Virtues and Perils of Anonymity

Should Intermediaries Bear the Burden?

by **Nicolo Zingales,*** Assistant Professor, Tilburg Law School. Fellow, Center for Technology and Society, Getulio Vargas Foundation.

Abstract: On October 10, 2013, the Chamber of the European Court of Human Rights (ECtHR) handed down a judgment (Delfi v. Estonia) condoning Estonia for a law which, as interpreted, held a news portal liable for the defamatory comments of its users. Amongst the considerations that led the Court to find no violation of freedom of expression in this particular case were, above all, the inadequacy of the automatic screening system adopted by the website and the users' option to post their comments anonymously (i.e. without need for prior registration via email), which in the Court's view rendered the protection conferred to the injured party via direct legal action against the authors of the comments ineffective. Drawing on the implications of this (not yet final) ruling, this paper discusses a few questions that the tension between the risk of wrongful use of information and the right to anonymity generates for the development of Internet communication, and examines the role that intermediary liability legislation can play to manage this tension.

Keywords: Internet intermediary liability, anonymity on the Internet, defamation, technological rights adjudication

Recommended citation: Nicolo Zingales, Virtues and Perils of Anonymity: Should Intermediaries Bear the Burden 5 (2014) JIPITEC 155, para 1.

A. Introduction: recognizing different types of anonymity

1 Anonymity is a feature, not a bug, of the Internet. As Larry Lessig explained when commenting on the clash between the technical and the social architecture of the net, "the *Internet* protocol doesn't require that [...] you credential who you are before you use the Internet."[1] In other words, it is only because of the *social* protocol that we are pushed towards identification[2].

2 At the same time, however, anonymity is also a fundamental feature in the social architecture for it gives individuals the ability to speak in a variety of circumstances where the revelation of their identity would compromise it. Peter Steiner effectively illustrated the centrality of anonymity to our understanding of the Internet in a cartoon published in The New Yorker in July 1993, which birthed the famous adage "On the Internet, nobody knows you're a dog"[3]. The cartoon featured a dog sitting in front of a computer and (presumably) inserting his preferences and generalities into a virtual profile, sharing the insight of the adage to a fellow dog. That sentence reflected an essential property of Internet communication: individuals engaged in such communication can mask the real identity *to their audience*. The "masking" can be accomplished by two different means: online anonymity and pseudonymity. While both are manifestations of the broader concept of anonymity - the latter being an attenuated version of the former- it is important to make clear in what respect the two differ, and the extent to which they relate to "real world" anonymity.

3 The most direct form of online anonymity for a user is, when permitted by the platform where communication takes place, to avoid giving his or

her generalities altogether. In this case, any message or action by the user is labeled as originating from "anonymous" or, alternatively, with some kind of serial number following the word "user." A similar type of online anonymity can be attained if, in a system of mandatory user registration, there is no requirement to provide information which will make him or her actually identifiable as pre-condition to accede to or actively engage in the platform. Although there is no agreed-upon definition of the exact type of information that would trigger a loss of online anonymity[4], it is generally understood that authentication via email address to "join the community" would suffice for that purpose. In contrast, pseudonymity does not exclude long-term relationship with the community of the platform, but presupposes the creation of a user profile that identifies him or her within that community as the holder of a particular pseudonym. However, the system of registration does not guarantee that the online "persona" chosen by the user represents, in any way, his or her real identity. In fact, pseudonymity not only enables people to maintain several online identities but also allows multiple individuals to manage a unique persona.

4 The "mask" provided by online anonymity and pseudonymity is not a peculiarity of Internet communication; the possibility of corresponding anonymously was long established prior to the invention of the Internet, and pseudonyms had been used throughout history by a number of literary figures, musicians and authors of political articles[5]. What is different in the context of the Internet is the ease with which the digitalization of communication and the advancement of tracking technologies have made it possible for a real identity to be uncovered. Not only are the logs of every communication originating from our devices systematically recorded by internet service providers or the servers through which we connect, but the use of cookies and other tracking mechanisms has significantly affected our ability to keep anonymity *vis a vis* the websites that we visit; in addition, the tools available to infer real identity from network analysis, patterns of behavior, and data mining have minimized the extent to which pseudonymity can be considered an effective anonymization technique *vis a vis* not only the other users of that particular website, but more crucially the State and private entities offering their services online. In fact, extensive literature points out the failure of the conventional mechanisms currently used to secure anonymity[6]; in other words, "real world" anonymity has simply become much more difficult to accomplish today, in a society that is increasingly based on online interactions.

5 Furthermore, new technologies have emerged that afford platforms the opportunity to authenticate the identity of users in an increasingly reliable manner: for example, certain platforms have started using software to verify identities by scanning national ID cards[7], and asking security questions- the answer to which must match the one contained in the credit file linked to a particular person's bank account[8]. Soon, we might be confronted with widespread use of facial recognition technologies for ID verification, which have already become available on the market[9]. Currently, these advanced verification technologies are used on an opt-in basis, in exchange for access to special privileges or simply to promote a higher trust with the other members of the community. Yet, it is not hard to imagine a future in which the gap between basic and premium services is so significant as to make the anonymous use of Internet inconceivable as a practical matter. It is precisely to warn against this danger that this paper aims to offer a critique of a judgment of the European Court of Human Rights which, if confirmed on appeal, would likely lead to the realization of this gloomy picture.

6 Before plunging into the specifics of the judgment, however, it is important to clarify that a discussion on anonymity cannot abstract from the questions "against whom" and "in what circumstances", both of which qualify as different subtypes of anonymity. The first question departs from the assumption that anonymity is to be seen as an absolute quality –i.e., *erga omnes*- and recognizes that an individual might just aspire to achieve anonymity *vis a vis* the other users of the platform, as opposed to an internet service provider, or the public authority. In this respect, one should differentiate between: (1) platform anonymity; (2) customer anonymity; and (3) citizen anonymity[10].

7 (3) (Citizen anonymity) is invariably the most protected type, one with constitutional rules in place in different countries to guard citizens from arbitrary interferences, yet one which tends to be most easily abridged for law enforcement purposes, and probably the hardest to ensure at the technological level[11]. (2) (Customer anonymity) refers to the identity given to the provider of the Internet connection –which can only be hidden in very limited circumstances; for example, from a public wifi not requiring registration, or another online service –in which case, anonymity can be ensured through the use of VPNs, web proxies or anonymity networks[12], along with decentralized and anonymized payment systems. What remains under (1) (Platform anonymity) then is just a thin version of anonymity, which can be achieved *inter alia* under some form of pseudonymity. It is clear that escaping identification by the three target audiences at the same time can be very challenging and can, occasionally, be an impossible task to accomplish.

8 The second important clarification concerns the circumstances in which anonymity should be

protected. In practice, this depends on the weight of the respective interests of the two sets of stakeholders: those claiming or exerting anonymity privileges and those who invoke identity disclosure. For example, in the case of threat of serious criminal offences, the public authority will have broader powers of investigation under (3); likewise, the discretion of a prosecutor or a judicial authority to curb anonymity under (1) and (2) will be significantly broader[13]. On the other hand, the need to protect (who?) from an imminent threat of violence or other seriously adverse consequences will enhance the weight of anonymity interests, possibly even at the expense of legitimate law enforcement operations. In short, the protection of anonymity can hardly be seen as a monolithic concept: anonymity has different breadth depending on the target group against which it operates, and a balancing between conflicting interests is often necessary to understand the contours of its protection.

9 The following section puts platform anonymity into context by describing the facts and the issues at stake in the case of *Delfi v. Estonia*[14], where the European Court of Human Rights attributed the anonymous character of the comments a role of trigger for a special responsibility of host providers. After an introduction to the facts of the case and the domestic proceedings, the second section will highlight the problematic aspects of the reasoning followed by the Court to reach that conclusion. Subsequently, the third section will provide an assessment of the adverse implications that a similar judgment would have on the creation of user-generated content on the Internet. Finally, the fourth section will conclude by suggesting which principles should be followed to promote an intermediary liability regime that ensures prompt and effective remedies while respecting the fundamental right to anonymity.

B. The Delfi judgment

I. Domestic proceedings

10 Delfi is an internet news portal operating in Estonian, Latvia and Lithuania, which publishes up to 330 news articles per day. Delfi enables user comments in a blank space at the bottom of each article, next to another blank space for the commenter's name and (optional) email address. On January 24, 2006, Delfi published an article entitled "*SLK Destroyed Planned Ice Road*", which described the incident whereby the SLK public ferry, which offers transportation between the mainland and some islands, decided to change its route and, as a result, ended up destroying so-called "iced roads" -- built each winter on parts of the frozen Baltic Sea, offering an alternative connection to some of those islands. Destroyed ice roads were in direct competition with the ferry, whose majority shareholder was Mr. L. For this reason, some (20) of the several (186) comments received contained personal threats or offensive language against L. These comments were not detected by the automatic deletion system, which is based on certain stems of obscene words, and were not flagged as offensive by any user through the "notice and take-down" framework provided by the portal.

