Cited as: Wang, F. (2012) Response to Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries, 2012, Issue 91 *Intellectual Property Forum* 93-98.

Current Developments – Europe

EUROPEAN UNION

Dr Faye Fangfei Wang
Senior Lecturer in Law

Brunel Law School, Brunel University, London, UK
Correspondent for the European Union

Response to Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries

Introduction

Online intermediaries play an important role in the information society, and as a result regulators have been taming the Internet through the use of online intermediaries.[1] There are a variety of forms of online intermediaries. Hosting service providers can be categorised as one type of online intermediaries. Giving a definition to the hosting service provider can be challenging as it is a relevant term. For example, the social network provider can be considered as the hosting service provider if that social network provider owns and runs its server consisting of "the storage of information provided".[2] If another service provider leases server capacity to the social network provider, that service provider which leases server capacity should be considered as the hosting service provider. Hosting service providers have been actively engaging in the "notice and takedown" practice regarding illegal online content. However, how far the responsibility and liability of hosting service providers should go remains a controversial issue.

The European Commission opened the Public Consultation on Procedures for Notifying and Acting on Illegal Content hosted by Online Intermediaries (the consultation) between 4 June 2012 and 5 September 2012 (and it was extended to 11 September 2012).[3] This consultation aims to collect opinions on how to develop a clean and open Internet by reviewing the provisions under Article 14 of the EC E-Commerce Directive; and is deemed to be another attempt in regulating the liability of online intermediaries after the publication of recent comments and reports on the enforcement of intellectual property (IP) rights (the application of the EC Directive on Intellectual Property Rights Enforcement),[4] and the public consultation on the future of e-commerce and the implementation of the E-commerce Directive.[5] The focal point of the consultation lies in questions on whether hosting service providers should have a procedure for notifying illegal content and what actions hosting service providers should take against illegal content.

This article responds to the consultation and provides commentaries on necessary measures to be considered for the establishment of "notice and action" procedures in the EU with some reference to current development in the United States (US) regarding IP rights, defamation and data privacy infringement.

Notice and Action Procedures in Europe

Notice-and-action (N&A) procedures in this consultation are also known as "notice and takedown" procedures (NTD) in other countries such as the UK and HK. Some other European official documents also use the wording – "notice and takedown", which can be found in the European reports and comments on e-commerce and IP rights enforcement.

The N&A procedures are also called "takedown procedures" or "takedown notice" in the *Digital Millennium Copyright Act* in the US.[6] The NTD procedures are commonly understood as: starting whenever someone notifies a hosting service about illegal content on the Internet and concluding when an online intermediary takes down (i.e. blocking or deleting) the alleged illegal content."[7] The NTD procedures are deemed to be "indispensable measures in the fight against the sale of Counterfeit Goods over Internet Platforms".[8] It was also popularly used to fight again other IP rights infringement, defamatory content, terrorism related content, illegal online gambling, child abuse content, misleading advertisements or incitement to hatred or violence on the basis of race, origin, religion, gender, sexual orientation etc.[9] In other words, the NTD procedures have been horizontally applied across a variety of legal subject matters.

However, such horizontal application has been implemented at various levels in different countries. In addition, each country has developed this mechanism with different strength. For example, in the US there is debate over how to enhance fairness under such procedures. In the case of *Lenz v. Universal Music Corp.*,[10] the Court introduced the fair use analysis under the takedown procedures in order to ensure the critical balance between a copyright owner's monopoly and the rights of the public.[11] That is, the copyright owner is required to conduct a fair use evaluation prior to issuing a takedown notice.

In the EU, there is debate over how to improve effectiveness under such procedures, for example, the "without undue delay" principle for data breach notification is introduced in the EC E-Privacy Directive.[12] The Proposal of General Data Protection Regulation further enhances

this principle by inserting Article 12(2) that "the controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken". Recital (67) / Article 31 of the Proposal of General Data Protection furthers the requirement that "the controller should notify the breach to the supervisory authority without undue delay and where feasible, within 24 hours. Where this cannot be achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification".[13] That is, a timescale for the "notice and takedown" procedures has been considered as a crucial measure to improve and enhance the effectiveness (and even fairness) of such procedures.

