FREEDOM OF EXPRESSION ONLINE: THE REDEFINED ROLE OF SOCIAL NETWORKS

Matija Damjan[1]

https://doi.org/10.24040/pros.07.05.2021.ssp.47-59

Abstract

The EU's general information policy of the internet has been defined through intermediary liability rules of the E-Commerce Directive of 2000. These are not well adapted to the current online environment where social networks have become the main channels of public debate online. Social networks benefit from publishing offensive users' content that generates clicks and are disinclined to remove it. Yet, they are free to arbitrarily remove or censor any content, regardless of its illegality. The paper discusses the rebalancing of rights and responsibilities of social networks under the new Copyright Directive and the draft Digital Services Act.

Keywords

Social networks, intermediary liability, freedom of expression, digital services, notice-and-takedown

Introduction

Social networks, particularly Twitter and Facebook, have become important channels of public communication, enabling celebrities, politicians, businesses, etc. to directly address their fans, voters, or customers, but also allowing ordinary individuals to express their opinions and engage in public discussions online. Hence, they play a vital role in exercising the freedom of expression and information guaranteed, *inter alia*, in Article 10 of the European Convention on Human Rights and Article 11 of the Charter of Fundamental Rights of the European Union. Yet not all forms of online expression are protected and there is a legitimate public interest for constraining hate speech, defamatory allegations, violations of IP rights and personal data, and other forms of illegal information. Social networks have proven to be quite suboptimal forums for open and democratic public debate. On one hand, their business model benefits from any content that attracts wide public attention and generates

[1] Assistant professor at the Faculty of Law, University of Ljubljana, and secretary general of the Institute for Comparative Law at the Faculty of Law in Ljubljana. The research was supported by the Slovenian Research Agency under the research programme P5-0337 „Legal challenges of the information society".

clicks, thus discouraging the operators from removing any offensive users' uploads until expressly required to do so. On the other hand, social networks are free to arbitrarily remove or censor any content they wish, regardless of its illegality, and without allowing the uploaders to prove that the removal is unjustified. No effective legal remedies exist to protect free speech on social networks. This makes social networks quite inefficient and unfair platforms for free online communication, often generating hate speech rather than promoting free exchange of ideas.

Thus far, the European Union's general information policy of the internet has been largely defined through intermediary liability rules. The E-Commerce Directive[2] of 2000 has introduced a safe haven for hosting providers, who can escape liability for illegal content posted by their users by complying with the notice-and-takedown system, which shifts the burden of discovery and notification on the affected parties. This system also applies to social networks, although they are hosting providers merely in technical terms, but are in fact in the business of harvesting their users' data and marketing it to advertisers. However, the EU is currently in the process of creating new rules more specifically tailored to the characteristics of social networks. The 2019 Directive on Copyright in the Digital Single Market introduced more stringent copyright liability rules for "online content-sharing service providers" and the draft Digital Services Act, currently proposed by the European Commission, would require "very large online platforms" to take a more active role in preventing the dissemination of illegal content and societal harms. This paper will outline the proposed solutions and evaluate the rebalancing of the rights and responsibilities of social networks and their users.

Intermediary liability rules under the E-Commerce Directive

Internet intermediaries act as gatekeepers who control the access to any kind of online information that is available through their services, so they could in principle be held liable whenever such information is unlawful. However, the European Union legislation adopted in the early 2000's protected the emerging IT industry from excessive legal risks that could be associated with such a wide liability.[3] As a general principle, the E-Commerce Directive

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17. 7. 2000, p. 1–16.
[3] Rowland, Kohl, Charlesworth, p. 73; Spindler, p. 3–4.

prohibited Member States from imposing on internet intermediaries any general obligation to monitor their users' activities and prevent them from posting illegal content. Of course, this prohibition is also important to protect the internet users' privacy and business confidentiality.[4] It does not, however, prevent national authorities from imposing monitoring obligations in specific cases.[5]

The E-Commerce Directive established a single liability regime for all types of unlawful online content. It is based on a compromise under which internet intermediaries are not responsible for illegal content in return for being constructive in removing illegal content at the request of the affected third parties (rightsholders).[6] The Directive distinguishes between three types of intermediary activities based on the role that the intermediary plays in the online communication chain: mere conduit, caching and hosting.[7] Mere conduit and caching of information are technical services can be compared to the services of telephone companies or the post office.[8] Therefore, the E-Commerce Directive shields the conduit and caching providers from liability as long as they provide their service in a technically neutral manner without interfering with the information that is transmitted or cached.