11 On March 9, 2006, approximately six weeks after the publication of the article, L.'s lawyers requested the removal of the comments and claimed damages for compensation against Delfi. While Delfi complied with the request by removing the comments the same day, it refused compensation. As a result, L.'s lawyers brought a civil suit against Delfi to the Harju County Court. The County Court initially dismissed the claim citing that content hosts were granted safe harbor under the Information Society Act (the Estonian implementation of the EU Electronic Commerce Directive), according to which:

Section 10 – Restricted liability upon provision of information storage service

"(1) Where a service is provided that consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

1) the provider does not have actual knowledge of the contents of the information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;

2) the provider, upon obtaining knowledge or awareness of the facts specified in subparagraph 1 of this paragraph, acts expeditiously to remove or to disable access to the information.

(2) Paragraph 1 of this section shall not apply when the recipient of the service is acting under the authority or the control of the provider."

Section 11 – No obligation to monitor

"(1) A service provider specified in sections 8 to 10 of this Act is not obliged to monitor information upon the mere transmission thereof or provision of access thereto, temporary storage thereof in cache memory or storage thereof at the request of the recipient of the service, nor is the service provider obliged to actively seek information or circumstances indicating illegal activity.

12 However, on October 22, 2007, the Tallin Court of Appeal quashed the judgment, finding the Information Society Services Act was inapplicable, and remanded to the County Court. In the subsequent judgment, the County Court on June 27, 2008, found in favor of the claimant, qualifying Delfi as a "publisher" of the comments (and not only of the news article) and awarded the equivalent of 320 Euros of damages compensation. The Court of Appeal upheld the judgment on December 16, 2008, on the basis of the consideration that Delfi should have created an effective system ensuring rapid

removal of unlawful comments, and that imposing the burden of monitoring on the potential victims runs against the principle of good faith. Finally, the Supreme Court on June 10, 2009, dismissed Delfi's further appeal, clarifying that in contrast with the hypothesis of service provider falling under the safe harbor of sections 10 and 11, a provider of content services "*govern[s] the content of information that [i]s being stored*". It went on to explain that the company has to be considered a publisher because:

> "The number of comments had an effect on the number of visits to the portal and on [Delfi]'s revenue from advertisements published on the portal. Thus, [Delfi] had an economic interest in the comments."

13 In addition, Delfi was deemed to have control over the publishing of comments because:

> "It enacted the rules of comment and removed comments if the rules were breached. The users, on the contrary, could not change or delete the comments they had posted; they could merely report obscene comments."

14 Finally, the Court concluded that Delfi, on the basis of the general *neminem laedere* obligation, should have prevented clearly unlawful comments from being published, and removed such comments of its own volition whenever published. As a result of this judgment, Delfi lodged an application to the European Court of Human Rights on December 4, 2009, alleging a violation of its freedom of expression by Estonia. On October 10, 2013, the First Section of the Court released its long-awaited verdict, finding no violation of article 10 (freedom of expression). The judgment was appealed and, subsequently, referred to the Grand Chamber -- an avenue that is reserved for a very limited number of cases upon the discretion of the Court. In the following subsection, I sketch the relevant passages of the First Section's reasoning and offer a critical appraisal about its interpretation of the intermediary liability provisions.

II. ECtHR proceedings

15 The first legal question at hand in this proceeding was not whether or not there was an interference with Delfi's freedom of expression (which was an undisputed fact) but whether or not such interference was "prescribed by law" in accordance with article 10 of the European Convention of Human Rights (ECHR) [15]. In this regard, the Court emphasized the importance that the law be formulated with sufficient precision to enable a citizen to regulate its conduct, yet specific enough that the degree of foreseeability depends on the content of its text, the field it is designed to cover, and the number and status of those to whom it is addressed[16]. In this case, the Court found that the pertinent legislative and constitutional provisions, as interpreted by the case-law and in consistence with the evolution of technologies, established the principle of media responsibility for publication of defamatory comments with sufficient clarity[17].

16 While I have no knowledge of the developments of the case-law alluded to by the Court -- according to which anyone who discloses defamatory information to third parties could be found liable, even if he or she was not the publisher of the article[18] -- it seems hard to miss that the Supreme Court's interpretation is in direct conflict with the principles laid out in the EU Electronic Commerce Directive[19], which are, specifically, meant to foreclose *any* possibility of secondary liability for damages by a content host who does not play an active role giving him knowledge or control of the data stored[20]. This is an unavoidable conclusion if one considers that, following the interpretation of the Court of Justice of the European Union [CJEU] in the *Google France* case[21], conduct that is merely technical, automatic and passive is shielded from liability under article 14 of the Directive -- and that the involvement of Delfi in content regulation was just that: an automatic screening of offensive content.

17 The second, more intricate question that the Court had to entertain was whether or not the interference with freedom of expression was necessary in a democratic society, in particular to protect the reputation of others. The Court addressed the question focusing on four factors: the context of the comments; the measures applied by the applicant company (Delfi) to prevent or remove them; the alternate liability of the authors of those comments; and the consequences of the domestic proceedings for the applicant. The remainder of this section will focus on the three most salient factors, which are dense with legal considerations, and will leave the fourth with mostly factual considerations made by the court[22].

18 The first factor -- the context of the comments -- offered the court an opportunity to depart from the standard treatment of intermediary liability; what was somewhat unusual in this case is that the intermediary was also a publisher for the content that provoked the comments it hosted. However, from this circumstance alone, the Court seemed to take a jump to conclude that the controversial subject of the published article determined a higher standard of care for the applicant company (Delfi). According to the Court, this was justified for three main reasons: because the article dealt with matters that affected negatively a large number of people; because it attracted an above average number of comments; and because Delfi had a reputation of publishing defaming and degrading comments -- being one of the websites about which the editorial board of the weekly newspaper Eesti Ekspress

complained in a letter sent in 2005 to high-level government officials.

19 However, it should be noted in this regard that, while Delfi had no reason to know or to take into account the concerns expressed in the letter, the remaining two grounds appear insufficient in themselves to raise the standard of care -- in order to benefit from the safe harbor, a content host simply needs to follow the rule that content must be removed only upon existence of actual knowledge or awareness of the illegality of the content – both of which were missing before L.'s lawyers submitted their requests. Constructive awareness of illegality can be found, according to the ECJ, when a "diligent economic operator should have identified the illegality in question"[23]. Although no further clarification has been given by the ECJ concerning the notion of "diligent economic operator," one can find a valid comparator in the test devised by US courts to interpret the analogous "awareness" contained in 17 U.S.C. § 512(c)(1)(A) for content hosts in the copyright infringement context: the so-called "red flag doctrine." The doctrine has been recently clarified by two judgments of the US Court of Appeals for the Ninth Circuit and the Second Circuit[24], in the sense that for constructive knowledge to have been inferred, a court had to have established that a defendant was subjectively aware of facts that would have made the specific infringement "objectively" obvious to a reasonable person. None of the elements cited by the court appear to indicate such awareness -- although, it is true that, differently from the "classic scenario" of content hosts, the applicant company was also publisher of the news article, in the first place, which puts it into a privileged position of subjective awareness of the circumstances cited by the court. The mere fact that the article was on a controversial subject and attracted more comments than usual do not make "obvious" that it would trigger defamatory comments. Likewise, jurisprudence concerning the liability limitations established by 47 U. S.C § 230 for offensive content would shield a website from liability as a provider or a user of an interactive computer service[25], and only an active type of hosting that materially contributes to the alleged unlawfulness would disqualify it by turning it into an information content provider[26].

20 The second factor considered was the set of measures taken by the applicant company to prevent or remove the illegal comments. Here, the Court acknowledged the convenience and easy accessibility for users of the system in place for takedown requests; however, it lamented that this was only an *ex-post facto* system which, in combination with the (weak) prior filtering adopted by the company, did not ensure sufficient protection for the rights of third persons. This is another crucial passage of the judgment which, largely because of the case-specific nature of ECtHR rulings, leaves us with a certain degree of uncertainty going forward. The ECtHR seemed content with the system of notice and takedown, thus implying that the deficiencies were in the other means of protection against defamatory comments -- the word-based filtering. But, can an automatic screening system ever confer sufficient protection for the right of third parties? Also, how much does the foreclosure of the possibility for users to modify or delete their own comments count for the purposes of attaining sufficient protection? The Court concluded precisely for this particular aspect that Delfi "exercised a substantial degree of control over the comments of its portal, even if it did not use the control to the full extent as it could have"[27]. This is inextricably linked to the fact that commenters were not registered users of the community, i.e. that the website allowed online anonymity for commenters.