Despite the continuous development of the NTD procedures in the EU, member states are still facing one major challenging issue, that is, the consistent or harmonised interpretation of the "notice and takedown" procedures under the EU legislation such as the EC E-commerce Directive (2000/31/EC), EC e-Privacy Directive (2009/136/EC), EC Directive on IP Rights Enforcement (2004/48/EC), EC Information Society Directive (2001/29/EC) etc. Among all the cornerstone of the legislation regarding the "notice and takedown" procedures on the Internet is Article 14 of the EC E-commerce Directive. It provides that:

> *Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:*
>
> *(a) the provider does not have* ***actual knowledge*** *of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*
>
> *(b) the provider,* ***upon obtaining*** *such knowledge or awareness,* ***acts expeditiously*** *to* ***remove*** *or to* ***disable*** *access to the information.*[14]

This defines the core factors for the determination of a hosting service provider's liability – "actual knowledge", "actions (remove/disable)" and "manners (expeditiously)". The wording of this provision is exactly the same as the relevant provision in the US *Copyright Act*,[15] though the EC E-Commerce Directive is applicable to a wider scope of subject matters, known as a horizontal approach, as discussed earlier. The meaning of the three core factors is rather disputable in practice and there is need for further clarification to avoid legal fragmentation and uncertainty for hosting service providers. It places reliance on standardising two components: the content of notification (formality and details of information) and the action against illegal content in response to notification.

Notification of Illegal Content

Hosting service providers may acquire "actual knowledge" and "awareness" of illegal activity or information upon the receipt of notification of illegal content. A notification of illegal content is usually required to be in a prescribed format to make the hosting service provider aware of alleged illegal content. In the EU, the Court of Justice of the European Union in the recent case of *L'Oréal and Others v eBay* ruled that if notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, hosting service providers may not be able to identify the illegality and take actions expeditiously to remove or disable access.[16] In the US, in *Hendrickson v eBay Inc.*, it was held that it was inadequate to simply provide eBay with the movie's title without specifying the eBay item numbers' listings.[17] In other words, information regarding the alleged illegal content should be sufficiently precise and adequate substantiated for hosting service providers to gain "actual knowledge" and "awareness" of illegal activities.

To enhance this, in practice, some hosting service providers have voluntarily put in place technical mechanisms/systems for the "notice and takedown" process. For example, it is notable that eBay has developed a NTD system called "VeRO" (Verified Rights Owner) – a filter program – that is intended to provide IP owners with assistance in removing infringing listings from the marketplace. It requires that the complainant fill out the standard Notice of Infringement form specifying the allegedly infringing listings and infringed works and completing with an original authorised signature, and fax it to eBay.[18]

Amazon has also introduced their self-regulated "notice and takedown" procedures to deal with rights infringements. Different from eBay, Amazon sets up separate formats for different rights infringement such as "notice and procedure for notifying Amazon of defamatory content" and "notice and procedure for making claims of right infringements". The Complainant will need to send a printed and signed copy of defamatory content notice after filling in a downloadable form to Amazon.[19] Different from notification of defamatory content, the complainant is only required to fill in an online form regarding alleged infringements such as copyright and trademarks

concerns and click the "submit" button to complete the report infringement process.[20]

In the author's opinion, if hosting service providers impose exclusive offline notification methods such as fax and post, it may not appear to be user-friendly taking into account the common use and popularity of email and other electronic communications in the information society. As the consultation rightly pointed out, the EC Directive on Electronic Commerce has not addressed the requirements regarding the means of communication, format and content of notification, and although the Court of Justice of the European Union (CJEU) in *L'Oréal and Others v eBay* indicated that a notice should be sufficiently precise or adequately substantiated to have effect, the Court has not indicated the requirements of meeting such purpose.[21]

In the author's opinion, making the "notice and takedown" procedures as user-friendly as possible is of fundamental importance as this is one of the most effective ways to promote the usage of such system to protect users and other rights holders' rights and at the same time minimise the possibility of the avoidance of responsibilities by hosting service providers. Thus, ideally this principle should be made compulsory to hosting service providers by regulators. It is incontrovertible that having a fair procedure in place that users can easily notify of illegal content to hosting service providers will not only boost users' confidence in using online marketplaces but also help service providers gain a good reputation.