The activity of hosting consists of the storage of information provided by the user of the service and, typically, making this information available to third parties. This clearly also covers the services of social networks. The hosted information can be controlled by both the user and the service provider, but hosting providers generally restrict themselves to the administration of server infrastructure. Nevertheless, due to the longer duration of hosting, the hosting provider has a greater role in the publishing process and firmer control over the users' information than other intermediaries.[9] Under the E-Commerce Directive, a hosting service provider is not liable for the information stored at the user's request if the provider does not have actual knowledge of illegal activity or information and is not aware of facts or circumstances from which the illegal activity or information is apparent.[10] As soon as a hosting provider learns of illegal activity or information or of the facts or circumstances from which the illegality might be apparent, they must act expeditiously to remove the unlawful

[4] Harper, p. 31.
[5] Recital 47 of the E-Commerce Directive.
[6] Harper, p. 30–33, Edwards, p. 59–61.
[7] Rowland, Kohl, Charlesworth, p. 71.
[8] Idem, p. 75.
[9] Edwards, p. 65.
[10] The absence of actual knowledge of illegal activity or information suffices to avoid criminal liability, whereas the conditions to avoid civil liability are somewhat stricter. Edwards, p. 65.

content or disable access to it. This system is referred to as the "notice-and-takedown" system, since the hosting providers are not required to search for illegal content posted on their online platforms, but must promptly remove or block such content when they are notified of the infringement by the affected party.[11] In recital 48, the Directive allows Member States to require hosting service providers to apply duties of care, which can reasonably be expected from them in order to detect and prevent certain types of illegal activities.[12]

The E-Commerce Directive requires service providers to *act expeditiously* upon receiving a takedown notice to remove or to disable access to the illegal information but does not define whether expeditiously means immediately after receiving the takedown notice or whether the service provider may take time to examine the illegality of the content at stake before deciding on its removal. Quick action is necessary to ensure effective protection of the affected parties' rights. On the other hand, immediate removal upon receiving any takedown request would allow the abuse of such requests to get rid of any unwanted online information regardless of its illegality. A very short deadline for the takedown can also present a practical problem for smaller service providers who do not have appropriate staff ready at all times. Recital 46 of the Directive stresses states that the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level. Therefore, the length of time reasonably necessary to take such action should be judged by taking into account the circumstances of each case.[13]

A court or administrative authority can also order the service provider to terminate or prevent an infringement for reasons such as crime detection and prevention, the protection of privacy, of classified information and of trade secrets. In case *Glawischnig-Piesczek,*[14] the Court of Justice of the EU (CJEU) held that an injunction can compel the provider to remove or block such content worldwide and that it may be formulated so as to include the removal or blocking of content identical or equivalent to the content previously declared unlawful.

[11] Rowland, Kohl, Charlesworth, p. 85.
[12] Mazziotti, p. 168.
[13] Edwards, p. 66–67.
[14] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, ECLI:EU:C:2019:821.