21 This brings us to the third and most important factor for purposes of this analysis: was the attribution of secondary liability necessary simply because it would have been excessively difficult for the victim to recover by bringing a claim against the actual actors of the comments? On this point, the Court relied on a three-fold argument: first, it recalled its judgment in *Krone Verlage (no.4)*[28], in which it found that shifting the defamed person's risk to obtain redress to the for defamation media company, usually in a better financial position than the defamer, did not amount to a disproportionate interference with the company's freedom of expression. The argument advanced here is a sensible one, but what the court did not make explicit is that by relying on it, it extends a narrow precedent of media law into the broader universe of content hosting, where the circumstances might be widely different. For example, it is not always clear that the degree of solvency of an owner of a small blog or platform would be superior to that of an author of a comment. Second, the Court pointed out that, as submitted by the government, it is very difficult to establish the identity of the alleged infringer for the purposes of bringing a civil claim. This argument has merits, too, as disclosure of identity does present serious technical and legal difficulties: from a technical perspective, even admitting that the website retains (at the time of discovery of the defaming statement) the logs regarding activity of its users, it is not to be taken for granted that the internet service provider still has the data regarding the assignment of IP addresses at that particular time –not to mention that the user might have resorted to some of the anonymization techniques described *supra*[29]. From a legal perspective, it is true that many countries do not establish a procedure for the disclosure of connection and traffic data for the purpose of civil proceedings, and the *Promusicae* case clarified that European law does not require it[30]. However, it is also

true that registration via email or other information is not a panacea for the identification difficulties: ill-intentioned users will always be able to circumvent the formalities imposed, in this particular case, simply by creating an email address associated to a fake name and address, and possibly using a secured connection away from their actual residence. Thus, the argument of "difficulty" on its face could be used to support a general principle of civil liability of intermediaries for the speech that they enable, and that is precisely against the wisdom that underlies the safe harbors contained in the E-commerce Directive and other intermediary liability legislations around the world. Third, and this is the argument that has been most critically received, the Court asserted that "it was the company's choice to allow comments by non-registered users and, [...] by doing so, it must be considered to have assumed a certain responsibility for their comments". What does this newly established concept of responsibility for anonymous comments imply? The hint given by the Court in the following passage, in acknowledging the tension between "the importance of the wishes of Internet users not to disclose their identity in exercising their freedom of expression" and "the spread of the Internet and the possibility – or, for some purposes, the danger – that information once made public will remain public and circulate forever," that the imposition of such responsibility would be necessary because intermediaries constitute the nevralgic point where this tension is most aptly managed. In other words, it would be up to intermediaries to decide how to structure their services in such a way as to ensure proper balancing between freedom of expression and anonymity on the one hand, and protection of dignity and informational self-determination on the other. Most importantly, intermediaries can be held responsible whenever such balance swings too heavily in favor of one of these two conflicting interests. This is based on the assumption that it is both less costly and more effective to impose such responsibility on them than relying entirely on private citizens to detect illegal material and enforce the law against alleged infringers. Yet, what this assumption fails to properly acknowledge is the different role played by intermediaries in detection and enforcement: due to the imperfection of identification technologies, which are prone to errors of type I (overinclusion)[31] and type II (underinclusion)[32] -- the deployment of machines for the detection of illegal content must be combined with a certain extent of human interaction. However, it is argued that because of the ease of disclosure and the amount of information available on the Internet, the legal system cannot expect that such human interaction occur on a systematic basis prior to making such information available; that would clearly impose an excessive burden on the intermediary, as it would weigh significantly on the shoulders of small and medium-sized intermediaries, and thus limit the amount of competition in the market for content hosts, thereby increasing market concentration and, potentially, the ability of the remaining players to restrict speech on their platform. For this reason, the new concept of responsibility established by the ECtHR not only appears in conflict with the explicit exclusion of monitoring obligations in the E-Commerce Directive and its national implementations, but it is also likely to endanger competition in the market for content platforms. The following section will elaborate more on this and other issues that this judgment has brought to the forefront.

C. Towards the end of online pseudonymity?

22 The previous section explained and criticized the way in which the ECtHR has reached the conclusion that states can impose secondary liability for defamatory comments posted by non-registered users, even if a content host has promptly reacted to a victim's notification. This section takes this conclusion as given, and explores the implications that the enactment of such a policy could have for the governance of content on the Internet.

23 Although the judgment did not prescribe any particular procedure that would prevent content hosts from further incurring into liability in Estonia and in other regimes that replicate the same conditions[33], two clear routes seem possible: 1) the most straightforward solution: disabling anonymous commenting and anonymous user content creation, and 2) the most challenging and articulated solution: increasing *ex-ante* control over comments.

24 Logically, the vast majority of operators will, for practical reasons, choose n. (1). For this reason, it is important to stress that this move, combined with the recent trend of certain social networks[34] and microblogs[35] to adopt a "real name" policy, can be a dangerous step towards the establishment of an integrated real-name-based network. While a reading of the *Delfi* judgment suggests that the news portal would probably have been able to escape liability by allowing users to interact under a pseudonym, the underlying rationale for this was -- at its core -- the difficulty of identifying infringing users for purposes of compensation. Now, although a registration via email makes a user somewhat more traceable, it is a far less effective means to that end than registration with a government-issued ID -- as *supra* mentioned, it is not hard for a user to circumvent the requirement in order to avoid recognition of his or her real identity. Thus, the idea that courts will in the near future find the use of pseudonyms insufficient from an enforcement perspective does not seem far-fetched. Registration

through government ID is likely to be effective regardless of the procedure chosen to enforce it. Currently, the solutions implemented on the market are of three types: the strictest form of verification is that of scanning the document to ensure it matches the credential in the website, as in the case of Airbnb[36]; the intermediate form is the one in place in China, where people are required to provide their ID number (which may or may not be checked by the relevant authority) before logging in microblogs; and finally, the weakest form of oversight is that of social networks like Facebook and Google Plus, where an ID may only be requested in case of contestation of the self-declared generalities. In all these scenarios, the request for verification is accompanied by the threat of criminal sanctions for use of a fake ID, which in turn may be considered sufficient for obtaining an order to the Internet service provider to disclose connection and traffic data in relation to that particular user. In any case, it is clear that an immediate consequence of this ruling would be a slippery slope towards real-name Internet surfing.

25 Fragmentation of cyberspace would be another problem caused by a bias against platform anonymity, at least as long as countries do not adopt a uniform system of legal protection for online anonymity or pseudonymity. For example, Germany's article 13 VI of the Telemedia Act of 2007 requires Internet service providers to "allow the anonymous or pseudonymous use of telemedia services and their payment, insofar as this is technically feasible and reasonable. The user must be informed about this possibility". Even though it has been clarified that this does not mean a right to stay anonymous *vis a vis* the service provider[37], which may require his or her real name in their contractual relationship, this provision has led to a court battle between the German data protection authority and Facebook over the possibility to use pseudonyms within the Facebook website[38]. Although the controversy was not resolved on the merit but with a finding of inapplicability of German data protection law in light of the processing of data occurring in Ireland, the difficulty in ascertaining the actual location of the processing data and the conflict between the application of two different data protection laws (one requiring and the other not requiring pseudonymity) highlighted how concrete the possibility is that multinational providers will be unable to enforce a real-name policy uniformly, across different countries. A similar conflict could occur with the analogous pseudonymity requirement recently introduced into legislation by the Australian Privacy Principles, which went into effect on March 12, 2014[39]. These inconsistencies may end up motivating several users to utilize VPNs or proxies in order to circumvent geo-location and receive the privileges offered by the law of a particular country, ultimately pushing towards anonymity not only *vis a vis* users of the platforms, but also against law enforcement agencies -- even for serious criminal matters.

26 Further segmentation is likely to occur even *within countries* if content hosts choose to adopt a mixed regime, in which they offer second-tier services to anonymous users, with limited or abridged capacity to create content and interact with other users. This would lead to the creation of a suboptimal Internet experience for those wishing to remain anonymous, and impair their ability to use the Internet to further what is its fundamental goal: enabling communication. As this practice turns into a convention, the use of differentiated services between anonymous and registered users will likely make anonymity so unattractive as to become, in the long run, gradually meaningless. In other words, modeling liability on the basis of characteristics relating to the originator of content, as opposed to the content, itself, would lead to the creation of an important bias against pseudonymous speakers, running counter to the idea of the Internet as a global public resource available to all, and an empowering technology. As a matter of fact, this would lead to the exclusion of the voices of several people who seek anonymity for a variety of legitimate reasons that are often related to safety, fear of retaliation or repercussions in the professional context, and prejudices which a potential speaker wishes to overcome in order to freely engage in Internet communication[40]. Again, this will push those people who treasure anonymous speech to increasingly resort to circumvention technologies -- and, if necessary, even the use of fake IDs -- thus, simply increasing the amount and scope of "illegal acts", and reducing the ability of public authorities to enforce a law that, depending on the amount of "civil disobedience" generated by the adoption of these policies, will be perceived less and less socially acceptable. And, given the magnitude of the public outcry following the recent revelations by Edward Snowden about the US National Security Agency and the civil movement that it has generated[41], one can expect significant support from the crypto community to ensure the protection of anonymity. To be clear, this is not to deny the importance of a phenomenon that is already occurring, and that regulators can arguably do little to prevent; the argument is simply that oppressive control inevitably leads to increased instances and forms of evasion. Much like between hackers and security systems, malwares and antivirus programmers, and, in some sense, peer-to-peer copyright infringers and the copyright industry, there will always be a set of more "skilled" or simply "undismayed" users managing to circumvent the technology of control that proves sufficient for the majority of the population. However, when such technology is used to deprive those users of their essential liberties (a reaction from content hosts that may unfold

from the confirmation of the Delfi judgment), the movement of protest and liberation from control will be of a much wider scale, thereby leading to the complete ineffectiveness and repulsion of the current system of law and governance.

