prevent illegal material on the web comes from an economic gain (decrease in potential losses) and not from an altruistic interest in decreasing illegal material available online.

From these variables we can derive the equation for benefit from investment in prevention mechanisms as the difference in the potential loses with different levels of investment:

$$[u - S(z,u)] * c_l * p - z \tag{1}$$

With positive value of investment z and in the presence of uncertainty, the point at which investment in security optimizes probability of being found liable is found by calculating the first order condition of the following function:

$$-S(z*,u) * c_l * p = 1 \tag{2}$$

This can be rewritten as:

$$-S_z(z*,u) = 1/(c_l * p) \tag{3}$$

The function above can be understood as the marginal productivity of higher investment in security. More specifically, it illustrates the relationship between the potential decreases in costs (litigation costs derived from liability for illegal content online) associated with an additional investment in prevention costs.

While we will not focus on the mathematics that allow to define the function $S(z, u)$ in practice, in the following sections we discuss the model as seen from the perspective of the legal debate about an optimal liability regime, in light of court rulings on liability of hosting services.

5 Implication and Debate

5.1 The effect of uncertainty

The presence of uncertainty affects the optimal level of investment by altering the equation in the partial derivative of the liability probability function. Recalling that with some degree of liability the problem for the hosting service has to do with how to prevent potential higher litigation costs, it is easy to see that with some undefined elements in the law, having targeted prevention mechanisms in place will be difficult for hosting service providers.

When uncertainty enters the equation its random nature cannot guarantee that investment in prevention mechanisms will be rational or effective. This occurs because of many errors that are introduced with uncertainty. For example, a hosting service may fail to prevent illegal material on the web simply by failing to identify what constitutes "illegal". Even if legality is well assessed, notice-and-takedown processess may not be "expeditious" enough, hence creating an error in the effectiveness of the measures in preventing possible. This is supported by examples of cases mentioned in section 2 where higher monitoring could be a determinant of actual knowledge and higher involvement can convert a host into an "active host". The incentive to invest is harmed no matter how effective the prevention mechanism may be. In turn, the liability probability function including the element u makes it so that the level of investment z may not lead to the desired minimization of potential losses $c_l * p$.

$$S(z*, u) = -1/(c_l * p) \tag{4}$$

The implication to society in terms of achieving a secure Internet is that with no definite answer as to what is optimal, hosting service providers will likely leave decisions on the level of care to the expectations they may have of what outcome is most likely in court. In the context of the ECD, which aims at harmonising the rules across the EU, leaving a decision on investment levels to be determined by expectations which may vary across different Member States is certainly suboptimal for stakeholders.

Furthermore, in the current setting with the vague distinction between active and passive hosting services, it is rational to assume that, in a court hearing, higher involvement with online content could be a determinant of being an "active" host. This de-incentivises further investment in prevention costs, as higher investment in z cannot guarantee lower costs of litigation in spite of the relationship with probability described in Assumption 3.

5.2 Removing the element of uncertainty

There is currently much legal debate as to what wording in Articles 12-15 would benefit stakeholders of hosting service providers by decreasing uncertainty. It appears that further specification of concepts such as "expeditiously" or "actual knowledge" would in practice be very hard to define and could even be detrimental. To illustrate, the concept "expeditiously" would probably need to include some kind of time measurement to reduce uncertainty. As a Commission working paper states, any specification of a time frame would probably turn out to be too short or too long. For example, the streaming of a live sports event would require immediate take-down to avoid any economic damage, while other type of content would allow for higher flexibility. [European Commission, 2012]. While we leave to lawyers the debate as to what wording would clarify the current liability regime, in this section we explore the economic consequences of removing uncertainty. In this setting, we study two extreme hypothetical situations: removing uncertainty towards strict liability or else removing uncertainty by completely removing any link of hosting service providers to liability.

5.2.1 Strict liability for hosting service providers

If strict liability were imposed, hosting services would find themselves in a setting were their incentives to invest are extremely high. Any possible illegal content on a platform would become the hosting service provider's responsibility and hence the hosting service would bear all economic costs. In the framework of our model, the new problem transforms the probability liability function in the following way:

$$S(z) = -1/c_l * p \tag{5}$$

Given Assumption 3, where we assume higher investment in prevention mechanisms to be decreasing in relation to probability of illegal material entering the platform, in this equation there exists an optimal level of investment $z*$. By removing uncertainty, we allow for the existence of an economically rational solution as ISPs have a targeted approach to preventing illegal material on their platforms.

While this would allow optimal decision-making, it also hampers the main reason the E-Commerce Directive was put in place in the first place: to allow economic activity online to flourish and the exchange of information. By making hosting service providers strictly liable, only those with more resources could afford to allow users to exchange material on their platforms as prevention mechanisms are expensive and controlling all activity online is practically impossible. There are therefore two dangers associated to the idea of strict liability for hosting service providers: pushing small hosting service providers out of the Internet and a threat to freedom of speech.

Smaller platforms would likely not be able to bear neither the very high cost of prevention nor the potential litigation costs hence we would see a decrease in the number of smaller players, with the harm that this implies for innovation and the sharing of content for users. At the same time, if hosting service providers were in control of all possible information uploaded, there is a risk that too much information would be prevented from reaching the platforms. In such a situation, sharing of all ideas online would become

subject to monitoring, whether illegal or not. This of course poses a threat to freedom of expression and exchange of information, which are rights enshrined in Article 11 of the EU Charter of Fundamental Rights.