Exemptions from liability in CJEU's case law

The exemptions from liability established in the E-Commerce Directive cover only cases where the intermediary activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.[15] This was typical of hosting services at the time of the adoption of the Directive. Today's social networks and other interactive online platforms, however, encourage users to publish and share their content to generate web traffic and increase advertising revenue. Providing access to user-generated content is the crucial element of any social network's business model.[16] Since a portion of user-generated content will always be illegal, the question arises whether the provider of such service could always be deemed to have been aware of the illegality and thus required to act.[17]

The CJEU's case law interpreting the E-Commerce Directive has been generally favourable for the service providers. In the case *Google France v. Louis Vuitton* (AdWords),[18] the Court held that Google could only be held liable for violations of Louis Vuitton's trade marks in its paid referencing service 'AdWords' if it actively cooperated with advertisers in the creation of the content of their ads. Since Google had set up an automated process for the selection of keywords and the creation of ads, the service provider retained its technically neutral role and was able to avoid the liability.[19] This view was confirmed in *L'Oréal v. eBay*[20] in relation to the operator of on online marketplace through which users were selling counterfeit goods. CJEU held that eBay could not be denied the possibility of invoking liability exemptions merely because it stored sales offers on its servers, set out the terms of its service, received payment for it, and provided general information to customers. However, the exception cannot be invoked by a service provider who is aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality and acted accordingly. The Court did not specify what activities the duty of care entails since these depend on the circumstances of each case.

The E-Commerce Directive prohibits general monitoring obligations but allows the Member States' courts or administrative authorities to impose limited monitoring obligations

[15] Recital 42 of the E-Commerce Directive.
[16] George, Scerri, p. 3–5; Murray, p. 107–110; Rowland, Kohl, Charlesworth, p. 89.
[17] Edwards, p. 67.
[18] Case C-236/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, ECLI:EU:C:2010:159.
[19] Rowland, Kohl, Charlesworth, p. 88
[20] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others*, ECLI:EU:C:2011:474.

in specific cases. However, the CJEU has held in cases *Scarlet Extended*,[21] *Sabam v Netlog*[22] and *UPC Telekabel*[23] that an injunction may not compel internet intermediaries to establish a permanent system of preventive filtering of user data to protect themselves from civil liability. The requirement of the intermediary's actual knowledge or awareness of the unlawful information does not include the knowledge that could only be obtained through monitoring of the hosted contents.[24]

Dealing with baseless takedown requests

The E-Commerce Directive does not specify the form and content of the takedown request that obliges the hosting provider to remove the unlawful information. It is not clear, for example, whether a phone call or a text message are sufficient and whether the service provider must also act upon receiving an anonymous notice. Clearly, the notice should specify the illegal content whose removal is requested and probably specify the rights that have been violated by the publication of the content. It is also not clear to what extent or by what means the service provider may assess the merits of the takedown request. Requiring the service provider to act upon each takedown request regardless of its form and merits would facilitate the abuse of the notice-and-takedown system to remove any unwanted online content, regardless of its legality. Such private censorship would take place without involvement of the courts.[25] According to some reports, at least one third of the takedown requests received by service providers are unfounded in practice.[26] Several studies have shown that service providers often automatically block disputed content after receiving a takedown request, without verifying the accuracy of the claims, even when they are manifestly unjustified (e.g. because the copyright has long since expired).[27]

Recital 46 of the E-Commerce Directive allows Member States to prescribe the conditions and procedures which both the party requesting the removal of online content and

[21] Case C-70/10 *Scarlet Extended SA v SABAM*, ECLI:EU:C:2011:771.
[22] Case C-360/10 *SABAM v Netlog*, ECLI:EU:C:2012:85.
[23] Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192.
[24] Rowland, Kohl, Charlesworth, p. 87.
[25] Rowland, Kohl, Charlesworth, p. 86.
[26] Urban, Quilter, p. 666.
[27] See Lumen research project of the Berkman Klein Center for Internet & Society at Harvard University, which has created a database containing millions of takedown notices. URL: https://lumendatabase.org.

the hosting service provider must follow. Yet, Member States have generally not legislated to provide any additional procedural safeguards in the notice-and-takedown mechanism, such as requiring the written form of the notice, the signature of the rightsholder, contact information of the complainant and a clear identification of the infringing material. In the absence of explicit regulation, such conditions could be adopted by service providers themselves through self-regulation. It can be argued that the service providers should avoid liability if they refuse to block or remove infringing content when the complaining party failed to follow the service provider's reasonable procedural requirements.