27 We have already touched in the previous section upon the main challenges to an effective implementation of the alternative solution (n. 2) to disabling pseudonymity following the *Delfi* judgment, i.e. enhanced content oversight. In particular, it has been pointed out that the sensitivity of certain fine-grained distinctions required in determining the legality of content makes it impossible to rely on a completely fool-proof machine, and that systemic human oversight implies substantially raising the costs of doing business for content hosts. So, what kind of scenario can we expect in the aftermath of *Delfi*, were the notion of responsibility for pseudonymous comments to be confirmed by the Grand Chamber? The most visible consequence would be that big players with adequate economies of scale and of scope would be willing and able to use reliable algorithms for the detection of potentially illegal content, as they are currently doing for copyright infringement. The other, small- and medium-sized websites would probably end up outsourcing this task to independent technology providers, which are increasingly emerging in the marketplace[42], but will never attain the same degree of accuracy and effectiveness. As the economics of search engines demonstrates[43], the key factor to the improvement of algorithms is not simply a large enough amount of data points to form a rich database of "potentially illegal" content (although that is clearly a first threshold requirement), but more importantly, the capacity to connect through them in a sensible manner. This can only be done through continuous experimentation, which in turn requires a continuous flow of traffic that can be used to test, verify and challenge the accuracy of the connections established by the algorithms. For this reason, it is clear that large operators already have a significant advantage over small content hosts, which are unlikely to catch up absent a regulatory obligation on the part of the established operators to share their tools for detection. Worse yet, the scenario prospected here would increase the dominance of the big market players, in light of the liability that is likely to be imposed upon the adopters of "inferior" technologies in the detection of illegal content; this is because large operators would be able to rely on a *bonus pater familias* defense[44], proving their diligence in having adopted "state-of-the-art" technology to detect defamatory content. What is unclear from the Delfi judgment is the extent to which a content host would also need to prove that the utilized technology is effectively functioning for its purpose; again, this is largely due to the case-specific nature of ECtHR rulings, but a question remains concerning how much more sophisticated (and effective) should Delfi's screening system have been in order to escape liability, in the Court's view. This may leave some wiggle room for smaller platforms that achieve a sufficiently effective detection algorithm, but they would have to risk their judgment regarding the margin of error that is likely to be tolerated for the purpose of accepting a particular technology as offering "adequate protection" of the rights of third parties.

28 In any case, it should be kept in mind that the potential sufficiency of an effective detection algorithm was considered in *Delfi* only in conjunction with the operation of a user notification system, whereby requests for takedown could be received by the company so as to proceed expeditiously to removal. This constitutes an essential component of the envisaged system of protection, which enables the achievement of the ultimate purpose by complementing the best technology with the sensibility that only a human being can have towards nuanced uses of language and complex balancing exercises. In the case of smaller platforms, for the reasons mentioned above, the extent of human involvement will have to be extensive, if not exclusive. As noted, this runs contrary to the provision excluding the imposition of monitoring obligations, which is widely recognized in Internet intermediary liability regimes around the world[45]. Others have expressed disappointment with the fact that the Court in Delfi has seen this prohibition as an innovative policy measure, and not strictly as a requirement of human rights law[46]. In fact, what the Court is missing here is, on the one hand, the privacy issues stemming from such practice and, on the other, the consequences that this is likely to generate in terms of competition amongst platforms and their ability to set restrictive terms of service, to the detriment of the freedom of expression of their users.

D. How to stop it

29 Although the core objective of this article is to show the problems that an acceptance of *Delfi* would generate for intermediaries and Internet users, it seems appropriate to suggest, also with a *pars construens*, how the Court *should* have ruled – and how the Grand Chamber should approach this issue going forward.

30 As it has been stressed already, there are a number of situations where anonymity constitutes, as an enabler of speech, an essential pre-requisite to the enjoyment of human rights. At the same time, it is clear that not all cases of anonymity are matters of human rights, and it is very difficult to ascertain the extent to which a request for anonymity belongs to

one group or the other. First of all, this is a difficult task because anonymity is not a human right, in and of itself; rather, it may constitute an intermediate condition for the enjoyment of a variety of human rights – such as freedom of expression, privacy, life, liberty and security, freedom of thought, conscience and religion. Therefore, in order to establish whether anonymity is required by human rights law, it needs to be determined the extent to which it is needed for the enjoyment of one of those rights. This is inherently hard to accomplish because the merits of the argument that may be put forward in support of protection of anonymity depend on the accuracy of a prospective evaluation, i.e. on the occurrence of an action or a series of actions in the future.

31 Secondly, the very act of evaluating the necessity of anonymity in a particular case requires a disclosure that may defeat its purpose: unless there is strict separation between the entity that is seeking disclosure and the one who is adjudicating, combined with a strong system of safeguards to prevent leaks from the latter, anonymity may be compromised by the mere act of evaluating whether it is well-founded.

32 Due to the complexity of these evaluations, it is quite logical to expect intermediaries to steer away from case-specific assessments and, therefore, embrace categorical solutions- generally speaking, either allowing or not allowing online anonymity or pseudonimity. However, as we have seen in Section 1, anonymity is not a monolith: it is a concept which can be modeled in scope and depth. Accordingly, in order to allow for the emergence of a human-rights compliant solution, it is necessary to identify which aspects of anonymity are specifically sought by users. Since the range of users and demands is very wide across different groups and geographies, it is argued here that a key, and often underestimated, value for the establishment of balanced and respected legal rules of anonymity protection is the encouragement of competition on this feature: only competition in the market can ensure the continuous availability and improvement of empowering technologies.

33 This is exactly the opposite of what the *Delfi* decision stimulated: a system of incentives that impose technological mandates tipping the market in favor of the already-established big players deters market-based solutions to the problems of human rights compliance, and impairs the ability of the State to ensure protection of the rights of users *vis a vis* intermediaries. In contrast, a market-based system would enable the existence of certain platforms that offer better protection for privacy and of the reputation of others, even if it comes, admittedly, at some cost for ease of use or freedom of expression. Thanks to the ability of technology to incorporate the modularity of anonymity, protection can be granular and tailored to the needs of users, allowing competition to unleash on even the smallest details. As a result, people would get to learn about the pros and cons of new technologies and would be naturally attracted to those platforms and applications that offer features (including anonymity privileges) that best cater to their needs.

34 However, it is necessary to draw a line in order to prevent those technologies from making law enforcement impossible or unfeasible. Competition in technological solutions to anonymity is, indeed, welcome for the development of innovative solutions, but only as long as it occurs within a framework of minimum standards -- which may be called of "procedural" and "substantive" due process -- that protect fairly and equally the interests of the parties involved. For this reason, it is suggested here that the ECtHR should have reflected on what those standards are, particularly to the extent to which an alleged infringer has a right to have its anonymity protected by a third party, and eventually asked this question: should the intermediary bear the burden for failing to actively engage in the evaluation of such entitlement? I suggest that it should not; rather, the ability of the intermediary to provide a forum for the evaluation of respective weight of the claims of protection can be harnessed to promote the respect of ECHR rights in a consistent manner across ECHR member States.

E. Delineating a "due process" doctrine from the existing ECtHR case-law

35 Since we are discussing an ECtHR case, the solution should, in principle, be sought in the jurisprudence of that Court, defining the way to handle balancing of the right to anonymity of third parties with conflicting state interests. While the Court only adjudicates specific matters and grants States a certain margin of appreciation in undertaking their balancing of conflicting interests, there are situations where it has made clear that a State has exceeded its margin, crossing the line of permissible interference with a Convention's right. Thus, these "red lines" crossed by the Court can be taken as useful guidance in defining minimum standards. Such red lines are concerned with both substantive and procedural due process concerns.

36 First of all, procedural due process: to define whether the State's appreciation has remained within an acceptable limit, the Court needs to ascertain whether the interference was prescribed by law. As often clarified by the Court[47], such law should not only be formally in place, but also be both adequately accessible and foreseeable. This means that it must afford a measure of legal protection against arbitrary

interferences by public authorities with the rights safeguarded by the Convention, indicating with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise. This measure of protection can only be guaranteed if the law describes the scope of the discretion granted to the authorities with sufficient clarity, and includes legal procedural safeguards commensurate with the importance of the principle at stake. At a minimum, this must include the guarantee of review by a judge or another independent and impartial decision-making body. For example, in *Sanoma Uitgevers B.V.*[48], the Court was required to decide the proportionality of the interference by the police with the right to non-disclosure of anonymity for public order reasons. Here, the right to anonymity concerned the identity of third parties engaged in illegal car races, who appeared in the pictures taken by a reporter that had been authorized to do so only after having guaranteed that it would preserve the anonymity of the participants. However, prior to the publication of the reporter's article, police officers suspected that one of the vehicles participating in the race had been used as a getaway car following a ram raid. Having been informed of the picture taken at the race, the authorities compelled the editor of the magazine to release the photos, which enabled the police to identify the drivers of that car. The Court found this to be an interference with regards to the journalistic privilege of source protection (stemming from the right to freedom of expression[49]) and not prescribed by law, in that the legal system did not allow review by an independent body *before* access and use of the seized material.