5.2.2 No liability of hosting service providers

On the other hand, if no liability were imposed on a hosting service provider, there would also be an optimal solution to the equation mentioned above. When the hosting service providers need not bear the cost of potential litigation, the optimal solution would be not to invest at all in prevention of illegal content online.

$$S(z*, 0) = 0 \tag{6}$$

While this is optimal (i.e. least expensive) for hosting service providers, a move towards less liability would exclude hosting service providers from the fight against illegal material online. Taking into account societal preference for a safe Internet, no liability for hosts would likely mean that the costs of preventing online content from reaching the viewers would be borne by either public authorities or private activist groups.

From both economic and legal point of view, such an outcome would be problematic. On the one hand, involving public authorities in overseeing online content would raise issues of breach of privacy, as seen for example in the public outrage at NSA actions in the United States after the 9/11 terrorist attacks. On the other hand, relying solely on social activism could lead to under- or over-surveillance and would likely result in increased costs of litigation for hosts, viewers and potential victims of illegal content.

6 Conclusion

The discussion presented in this paper reveals the numerous facets of the problems faced by hosting services, law-makers and users regarding illegal content online. Our analysis reveals the difficulties in reconciling the need for legal certainty with the creation of an environment where users are protected,

while at the same time allowing hosts to operate their businesses profitably.

Given the diverging interpretations of the current legal framework under the ECD, we attempt to contribute to the discussion about an optimal level of liability for hosting services. By applying a number of different theories and specifically focusing on the relevance of the GL model of cybersecurity, we showed that an optimal level of investment in prevention of illegal material is difficult, if not impossible to define, given the random nature of uncertainty. This in turn leaves the important decision on the level of involvement towards online content to the expectations of hosting service providers about the outcome of potential litigation. For the purpose of achieving a safe cyberspace across the European Union, such a framework remains suboptimal.

We show that from an economic point of view, any change towards the extremes of either strict liability or no-liability would not be desirable. Strict liability would turn the Internet into a space fully controlled by hosting service providers which would threaten the fundamental freedom of expression guaranteed to EU citizens. Besides, it would likely force smaller hosting service providers out of the market. Yet a move towards no-liability would imply hosting service providers would not participate in the costs of the fight against illegal behaviour online.

From both economic and legal points of view, implications of our analysis are twofold. Firstly, clarity is needed about distinction between active and passive hosting service providers, preferably expanding the number of hosts categorised as passive. This would give breathing space to smaller hosting platforms with less funds available for screening of online content by extending the liability exemption. Secondly, when looking at costs and benefits of the legal framework, the situation of users should be taken into account alongside the incentives for hosting service providers. A more balanced approach would allow for a fairer, safer, and more socially optimal liability framework for online platforms.

References

C Beccaria. On crimes and punishments and other writings, ed. r. bellemy (1995), 1767.

Gary Stanley Becker, William M Landes, and National Bureau of Economic Research. *Essays in the Economics of Crime and Punishment*. National Bureau of Economic Research New York, 1974.

Juan Benjumea Moreno. Publisher or technical provider? monitoring as editorial control and the "safe harbour" of art. 14 e-commerce directive. *Jura Falconis*, 2012.

Jeremy Bentham. *Principles of penal law*. W. Tait, 1843.

Ronald H Coase. The problem of social cost. *Journal of Low and Economics*, 3:1–44, 1960.

Court of Cassation. Société nord-ouest & ugc images v. dailymotion. ., .(.), 2011.

E-Commerce Directive. Directive 2000/31/ec. 2000.

European Commission. Press release - electronic commerce: Commission proposes legal framework. Technical report, 1998. URL $http : //europa.eu/rapid/press - release_I P - 98 - 999_e n.htm?locale = es$.

European Commission. First report on the application of directive 2000/31/ec of the european parliament and of the council of 8 june 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market. •, European Commission, 2003.

European Commission. Commission staff working document, online services, including e-commerce in the single market. 2012.

Lawrence A Gordon and Martin P Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

Internet-Live-Statistics. Number of internet users, 2016. URL `http://www.internetlivestats.com/internet-users/, accessed 19th May 2017`.

Jason Scott Johnston. Uncertainty chaos and the torts process: An economic analysis of legal form. *Cornell L. Rev.*, 76:341, 1990.

Doug Lichtman and Eric Posner. Holding internet service providers accountable. *Supreme Court Economic Review*, pages 221–259, 2006.

A Mitchell Polinsky and Steven Shavell. *Handbook of law and economics*. Elsevier, 2007.

Steven Shavell. Strict liability versus negligence. *The Journal of Legal Studies*, 9(1):1–25, 1980.

Steven Shavell. *Economic analysis of accident law*. Harvard University Press, 2009.

Robert Watts. David cameron: Web firms have a 'moral duty' to wipe out indecent images, 2013. URL $http://www.telegraph.co.uk/technology/internet/10192789/David-Cameron-Web-firms-have-a-moral-duty-to-wipe-out-indecent-images.html, accessed19thMay2017$.