This view is supported by the CJEU's statement in *L'Oréal v. eBay* that an intermediary may escape liability where the notifications of allegedly illegal activities or information turn out to be insufficiently precise or inadequately substantiated to enable a diligent economic operator to identify the illegality. Therefore, the European Commission's 2017 Communication on Tackling Illegal Content Online[28] recommends that online platforms should put in place effective mechanisms to facilitate the submission of notices that are sufficiently precise and adequately substantiated to enable the platforms to take a swift and informed decision about the follow-up. This should facilitate the provision of notices that contain an explanation of the reasons why the notice provider considers the content illegal and a clear indication of the location of the potentially illegal content (e.g. the URL address). Users should normally not be obliged to identify themselves when reporting what they consider illegal content, unless this information is required to determine the legality of the content (e.g., asserting ownership for intellectual property rights).

New liability rules for copyright violations

The emergence of social networks and other interactive online platforms has blurred the distinction between hosting service providers and content providers. Social networks such as Facebook, Instagram, Twitter or YouTube have been generating tremendous advertising revenue from the content uploaded by the users of their services whilst still benefiting from the safe haven provisions of the E-Commerce Directive.[29] Since a substantial share of all content uploaded on social networks infringes upon copyright or related rights, the issue of

[28] Communication COM(2017) 555 final, Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms, Brussels, 28. 9. 2017.
[29] George, Scerri, p. 3–5; Murray, p. 107–110.

specific treatment of social networks was first addressed in the 2019 Directive on Copyright in the Digital Single Market.[30]

A new category of internet intermediaries was introduced: online content-sharing service providers, defined as providers of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by the users, which the service provider organises and promotes for profit-making purposes. The description fits the social networks perfectly and expressly excludes non-profit online encyclopaedias (e.g. Wikipedia), non-profit educational and scientific repositories, open source software development and sharing platforms (e.g. SourceForge and GitHub), electronic communications service providers, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use. The provisions have been carefully drafted to cover only the established social networks; thus, newly established content-sharing service providers whose services have been available to the public for less than three years and whose annual turnover is less than € 10 million are partly exempt from the new liability rules.

When such a service provider gives the public access to copyrighted works uploaded by its users, this now qualifies an act of communication to the public of these works by the service provider itself. The service provider needs permission from the rightsholders for such use, e.g. through a licence agreement with a collecting society. Without proper authorisation, content-sharing platforms can be held liable for copyright infringements committed by their users.[31] This means that, as far as copyright violations are concerned, the liability rules have been reversed for online content-sharing service providers. However, they can still avoid liability if they can demonstrate that they have made best efforts to obtain an authorisation and to ensure the unavailability of the works for which the rightsholders have provided the relevant and necessary information; and that they have acted expeditiously to block or remove the notified works and to prevent their future uploads.[32]

The prohibition of general monitoring obligations still applies, but it is hardly conceivable how the removal of all copyright infringing content from social networks and the

[30] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p. 92–125.
[31] Critics have been pointing out that online platforms will not be able to obtain licenses for all users' content, as collecting societies do not represent all copyrighted works distributed on the internet. Hence, a lot of copyright-protected content will have be taken offline. Spindler, p. 13.
[32] Spindler, p. 13.

prevention of its future uploads could be achieved otherwise than by using automated filtering tools.[33] These could be a step towards private censorship of user content.[34] The issue is expected to be resolved through high industry standards of professional diligence, which are to be defined in consultation with all relevant stakeholders. The standards will need strike a balance between fundamental rights, particularly the freedom of expression and the freedom of the arts, and the right to property, including intellectual property.[35]

Overhaul of liability rules under the draft Digital Services Act

In December 2020, the European Commission introduced a proposal for a Digital Services Act[36] that would rewrite the existing rules on the liability of internet intermediaries. Under the draft proposal, the E-Commerce Directive would be replaced by a regulation encompassing a single set of rules applicable across the whole EU without relying on the Member States' implementation. The proposal retains almost literally the existing safe haven provisions based on the distinction between mere conduit, caching and hosting, but supplements them with additional rules concerning some of the issues that have been left unresolved under the E-Commerce Directive.