37 In more complex cases, the Court needs to engage in a more detailed overview of the balancing of the interests at stake. However, the way it does so and avoids substituting itself *in toto* to the judgment of the states is by adopting a procedural posture (also known as "proportionality balancing"[50]) -- that is, defining whether the appropriate procedural framework was in place to be able to satisfy (in general terms) the holders of the different interests at stake, and whether the measure adopted is, as a result, more restrictive than necessary. In doing so, by ranking values and solving conflicts on the basis of relative weight, it inevitably delineates a doctrine of "substantive due process".

38 In *Godelli*[51], for example, the Court had to determine whether the grant of perennial anonymity to women giving birth in public hospitals was a proportionate interference with the applicant's right to know her origins, which is integral part of the right to respect for private and family life. The reasons given for the existence of a law guaranteeing such a strict adherence to anonymity were the protection of a woman's interest in remaining anonymous in order to protect her health by giving birth in appropriate medical conditions, the freedom of women to decline their role as mother or to assume responsibility for the child, and the general interest of the State to protect the mother's and child's health during pregnancy and birth and to avoid illegal abortions and children being abandoned in ways other than under the proper procedure. Despite recognizing these objectives as well-founded, the Court contrasted the measure taken by the Italian State with the more flexible approach of France, analyzed in *Odièvre*[52], which permitted a son or daughter to obtain non-identifying information about the anonymous parents and to request the mother's identity be disclosed with the consent of the latter to a National Council for Access to Information about Personal Origins. It concluded that, since the Italian system did not attempt to strike any balance between the competing rights and interests at stake, the interference was disproportionate.

39 In a vocal dissent, Judge Sajo stressed the importance of what he believed to be direct emanation of the highest value of the convention: the right to life. Reflecting on the system of incentives that the provision in question created, he pointed out that what this serves, ultimately, is the right to life of the offspring – which would have, otherwise, been endangered. Interestingly for our purposes, he specified:

> Of course, the right to life is only indirectly protected by the anonymity provision. However, this supremacy is decisive for me in the balancing exercise, which cannot be limited to a conflict between two Article 8 right-holders.

40 While it is questionable –as deemed by the majority- that this principle would necessarily lead to the permissibility of a blanket grant of anonymity, this judgment is illustrative of one important parameter in the methodology that should be used to assess the rank of anonymity protection: above all, anonymity should be guaranteed when it clashes against the right to life (protected by article 2 of the Convention). At the same time, because of the rank of the right to life in the Convention, anonymity should be protected more forcefully when it is justified by the need to protect such a right.

41 A further notable aspect of the dissent is its focus on the long-term consequences of the decision, and in particular on the incentives that a grant of disclosure would have on the behavior of prospective mothers in similar cases. This is precisely the kind of reasoning that would have allowed the Court to ascertain, in *Delfi*, the enormous consequences that a ruling allowing intermediary "responsibility" for user comments would have on the ability of individuals to express themselves anonymously in the future, and thereby receive protection for some

of their Convention rights while exercising their right to speak.

42 Another complex case on anonymity protection is *K.U. v Finland*[53], where the Court was asked to establish whether the absence in the legal framework of an injunction to compel ISPs to disclose the identity of a subscriber liable of a criminal offence amounted to a disproportionate interference with the right to respect for private and family life for the victim, and a justified interference with his right to an effective remedy. In particular, such possibility existed for certain offences, but not for the type of misrepresentation committed by the customer in question (posting the photo and contact information of a minor and inviting people to contact him "to show him the way"). The Court noted that the facts at hand concerned a serious matter of interference with private life in the sense protected by article 8 ECHR (because of the potential threat of sexual abuse), and that effective deterrence against grave acts where fundamental values and aspects of private life are at stake requires *efficient* criminal law provisions[54]. The Court conceded that freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, but remarked that such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others[55]. For this reason, and without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, the Court made clear that "it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context[56]".

43 This judgment illustrates again the typical approach taken by the Court to complex balancing: bearing in mind that its role is not to substitute its view to that of the member State in question, it ensures that the adequate procedural framework is set in place so that the conflicting interests are taken into account. However, what procedural framework will be considered adequate depends on the weight attached to the interest to be protected. In this case, having regard for the potential threat to the victim's physical and moral integrity, the Court reminded us? of the vulnerability of individuals at such a young age (12 years old) and concluded that there had been a violation of article 8 because both the public interest and the protection of victims of crimes committed against their physical and psychological well-being require the availability of a remedy enabling the actual offender to be identified and brought to justice.[57]

44 Again, one can see the role that incentives play in this regard: the reasoning of the court is that if there is no possibility of identifying the perpetrator and bringing him to justice, it is unlikely that prospective offenders will refrain from engaging in such conduct in the future. And once again, what the Court took issue with was the lack of an appropriate procedural framework to duly take into account the respective interests at stake, which the State had a positive obligation to ensure[58]. By doing so, the Court showed the way in which substantive considerations are to be taken into account for "procedural due process" purposes: when balancing between conflicting interests, States must ensure that the legal system does not neglect or insufficiently take into account the interest of protection from "grave" acts.

F. Situating platform anonymity within the existing technological framework

45 Today, technology offers an opportunity for companies to market products that incorporate modularity, and to ensure that such procedural framework can be implemented by design, enabling the intermediary to undertake a first instance balancing between competing rights and interests. For example, the recent platform Whisper grants anonymity but, in exchange, "vets" the content posted by users in line with its terms and conditions[59], deciding over publication on the basis of the public interest character of the matter to be disclosed[60]. Similarly, in the copyright context, Vimeo's Copyright Match immediately fingerprints its content and searches for matches in its database to detect any possible infringement by videos being uploaded by its users, enabling immediate removal. At the same time, however, Vimeo allows users to explain possible circumstances justifying the upload notwithstanding the match, including the open-ended and balancing-centered defense of "fair use"[61].

46 It should also be clarified that the specific programs or applications which guarantee anonymity by default are of two different kinds: one offering anonymity *vis a vis* users of the same platform ("platform anonymity") but not *vis a vis* the internet service provider ("customer anonymity[62]") or the public authority ("citizen anonymity)[63]; the other (and more difficult to accomplish) gives partial "citizen anonymity" and "customer anonymity", through the use of Tor or VPNs and other technological arrangements that minimize the disclosure of identifying information[64]. However, both types of anonymity are imperfect: they only operate at one layer -- respectively, the application layer and the network layer. In addition, the latter also requires the users to de-identify themselves by

clearing cookies between sessions and not logging into identifying applications. Furthermore, some countries (as well as some payment intermediaries[65]) have started to block or prohibit VPN providers[66], thus making the task even more complicated for an average user. Even admitting that skilled users will easily circumvent those blocks and that highly sophisticated identification techniques exist for exceptionally important targets, it should be borne in mind that more complexity requires higher expenditures for law enforcement, and it is therefore unwise for a legislator to devise a whole regulatory procedure focusing on anything other than the "average user". For an average user, who doesn't know all the precautions that he or she needs to take in order to be completely anonymous, nothing is available in the market that provides protection simultaneously at the application and the network level; so, when talking about platforms, it is clear that there will always be the possibility of tracing individual users, unless they have themselves combined the two functionalities above. It must be understood, therefore, that except for the very narrow group of skilled users, technological traceability dominates the net.

47 What this implies is that it is generally possible for platforms, in line with their terms of service, to retain, obtain and disclose the data they have gathered to perform their services. Some may voluntarily choose to erase data about their users in a very limited timeframe[67], and some may be forced by law to keep it for a longer period. The latter scenario had, in fact, materialized in the national implementation[68] of the EU Data Retention Directive (2006/24/EC), which established an obligation for providers of publicly available electronic communications services and of public communications networks to retain traffic and location data for up to six months or two years for the purpose of the investigation, detection, and prosecution of serious crime. However, the past tense is required when speaking about this Directive, since it was recently invalidated by a decision of the CJEU for its inconsistency with the protection of fundamental rights.[69] In the aftermath of the invalidation of the Directive, it is expected that its national implementations will be repealed or declared unconstitutional[70]. However, it is submitted here that a complete absence of European coordination on this matter would be problematic for the lack of uniformity that would arise as a consequence in national laws[71] and, worse yet, for the risk of insufficient protection of the rights of European citizens, who may have no, or limited, remedies available without the traffic and connection data.

48 One thing that the saga of the rejection of the data retention provisions[72] has taught legislators is that normative provisions introducing law enforcement measures with such a sweeping potential of interference with individual rights must contain adequate safeguards against abuse, and lay out with clarity the conditions on which interference with the right to private life and personal data would be allowed. In fact, the ECJ found problematic the fact that the retention obligations of the Directive applied even in the absence of evidence of any serious crime[73] and without requiring any relationship between the data and a threat to public security[74], but also that it provided no objective criterion to determine the limits and conditions of access and subsequent use of data by national authorities for the purpose of prevention, detection or criminal prosecutions of serious offences – a notion left for national member States to decide[75]. This decision shows a clear path for measures introducing technological solutions to rights adjudication, pointing to the need to specify conditions and limitations for the interference with fundamental rights, require end-means proportionality, and provide adequate safeguards against abuse.