Accordingly, the possible interpretation of the requirements of "sufficiently precise or adequately substantiated" can be proposed as that: (a) a notice should be allowed to be submitted by electronic means; (b) a notice should contain details of the sender but hosting service providers must not disclose the sender's personal details to other parties without informed consent except for crime investigation authorities; (c) a notice should specify the precise location and details of the alleged illegal content including but not limited to a URL, itemised number and detailed description of the alleged illegal nature of the content; and (d) a notice should be accepted by the hosting service provider regardless of whether the user can provide proof or evidence that the content provider (other rights' holder) could not be contacted or the content provider was contacted first but did not act, because acceptance to notification should be treated as a responsibility of hosting service providers to users so as to avoid diminishing the function of the NTD system.

Action against Illegal Content

In the EU, once the notified illegal content and its nature of infringement have been confirmed, the hosting service provider is expected to act "expeditiously" to remove or disable access to information according to the EC Directive on Electronic Commerce.[22] In the US, the responsible service provider is also required to respond "expeditiously" to a notice (e.g. copyright infringement).[23]

However, there is no clear definition of "expeditiously" and the specific actions required as to "remove or disable access". In practice, as the consultation indicated, some service providers may send the notice party a confirmation of receipt when they receive a notice and inform the notice party when the requested action has been taken.[24] This measure bears some similarity to that of the "without undue delay" principle for data breach notification discussed earlier.

For example, it was proposed that the controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken.[25] Likewise, the controller should also notify the breach to the supervisory authority without undue delay and where feasible, within 24 hours.[26] It is understood that regulatory explanation, taking into account judicial clarification, should be in place to enhance the consistent, efficient and harmonised actions against illegal content by hosting service providers. In the author's opinion, hosting service providers should be required to: (1) send a confirmation of receipt to the notice parties (i.e. the notice providers or rights' holders) when they receive a notice (by an automated email confirmation instantaneously or by other means within 24 hours); (2) consult the notice parties of alleged illegal content (for additional information and clarification) within 24 hours after the confirmation of receipt of the notice; (3) consult the users/clients (i.e the online content writer or information/content provider); concerning the allegation of content illegality (the so-called "counter-notice") within 24 hours simultaneously; and (4) inform both the notice parties and users/clients of any action that has been taken without undue delay depending on circumstances. This can be deemed as "a four-step approach" for the N&A procedure. It is unavoidable that there may be difficulties in implementing this four-step approach due to various expectations such as efficiency, fairness and appropriateness.

The debate is likely to fall into two areas: one is the area regarding the adoption of the counter-notice

system and the other is the area concerning the appropriate actions (i.e. remove or disable access) and the timeframe of such actions by the hosting service provider.

In the author's view, the counter-notice system should be recommended for the reasons that: first, lawsuits take a long time and the results may not be desirable in an online defamation case;[27] and secondly, users' rights are as important as other rights holders' rights (i.e. copyright holders' rights). Taking into account the balance that needs to be made, the counter-notice system has been introduced in many countries such as Finland, Lithuania, Poland, Germany and US.[28] The counter-notice system allows counter parties to dispute or deny the infringement alleged by the complainant and request online intermediaries reinstating the material or ceasing disabling access to the material or activity.

For example, in the US, if the complainant does not inform the service provider that he/she has filed an action seeking for a court action after 10 to 14 days upon the receipt of a counter notification, the service provider may reinstate the alleged materials.[29] Such measure has also been considered in other countries, for instance, Hong Kong also intends to introduce the counter-notice system in its Copyright (Amendment) Bill 2011.[30] Due to the conflicting interests between various parties and the public, having a counter-notice system in place will not only balance the rights between the users and other rights' holders but also best prevent unjustified notifications.

With regard to the issue concerning the appropriate actions (i.e. remove or disable access) and the timeframe of such actions, it is even more complex as it is intertwined with other issues horizontally such as criminal investigations from law enforcement authorities and diverse regulatory requirements of data privacy protection, IP rights enforcement, defamation defamatory content, online gambling, consumer protection and others.