Notably, the notice-and-takedown system (now referred to as notice-and-action mechanism) is regulated in more detail. Hosting providers must make sure that the mechanism is easy to access, user-friendly, and allows for the submission of notices by electronic means. Takedown notices will have to be sufficiently precise and adequately substantiated so that a diligent economic operator can identify on their basis the illegality of the content in question. This confirms that the hosting service provider is allowed to assess the merits of the request and, presumably, that it can take a reasonable time to do so. The notice will have to contain:

a) an explanation of the reasons why the information in question is to be considered illegal;
b) a clear indication of the electronic location of that information (URL);

[33] Idem, p. 16.
[34] Institut Suisse de Droit Comparé, p. 17–22.
[35] Cf. Spindler, p. 14.
[36] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final, Brussels, 15. 12. 2020.

c) the name and an electronic mail address of the submitter of the notice;
d) a statement confirming the good faith belief of the submitter that the information and allegations contained therein are accurate and complete.

The express requirements that the person requesting the removal of certain online content substantiates this request is to be welcomed since it should hinder frivolous submitting of clearly unfounded takedown notices in bad faith. The position of the uploader of the content in question is additionally protected by the requirement that the hosting provider, after deciding to remove or disable access to specific user's content, must inform that user of the decision and provide a clear and specific statement of reasons for it. The user should also be informed of any means of redress available, so that they are better placed to protect their rights, including the freedom of expression.

New requirements for (very large) online platforms

The draft Digital Services Act furthermore introduces two new categories of hosting services for which additional requirements apply before their providers can rely on exemptions from liability. These are online platforms and very large online platforms.

Online platforms are defined as hosting services which, at the users' request, store and disseminate information to the public (such as online marketplaces, app stores, collaborative economy platforms and social media platforms). Online platforms will be required to set up an internal complaint-handling system allowing the users of their services to complain, electronically and free of charge, against the platform's decision to remove or disable access to that user's content, to suspend or terminate the provision of the service to the user or to suspend or terminate the user's account. The complaints will need to be handled by humans, rather than relying fully on automated means. Additionally, the users will have the option to turn to any out-of-court dispute settlement body certified by the Digital Services Coordinator of the Member State to review the decisions of the internal complaint-handling mechanism.

However, online platforms will no longer be able to shift the whole burden of identifying illegal content to the persons whose rights are affected through the public availability of such information. Rather than opening the doors for the very contentious upload filters, the draft new rules require online platforms to rely on trusted flaggers, i.e.

independent expert entities that review content available on the platforms and report any illegal content. Trusted flaggers are already used in practice by the major social networks,[37] so the mechanism will not be a novelty, but the status of trusted flaggers will now be awarded by the Digital Services Coordinator of the Member State rather than the platforms themselves. Any takedown notices received from trusted flaggers will have to be processed and decided upon by the platform operator with priority and without delay.

Furthermore, the draft Regulation introduces important new measures against the misuse of online platforms‘ services. The platforms will be allowed and legally required to suspend for a reasonable time, after a prior warning:

a) the users of their service that frequently provide manifestly illegal content, and
b) the individuals or entities who frequently submit takedown notices or complaints that are manifestly unfounded.

The second new category of hosting services are very large online platforms, defined as online platforms that reach at least 45 million average monthly active users (10% of the EU's population). Clearly, what is aimed at with this term are the largest global social networks, since these present particular risks in the dissemination of illegal content and societal harms.[38] Apart from complying with the general requirements for hosting providers and for online platforms, very large online platforms will be required to perform an annual assessment of any significant systemic risks stemming from the functioning and use of their services. The assesment will need to include the risk of the dissemination of illegal content through their services; any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child; and the risk of intentional manipulation of their service for spreading fake news that might be harmful to public policy aims such as public health, minors, civic discourse, electoral processes and public security. Such risks may arise, for example, through the creation of fake accounts, the use of bots, and other automated or partially automated behaviours, which may lead to the rapid and widespread dissemination of information that is illegal content or incompatible with an online platform’s terms and conditions.[39]

[37] Communication COM(2017) 555 final, Tackling Illegal Content Online, point 6.
[38] Recitals 54-57 of the proposed Digital Services Act.
[39] Recital 57 of the Draft Digital Services Act.