49 The law at issue in the *Delfi* case, that was interpreted to apply to news publishers in the same way for user comments as for articles, would be unlikely to pass muster under this test. This is because such law shifts the responsibility for defamatory comments to a third party who is neither the author nor the publisher (since it does not edit the content), and does not clarify the conditions for such interference with freedom of expression. The rationale for the existence of such provision is, in the words of the ECtHR, the greater likelihood that an Internet news operator possesses the resources for continual monitoring of the Internet and an adequate financial situation for ensuring redress of the victim, compared to the little chances that a victim would have to be effectively compensated if it was required to address his or her claims to the original poster[76]. However, as pointed out earlier, the Internet has made it possible for everyone to become a publisher and run, for example, a news portal, therefore rendering the foundations of the argument of financial solvency that was traditionally applied to media somewhat shaky. In addition, the web offers also tools that enable users to easily monitor the Internet for the appearance of content regarding themselves or any information that they are particularly interested in, through search engine alert notifications.[77] In contrast, requiring a news portal to be the guardian of potential interests of anyone who might be affected by comments published by third parties in a news article amounts to a serious interference, both with the right to freedom of expression of the potential commenters and the right to property (protected by Article 1 of Protocol 1 of the Convention) of the portal operator. For these reasons, it appears that the shift of responsibility to the news publisher is more restrictive than would be necessary to achieve its aim, i.e. to ensure the ability of the victim to

become aware of a violation of their privacy, obtain prompt removal and recover from it.

50 Furthermore, the way such law has been interpreted by the ECtHR adds another layer to the problem, in suggesting that the news portal assumes a certain responsibility over comments when it allows for anonymous speech. As a matter of fact, the ruling of the court puts the measure in a light that sets the incentive for future content hosts to restrain anonymity –that is, to prevent content creation by unregistered users- and offers member States a (dangerous) opportunity to impose technological mandates for monitoring purposes, which is in direct conflict with the letter of the EU E-Commerce Directive. As noted, this would have serious consequences on the privacy and freedom of expression of users, both immediately and in the long run, by affecting competition in the market for news portals and, more generally, content hosting.

G. Conclusion: the need for standards of joint responsibility for intermediary conduct

51 Given all the above, it is submitted that the Court should have verified whether such interpretation of the law, resulting in an interference with the desire for anonymity of its users, was legitimate and proportionate in ensuring the effectiveness of redress of civil claims. Had it done so, it would have found already quite a consolidated jurisprudence in the EU providing a negative answer to that question, the general understanding being not only that monitoring obligations are explicitly excluded, but also that the law doesn't allow judges to force third parties to disclose identifying information of their customers. For example, as it was clear from the fact pattern from which a Spanish court raised a preliminary question to the ECJ in *Promusicae*, Spain does not allow the disclosure of identifying data for purposes of civil proceedings. A similar standard applies in Germany, where the ISPs can only be forced to disclose identifying information in serious criminal investigations[78] and in the case of alleged infringers of copyright on a commercial scale,[79] or otherwise obvious infringement of copyright[80]; and in Italy, where it is settled that a subscriber's information can only be disclosed by ISPs "in exchange for the protection of superior values protected by criminal law"[81]. In some jurisdictions, the possibility of obtaining such information is not foreclosed but is subject to a strict balancing of criteria that ensures the well-foundedness of the alleged victim and prevent potential abuse of the process: this is the case, for example, of the Netherlands, where the Supreme Court ruled that disclosure for civil proceedings is not prohibited by data protection law, provided that certain restrictive conditions are met[82]. Similarly, in Sweden an order for disclosure of this kind can be made if there is clear evidence of an infringement of an intellectual property right, if the information sought can be regarded as facilitating the investigation into an infringement of copyright or impairment of such a right, and if the reasons for the measure outweigh the nuisance or other harm which the measure may entail for the person affected by it or for some other conflicting interest[83]. Likewise, in United Kingdom the procedure of *Norwich Pharmacal* order can be used to require third parties involved in any kind of wrongdoing to disclose certain documents or information about the wrongdoer, but the granting of such requests is contingent on the weighing of a variety of factors which focus prominently on the balance of inconvenience[84]. One notable difference is France, where the system of injunctions seems to provide no explicit consideration for "equities" and rests entirely on the likelihood of success on the merit and irreparable harm[85], although it has been argued that balancing is increasingly conducted in intellectual property cases[86].

52 Instead, the Court should have clarified that the right to anonymity can be vital to ensuring the ability for users of a platform to engage in free speech while maintaining adequate protection for other Convention rights that can be adversely affected by the identification of the speaker. Accordingly, it should have been recognized that restrictions to anonymity must be done in accordance with the law and must be necessary in a democratic society for achieving an aim that is explicitly recognized by the Convention in relation to the article that is invoked for the protection of anonymity.

53 In the author's view, the fact that the restriction would occur, in the case at hand, through self-regulation by the intermediary in response to the incentives set up by the standard of liability imposed by the legislation, should not have exonerated the Court from reviewing the necessity and proportionality of the mechanisms of liability generated by that legislation, as interpreted by the courts and perceived by platforms in the market. In doing so, the Court could have, at least implicitly, defined the conditions under which such intermediary would be permitted to restrict anonymity without implicating the liability of the State for failure to comply with its positive human rights obligations. In particular, the Court could have established that a system of balancing operated by the intermediary and triggered by user notification would be compatible with the Convention, as long as it incorporates the standard of procedural and substantial due process that the Court has elaborated in its jurisprudence. Although going into detail as to what those standards imply would be beyond of the limited purview of the Court in a specific case, a roadmap on the major factors to be taken into

account and the procedural devices to be used for such balancing would be a significant step ahead towards clear and administrable responsibility of Internet intermediaries.

54 Incidentally, this framework would be largely transposable to the situation envisaged by the recent *Google Spain* judgment of the CJEU[87], which allows for the submission of notification to search engines for the erasure of links appearing in relation to one's personal name, and thereby attributes adjudicative powers to this particular intermediary. As a result, the clarification that could be provided by the Grand Chamber of the ECtHR is potentially of great relevance for the future of privacy and freedom of expression in the EU, not only with regard to disclosure of the identity of anonymous (or pseudonymous) commenters, but also in relation to the criteria that should be used by search engines to respond to requests of removal –and more generally, by intermediaries receiving takedown requests.

55 These criteria may be, concretely, topics that deserve, in and of themselves, another article, or perhaps an entire book, to be dealt with. My suggestion in that respect is that the definition of an overarching framework would allow intermediaries to offer in the market effective and viable solutions to anonymity conflicts, with a balancing methodology that duly takes into account all of the relevant factors. To go back to the title of this article and the question posed therein, the real answer lies not so much in choosing between the affirmative and the negative but in identifying the circumstances under which intermediaries and/or States should be held responsible for not having set an adequate framework for the evaluation of conflicting rights claims. Clear and predictable boundaries on the operating space for an intermediary in evaluating such claims would allow us to answer that question, at least succinctly, and set the seeds for a market of technological solutions to rights adjudication in accordance with the rule of law. Specifically, enabling platforms to set presumptions in favor or against anonymity disclosure in specific circumstances [88] would go a long way towards ensuring the quick resolution of those requests, avoiding an excessive hindrance to the freedom of expression of the content generators and ensuring the viability of the business model of many Internet intermediaries.

* Comments welcome at n.zingales@uvt.nl. This paper was selected among the five finalists of the Young Scholars competition at the Information Influx Conference of the Institute for Information Law on 2 July 2014. Comments from Prof. Joel Reidenberg of Fordham Law School are gratefully acknowledged.

1 L. Lessig, *Code v.2*, available at http://codev2.cc/, p. 35.

2 Although the primordial version of Internet (ARPANET) was built upon a cooperative network of trusted and verified connecting computers, this limitation was overcome as the network turned from a military project into a means of mass communication.

3 A. Debashis, On the Internet, nobody knows you're a dog, University of North Carolina at Chapel Hill (1993).

4 The handbook on European data protection law recently published by the European Union Agency for Fundamental Rights, the Council of Europe and the Registry of the European Court of Human Rights adopts a strict stance to the concept of "anonymisation", with direct bearing on the understanding of "anonymity", by requiring *all* identifying elements to be eliminated from a given set of personal data. However, at the same time the Handbook neither defines what such elements are, nor does it prescribe the complete, irreversible anonymization which would make it impossible any type of re-identification: making reference to recital 26 of the EU Data protection directive, it specifies that in the course of anonymisation, "*no element may be left in the information which could, by exercising reasonable effort, serve to re-identify the persons(s) concerned*". See European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (Luxembourg, Publications Office of the European Union, 2014), p. 45 (emphasis added).

5 See V. S. Ekstrand & C. I. Jeyaram, Our Founding Anonymity: Anonymous Speech During the Constitutional Debate, 28 American Journalism 35 (2011).