Moreover, the appropriate actions and timeframe should be clearly considered at each stage of communications throughout the four-step process. For example, in the US, the safe harbour provisions do not require the service provider to notify the user/client for the allegedly infringing material before it has been removed, but the service provider must promptly notify the user/client after the material is removed and the user/client can then decide on its actions (i.e. giving a counter-notice and/or filing a lawsuit).[31] In the EU, the practice is similar to that in the US. As a result, the hosting service provider will take down the content immediately after receiving a notice and will only be obliged to put it back online after receiving a counter-notice.[32]

However, such measure leaves the hosting service provider with the responsibility to assess the legitimacy of the alleged information, content or statement. So when the judgment goes wrong, the hosting service provider may disable or take down legal content. If the rights' holder (the notice provider) takes a step further and files a lawsuit against the user/client, the alleged materials will remain disabled, blocked or removed at least until the court makes the final decision.

The speed of taking down the alleged materials (either legal content or illegal content) may cause various effects. In other words, at which stage the hosting service provider is required to disable or remove access is going to affect speed and as a consequence cause different effects. This is going to be an on-going debate from an economic perspective, because Internet users may suffer from lost benefits or profits and even economic damages as a result of the alleged materials being wrongly taken down, and so do the rights' holder, who can make the exact argument.

From a social security perspective, certain type of damages can be magnified or escalate out of control if the hosting service provider does not take action to disable or remove it immediately, i.e. in the situation of live video streaming or national security threat subject matters. Nevertheless, from a general human rights perspective, both users and rights' holders should be given an equal opportunity to express their views on the alleged infringing materials before the materials are permanently taken down, provided that the alleged materials do not pose an immediate threat to the social security and public interest. This leads to the next controversial issue concerning the appropriate actions on whether the hosting service provider should disable access in the first instance without permanently removing, taking down or deleting the content.

First, certain rights (such as IP rights) are protected within the territory where such rights are registered. Permanently removing the content may hamper the users' rights to use the content in another jurisdiction. Secondly, certain concepts such as privacy and defamation are related to culture and democracy respectively, which the hosting service provider may not be in a position to make the judgment in terms of the legitimacy of the content. Thirdly, removing the alleged illegal materials may prevent law enforcement authorities to further analyse them and investigating crimes when

necessary. Finally, the hosting service provider should be technically in a position to remove exclusively the notified illegal content when several providers host the same content on a particular website.[33]

It was also notable that removing materials from a search engine does not necessarily remove them from the Internet, which may cause further complication and difficulty to locate the alleged materials afterwards for the purpose of criminal investigations.[34] After all, the N&A procedure should be realistic on the issue as to whether the hosting service provider has the capability to take the responsibility to assess the legitimacy of the alleged information, content or statements. In order to ensure the fairness and security, the hosting service provider should be obliged to notify the competent authorities without undue delay when there is any doubt on whether the alleged information, content and statements may constitute a severe breach of the social security and public interest. In any event, suspicious alleged illegal materials should be disabled in the first instance when the hosting service provider receives a notice, though the system may be abused by the notice provider when the underlying purpose of such notice is to prevent others from using lawful materials to gain dominant position or other benefits. It is understood that this can be protected by imposing sanctions for such abuse.

Conclusion

After all, the use of the wording – the "notice and action" procedures (the N&A procedures) in the consultation instead of the "notice and takedown" procedures (the NTD procedures) may be well justified in the sense that the "notice and takedown" procedures not only comprise "notice" and "takedown" actions but also involve other actions such as counter-notice, evaluation and other remedies as discussed above, though NTD (notice and takedown) has become an universal common name for such procedures.

What the N&A procedures should be depends on what the purposes of having such procedures in place are. It is known that the original purposes of the NTD procedures are debatable and such purposes should be now justified before the regulatory design. The intended role of hosting service providers (such as gatekeepers, guardians or even mediators and the like) will inevitably reflect on the scope of their responsibility and liability.

Whichever role regulators may decide on for hosting service providers, due process and fair use (fairness) should be considered as the two fundamental principles for the N&A procedure for the reasons that: (1) from the users' perspective, the adoption of such procedures may be for the creation of chilling effects and to suppress the freedom of expression or communications; and (2) from the Internet service providers' perspective, the deployment of such procedures is to exempt from the liability of hosting illegal content. However, according to the issues raised in the consultation, it appears that the system of the N&A procedures may be progressed to serve as a protocol to strike a balance between protecting the users' and various rights holders' rights and promoting the role of Internet service providers in response to the rapid development of social networking and other forms of electronic communications.

1 Kohl, U. (2012), The Rise and Rise of Online Intermediaries in the Governance of the Internet and Beyond – Connectivity Intermediaries, Volume 26, Number 2-3, *International Review of Law, Computers & Technology*, pp.185-210, 185.