Following the risk assessment, very large online platforms will have to put in place reasonable, proportionate and effective mitigation measures to address the specific systemic risks identified, such as content moderation or recommender system, limiting the display of advertisements or reinforcing the existing internal processes for the detection of systemic risks. Finally, very large online platforms will be subject, at their own expense and at least once a year, to independent audit to assess their compliance with the above requirements.

Conclusion

Social networks are starting to emerge as a special category of online intermediaries in the recent or nascent European Union legislation, which corresponds to their increasing role in the actual operation of the internet. Due to the social networks' importance in today's online communication, their global span, and the vast commercial benefits that their operators derive from these services it is appropriate that they should bear higher legislative requirements than "regular" internet intermediaries. To preserve the democratic function of the internet it is essential, however, that these requirements are not aimed only at removing illegal online content but also at protecting and facilitating free speech. For this reason, better defined notice-and-takedown procedures under the draft Digital Services Act are welcome, since they strike a balance between the interests of affected rightsholders and the users of hosting services. Hopefully, trusted flaggers, recommender systems and other proposed measures for social networks should be able to reduce the systemic risks of fake news, hate speech and the manipulations of social networks for political and similar purposes. In the end, however, the quality of online debate will always primarily depend on the conduct of the users themselves.

Bibliography

- EDWARDS, L.: The Fall and Rise of Intermediary Liability Online. In EDWARDS, L. – WAELDE, C. (eds.): Law and the Internet. Oxford: Hart Publishing, 2009. ISBN: 9781841138152. p. 47-88.

- GEORGE, C. – SCERRI, J.: Web 2.0 and User-Generated Content: legal challenges in the new frontier. In: Journal of Information, Law and Technology, vol. 2007, no. 2. ISSN: 1361-4169. URL: http://go.warwick.ac.uk/jilt/2007_2/george_scerri/.
- HARPER, J.: Against ISP Liability. Do ISPs have a duty to protect the world? In: Regulation, vol. 28, 2005, no. 1. ISSN: 0147-0590. p. 30-33.
- INSTITUT SUISSE DE DROIT COMPARÉ: Comparative Study on Blocking, Filtering and Takedown of Illegal Internet Content. Lausanne: Council of Europe, 2017. 34 p. URL: https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html.
- MAZZIOTTI, G.: EU Digital Copyright Law and the End-User: Berlin, Heidelberg: Springer, 2008. 374 p. ISBN: 978-3-540-75985-0.
- MURRAY, A.: Information Technology Law: The law and society. Oxford: Oxford University Press, 2010. 624 p. ISBN: 978-0199548422.
- PAPADOPOULOU, M.D. – MOUSTAKA, E.M,. Copyright and the Press Publishers Right on the Internet: Evolutions and Perspectives. In: SYNODINOU, T. et al. (eds.): EU Internet Law in the Digital Era: Regulation and Enforcement. Cham: Springer Nature, 2020. ISBN: 978-3-030-25579-4. p. 99-36.
- ROWLAND, D. – KOHL, U. – CHARLESWORTH, A.: Information technology law, 4th edition. London, New York: Routledge, 2012. 531 p. ISBN: 978-0-415-48227-1.
- SPINDLER, G.: Copyright Law and Internet Intermediaries Liability. In: SYNODINOU, T. et al. (eds.): EU Internet Law in the Digital Era: Regulation and Enforcement. Cham: Springer Nature, 2020. ISBN: 978-3-030-25579-4. p. 3-25.
- URBAN, J.M. – QUILTER, L.: Efficient Process or Chilling Effects – Takedown Notices under Section 512 of the Digital Millennium Copyright Act. Santa Clara High Technology Law Journal, vol. 22, 2006, no. 4. ISSN: 0882-3383. p. 621-693.