6 See e.g. P. Ohm, Broken promises of privacy: Responding to the surprising failure of anonymization, UCLA L. Rev., 57, 1701 (2009); A. Narayanan and E. W. Felten, No silver bullet: De-identification still doesn't work (July 9th, 2014), available at http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf (accessed July 2014); see also M. Braga, Sticky data: Why even 'anonymized' information can still identify you, The Globe and Mail (Aug 06, 2014) http://www.theglobeandmail.com/technology/digital-culture/sticky-data-why-even-anonymized-information-can-still-identify-you/article19918717/ (accessed August 2014)-

7 See "Introducing Airbnb Verified ID". Available at http://blog.airbnb.com/introducing-airbnb-verified-id/ See also https://myverifiedid.com/what-is-it.

8 See A. Hsiao, "ID Verify". Available at http://ebay.about.com/od/glossaryofebayterms/g/gl_idverify.htm.

9 See for example, http://www.facerec.com/ and http://www.facedetection.com/.

10 "Citizen" is used here as a generic notion, of an individual that is subject to the jurisdiction of the public authority in a particular state.

11 One significant step in the direction of "citizen anonymity" is end-to-end encryption of communication. However, while this can be a solution to prevent mass surveillance abuses by the authority, it is (1) unlikely to withstand individual and targeted efforts; and (2) concerning only the content of communications, and not the information regarding the end points of the conversation. See Eric J. Stieglitz, Note: Anonymity on the Internet, 24 Cardozo Arts & Entertainment Law Review 1395 (2007), 1401.

12 VPNs is the acronym for Virtual Private Networks, which create an encrypted connection between a PC and a remote server, preventing traffic data (including the IP address) to be transmitted to the visited website. Web proxies are browser add-ons which perform the same routing function, but do not encrypt all traffic and for this reason can handle many more requests at the same time. Both may retain traffic logs, which they can still be ordered to disclose through the regular legal process. Finally, there are special anonymity applications that enable users to access the Internet anonymously, much like in VPNs, but use a specific technique consisting in using multiple servers to relay data across several randomly chosen nodes of the network ("onion routing"). The most common example is

of TOR (acronym for The Onion Router), a free open network originally developed by the US Navy to protect government communication. With TOR, it is practically impossible to identify the IP address; however, data is more vulnerable when it leaves the last server (so called "exit server"), as it must be unencrypted before reaching the target website. Unsurprisingly, this weakness of TOR and other VPNs has led to a finding of liability on the part of the identifiable user operating an "exit server" which routed an illegal exchange occurred within a private and encrypted filesharing network, and resulted in an injunction from transferring the copyright infringing song with a maximum penalty of €250,000 or a six month prison term. See LG Hamburg, 24 September 2012 (308 O319-12).

13 A classic example, which will be discussed more in detail infra, is the possibility to obtain further information after having identified an alleged infringer through a "DNS reverse lookup" on the IP address used to perform a certain action, which traces the ISP who provided the Internet connection. As a general rule, the legal system does not offer the possibility in civil matters to obtain the names of the subscribers to whom the particular IP address identifying the alleged infringer was assigned; by contrast, this is a routine procedure in criminal matters, provided that the adequate procedures are followed. See e.g. Principle 7 of the Declaration on freedom of communication on the Internet, adopted on 28 May 2003 by the Committee of Ministers of the Council of Europe, according to which: "*In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police*" (emphasis added).

14 *Delfi v. Estonia*, Judgment of the ECtHR on 10 October 2013 (Application no. 64569/09).

15 In particular, article 10.2 recites: "*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*" (emphasis added).

16 At 72.

17 *Delfi*, at 75.

18 See in particular Supreme Court of Estonia, case no. 3-2-1-95-05 of 21 December 2005, and case no. 3-2-1-67-10 of 21 December 2010, both cited in the *Delfi* judgment at 38.

19 In particular, article 14 ("hosting) and 15 ("no general obligation to monitor").

20 See in this sense ECJ judgment of 12 July 2011 in Case C-324/09, *L'Oreal and Others.*

21 ECJ Judgment of 23 March 2010, joined Cases C-236/08 to 238/08, *Google France and Google.*

22 The fourth factor considered by the court was the consequences of the imposition of a damages liability for the applicant company, which, given its size and the relatively small amount awarded, weighed in favor of the finding that such (small) interference with the applicant's freedom of expression was not disproportionate.

23 Case C-324/09, *L'Oréal and others v. eBay* [2011], para. 120.

24 *UMG Recordings, Inc. v. Shelter Capital Partners*, 718 F.3d 1006, 1027 (9th Cir. 2013); *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 36, 38 (2d Cir. 2012).

25 For an overview, see J. R. Reidenberg et al., Section 230 of the Communications Decency Act: A Survey of the Legal Literature and Reform Proposals, Fordham Law Legal Studies Research Paper No. 2046230, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2046230 (accessed August 2014)

26 *Fair Housing Council*, 521 F.3d 1157, at 1168.

27 *Delfi*, at 89.

28 *Krone Verlag GmbH & Co. KG v. Austria* (no. 4), no. 72331/01, para. 32, 9 November 2006.

29 See *supra*, section I.

30 However, it does require that in the transposition of its Directives, "Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order"...and" must not only interpret their national laws in a manner consistent with those directives but must also make sure that they do not rely on an interpretation of them which would conflict with those fundamental rights or with the other general principles of Community law such as the principle of proportionality". See *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Case C-275/06. CJEU January 29, 2008.

31 See for instance, the recent case of the siren of a car in an uploaded performance of Grant Theft Auto, mistakenly confused with a famous copyrighted jazz song: http://www.escapistmagazine.com/news/view/130742-Kevin-Smith-Defends-Lets-Plays-Speaks-Against-YouTubes-Content-ID.

32 As was the case with the automated filtering adopted by Delfi. See *Delfi*, at 87.

33 An example is the UK Defamation Act 2013, which provides a defense from secondary liability for website operators only as long they allow victims to identify posters. According to Section 5 of the Act:

> *"(1)This section applies where an action for defamation is brought against the operator of a website in respect of a statement posted on the website.*
>
> *(2)It is a defence for the operator to show that it was not the operator who posted the statement on the website.*
>
> *(3)The defence is defeated if the claimant shows that—*
>
> *(a)it was not possible for the claimant to identify the person who posted the statement,*
>
> *(b)the claimant gave the operator a notice of complaint in relation to the statement, and*
>
> *(c)the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.*
>
> *(4)For the purposes of subsection (3)(a), it is possible for a claimant to "identify" a person only if the claimant has sufficient information to bring proceedings against the person".*

34 For Facebook, see https://www.facebook.com/help/292517374180078; for Google plus, see http://content.time.com/time/business/article/0,8599,2094409,00.html.

35 In China, the use of "real names" is mandated by government regulation. See D. Caragliano, "Why China's 'Real Name' Internet Policy Doesn't Work", The Atlantic (March 26, 2013). Available at http://www.theatlantic.com/china/archive/2013/03/why-chinas-real-name-internet-policy-doesnt-work/274373/.

36 See *supra*, Section I, footnote 4.

37 OLG Dusseldorf, MMR 2006, 618 at 620.

38 See S. Schmitz, "Facebook's Real Name Policy: Bye-bye, Max Mustermann?", 4 (2013) JIPITEC 3, 190. See also http://www.theverge.com/2013/2/15/3991458/german-court-rules-in-facebooks-favor-europeans-must-use-real-names-.

39 Available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-2-app-2-anonymity-and-pseudonymity.

40 For an account of beneficial motivations behind anonymity, see V. S. Ekstrand, "The Many Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law", 18 Journal of Technology Law and Policy 1 (2013). For an empirical study about the motivations behind pseudonymity in Google Plus, see http://infotrope.net/2011/07/25/preliminary-results-of-my-survey-of-suspended-google-accounts/.

41 Most notably, the International Principles Applicable to Communication Surveillance (https://en.necessaryandproportionate.org/text) and "The day we fight back" initiative (https://thedaywefightback.org/). More recently, see the "Reset the net "campaign (https://www.resetthenet.org/).

42 See for example Muso: www.muso.com; Tunesat: https://tunesat.com/tunesatportal/home; Discovery Anti-Piracy Service: http://info.icopyright.com/discovery-anti-piracy-copyright-infringement-check-duplicate-content; ACID: http://www.prnewswire.com/news-releases/autonomys-virage-automates-copyright-infringement-detection-for-online-video-57891637.html. For a longer list, see M. Barr, Tools to Detect Software Copyright Infringement, at http://embeddedgurus.com/barr-code/2010/09/tools-to-detect-software-copyright-infringement/.

43 See N. Zingales, Product Market Definition in Online Search And Advertising, 9 (1)Competition Law Review 29 (2013), 44.

44 *Bonus pater familias* is a Latin expression frequently used in Roman law and which can by and large be equated with the duty of care of a reasonable man in common law parlance. This also resembles the "diligent economic operator" criteria devised by the ECJ in *L'Oréal and others v. eBay* to infer awareness of illegality from circumstances in which "a diligent economic operator should have identified the illegality in question.

45 An example outside the reach of EU law and thus of Article 15 of the E-Commerce Directive is the Digital Millennium Copyright Act, whose section 512m provides that "Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on [...]a service provider monitoring its service or affirmatively seeking facts indicating infringing activity [...]".

46 M. Husovec, ECtHR rules on liability of ISPs as a restriction of freedom of speech, 9 (2) Journal of Intellectual Property Law & Practice 108 (2014) 109.

47 See for instance the *Sunday Times v. the United Kingdom* (no. 1) judgment of 26 April 1979, Series A no. 30, § 49; *Tolstoy Miloslavsky v. the United Kingdom*, 13 July 1995, § 37, Series A no. 316-B; *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V; *Hasan and Chaush v. Bulgaria* [GC], no. 30985/96, § 84, ECHR 2000-XI; and *Maestri v. Italy* [GC], no. 39748/98, § 30, ECHR 2004-I.

48 *Sanoma Uitgevers BV v Netherlands*, Merits and just satisfaction, App no. 38224/03 [2010] ECHR 1284, IHRL 3714 (ECHR 2010), 14th September 2010.

49 It should be noted also that the importance of the protection of journalistic sources for freedom of expression is explicitly recognized in Recommendation No. R(2000) 7, on the right of journalists not to disclose their sources of information, adopted by the Committee of Ministers of the Council of Europe on 8 March 2000. The Recommendation established (in its principle 3b) that the disclosure of information identifying a source should not be deemed necessary unless it can be convincingly established that:

i. reasonable alternative measures to the disclosure do not exist or have been exhausted by the persons or public authorities that seek the disclosure, and

ii. the legitimate interest in the disclosure clearly outweighs the public interest in the non-disclosure, bearing in mind that:
- an overriding requirement of the need for disclosure is proved,
- the circumstances are of a sufficiently vital and serious nature,
- the necessity of the disclosure is identified as responding to a pressing social need, and
- member States enjoy a certain margin of appreciation in assessing this need, but this margin goes hand in hand with the supervision by the European Court of Human Rights.
c. The above requirements should be applied at all stages of any proceedings where the right of non-disclosure might be invoked.

50 See A. Stone Sweet and J. Mathews, Proportionality Balancing and Global Constitutionalism, 47 Columbia Journal of Transnational Law 68 (2008).

51 *Godelli v. Italy*, (no. 33783/09), 18 March 2013.

52 *Odièvre v. France* ([GC], no. 42326/98, ECHR 2003- III.

53 *K.U. v Finland*, no. 2872/02, 2 December 2008.

54 *Id.*, at 43 (emphasis added).

55 *Id.*, at 49.

56 *Id.*

57 *Id.*, At 47.

58 In particular, the Court found that the positive obligations that are inherent in an effective respect for private or family life (see *Airey v Ireland*, 9 October 1979, Section 32, Series A no. 32) include the adoption of measures designed to secure respect for private life even in the sphere of the relations of individual themselves.

59 See A. Greenberg, "Whistleblower apps not as anonymous as they seem", Wired (May 16, 2014). Available at http://www.wired.co.uk/news/archive/2014-05/16/whistleblowers.

60 See R. Lawler, "Whisper CEO Michael Heyward Defends Gwyneth Paltrow Post", Wired (May 7, 2014) http://techcrunch.com/2014/05/07/whisper-michael-heyward-tc-disrupt/.

61 D. Witt, "Copyright Match on Vimeo". Available at http://vimeo.com/blog/post:626.

62 Customer anonymity *vis a vis* technical ISPs (that is, internet access providers) can only be achieved when using someone else's network which does not require authentication, and is not as such "offered" in the market.

63 Examples of this are platforms like "Whispers" and "Secret". See B. Ortutay, Whispers, Secret and Lies? Anonymity Apps Rise". Available at http://bigstory.ap.org/article/whispers-secrets-and-lies-anonymity-apps-rise.

64 See for example the new App "Onionshare", which allows transfer of file through the darknet allowing untraceability of the original sender (unless he or she makes a mistake in the anonymization procedure): see A. Greenberg, "Free App Lets the Next Snowden Send Big Files Securely and Anonymously", Wired (May 21, 2014). Available at http://www.wired.com/2014/05/onionshare/.

65 See "Mastercard and Visa block payments to Swedish VPN firms", The Register (4 July 2013), http://www.theregister.co.uk/2013/07/04/payment_block_swedish_vpns/; "Paysafecard begins banning VPN providers", Torrentfreak (25 August 2013), https://torrentfreak.com/paysafecard-begins-banning-vpn-providers-130825/.

66 See for instance "UK internet filter blocks VPNs, Australia to follow soon?", Torrent Freak (5 September 2013), http://torrentfreak.com/uk-internet-filter-blocks-vpns-australia-to-follow-soon-130905/; "Iran to crack down on web-censor-beating software", Daily News (10 June 2012), http://www.hurriyetdailynews.com/iran-to-crack-down-on-web-censor-beating-software.aspx?pageID=238&nID=22789&NewsCatID=374.

67 This has happened for the major search engines, which, partially under the pressure of the European Article 29 Working Party, have progressively lowered the amount of time they keep their users' search log to 6 months (180 days).

68 See the High Court's decision in *Chambers v. DPP* [2012] EWHC 2157 on [2012] 27 July 2012, holding the obligations established by the Directive applicable to social networks.

69 Judgment of the Court (Grand Chamber) on 8 April 2014, joined. Cases C-293/12 (*Digital Rights Ireland*) and C-594/12 (*Kärntner Landesregierung*)

70 See J. Rauhofer, D. Mac Síthigh, "The Data Retention Directive Never Existed", 11 (1) SCRIPTed (April 2014)

71 This is because the EU Data Protection Directive (95/46/EC) contains in its article 13 a list of justifications for which the States can adopt legislative measures to restrict the obligations of data processors, provided that such a restriction constitutes a necessary measure to safeguard:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

72 Prior to the invalidation of the Directive by the ECJ, the provisions laid down for its national implementation had been repealed in Germany, Romania, Bulgaria, Cyprus and Czech Republic. For a detailed account of the several decisions of invalidation, see E. Kosta, "The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Right to Privacy and Data Protection", 10 (3) SCRIPTed 2013; J. Durica, "Directive on the Retention of Data on Electronic Communications in the Rulings of the Constitutional Courts of EU Member States and Efforts For Its Renewed Implementation", 3 (2) International Journal for Legal Research (2013).

73 at 58.

74 At 59.

75 At 60-61.

76 At 92.

77 See for instance "Google Alert": http://www.google.com/alerts.

78 See Federal Constitutional Court, Mar 11,2008, 1 BvR 256/08 (F.R.G.).

79 See G. Frosio, Urban Guerrilla & Piracy Surveillance, Rutgers Computer & Technology Law Journal vol. 37 [2011], 27

80 Federal Constitutional Court, decision of 19.04.2012 (I ZB 80 /11)

81 Court of First Instance of Rome, 14 July 2007, n. 1187, AIDA 2007, 1049.

82 In particular: (1) it must be likely that the user acted unlawfully towards the applicant; (2) the applicant must have a real interest in obtaining the name and address of the user; (3) there may be no less intrusive means of tracing the data than through the ISP; and (4) in light of a balancing of the interests involved, those of the applicant must prevail. See *Lycos/Pessers*, HR (Supreme Court), November 25, 2005 [2006] NJ 9.

83 See ECJ judgment of 19 April 2012, case C−461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB* (paraphrasing Swedish legislation, in particular articles 53c and 53d of the Law on Copyright)

84 More specifically: (1) the respective strength of the case; (2) the relationship between the alleged wrongdoer and the respondent; (3) the possibility to obtain the information from another source and (4) whether the disclosure order would put the respondent into trouble which could not be compensated by the payment of all expenses. See *Norwich Pharmacal v. Customs and Excise* [1974] A.C. 133 HL, at 199

85 See for example the order by the Court of First Instance in Paris on 24 January 2013, where the Court interpreted the provision of article 6.7. of the "Law of 21 June 2004 for trust in the digital economy" (prohibiting public insults of racial character, that incite to discrimination, hate or violence for national, racial or religious grounds and to racial defamation) in combination with article 145 of the code of civil procedure (allowing, where there is a legitimate reason for the conservation or the collection of evidence before trial, the ordering of preliminary measures) to justify an order requiring Twitter to disclose the identity of 5 alleged infringers: see Tribunal De Grande Instance de Paris, Ordonnance de Référé 24/01/ 2013, *Union des Etudiants Juifs de France* and *J'accuse!...Action International Pour la Justicev. Twitter Inc.* and *Twitter France*, N. RG: 13/50262, 13/50276.

86 See I. Romet & P. Veron, "On the Way to French Balance, the French Approach for Patent Litigation", Who's Who legal (May 2011).

87 *Google Spain SL v. Agencia Española de Protección de Datos* (AEPD), Case C−131/12 (E.C.R. May 13, 2014).

88 These presumptions could simply replicate the conditions set forth by the case-law. In the US, for example, the US District Court for the DC Circuit held that anonymity should only protect those who fear retaliation or an unwanted intrusion of privacy, and not users of a peer to peer network who exchange song files. See *In re Verizon Internet Services, Inc.*, 257 F. Supp. 2d 244, 259 (D.D.C. 2003). This holding is consistent with the view taken by other courts, in ruling that peer to peer file-sharing "qualifies as speech, but only to a degree". See *Sony Music Entertainment v Does* 1-40, 326 F.Supp. 2nd 556 (S.D.N.Y., 2004).