2 EC Directive on Electronic Commerce 2000, Article 14.

3 A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content hosted by Online Intermediaries, available at http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=noticeandaction (last visited on 1 September 2012).

4 Synthesis of the Comments on the Commission Report on the public consultation on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, European Commission, July 2011, available at http://ec.europa.eu/internal_market/consultations/docs/2011/intellectual_property_rights/summary_report_replies_consultation_en.pdf (last visited on 1 September 2012).

5 Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), European Commission, 2010, available at http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm (last visited on 1 September 2012).

6 Pallas, L. (2011), "Deterring Abuse of the Copyright Takedown Regime by Taking Misrepresentation Claims Seriously", 46 *Wake Forest Law Review* p.745 -782, 745.

7 See note 3.

8 Memorandum of Understanding on the sale of counterfeit goods over the internet (hereafter, "the MoU"), 4 May 2011, European Commission, Brussels, available at http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf (last visited on 1 September 2012), Article 11.

9 See note 3.

10 572 F. Supp. 2d 1150, United States District Court for the Northern District of California, 8 August 2008.

11 O'Donnell, K. (2009) "*Lenz v. Universal Music Corp.* and the Potential Effect of Fair Use Analysis under the Takedown Procedures of Section 512 of the DMCA" *Duke Law and Technology Review*, 2009, pp.1-12, 10.

12 Wang, F. (2011), "Personal Data Breach Notification System in the European Union: Interpretation of 'without undue delay'", Issue 6, *European Business Law Review*, pp.741-757, see general.

13 Proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Commission, Brussels, 25.1.2012 COM (2012) 11 final, 2012/0011 (COD).

14 EC Directive on Electronic Commerce, Article 14(1).

15 *Copyright Act* Title 17 USC (1976), see §512 in general.

16 Case C-324/09, *L'Oréal and Others v eBay*, Court of Justice of the European Union, Luxembourg, 12 July 2011, para. 122.

17 165 F Supp 2d 1082 (CD Cal 2001).

18 eBay VeRo Program information, available at http://pages.ebay.co.uk/vero/notice.html (last visited on 1 September 2012).

19 Notice and Procedure for Notifying Amazon of Defamatory Content, available at http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=1040616#defame (last visited on 1 September 2012).

20 Notice and Procedure for Making Claims of Right Infringements – Report Infringement, available at https://www.amazon.co.uk/gp/help/reports/infringement (last visited on 1 September 2012).

21 See note 3, p.10.

22 EC Directive on Electronic Commerce, Article 14(1).

23 *Copyright Act* Title 17 USC (1976), §512(b)(2)(E) and §512(c)(1)(c).

24 See note 3, p.13.

25 Proposal of General Data Protection Regulation 2012, Article 12(2).

26 Proposal of General Data Protection Regulation 2012, Recital (67) and Article 31.

27 *McGrath v Dawkins & Others* [2012] EWHC B3 (QB) (England, High Court, 30 March 2012).

28 Spindler, G. Riccio, G. M. and Perre, A.(2007), Study on the Liability of Internet Intermediaries (Markt/2006/09/E Service Contract ETD/2006/IM/E2/69), 12 November, available at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (last visited on 1 October 2012), p.16.

29 *Copyright Act* Title 17 U.S.C (1976), see §512(g)(2)(c).

30 Copyright (Amendment) Bill 2011, Section 88D, available at http://www.legco.gov.hk/yr10-11/english/bills/b201106033.pdf (last visited on 1 September 2012).

31 *Copyright Act* Title 17 U.S.C (1976), see §512(g)(2)(a) and Frequently Asked Questions (and Answers) about DMCA Safe Harbour, available at http://www.chillingeffects.org/dmca512/faq.cgi (last visited on 1 October 2012).

32 See note 28, p.16.

33 See note 3, p.15.

34 Urban, J and Quilter, L (2005-2006), "Efficient Process or Chilling effects – Takedown notices under Section 512 of the *Digital Millennium Copyright Act*", Volume 22, *Santa Clara Computer & High Technology Law Journal*, p.621-693, p.626.

FRANCE

Emmanuel Baud, Virginie Desmoulin and Sabine Rigaud[1]

Jones Day
France
Correspondents for France

Apple Infringes the French Trade Mark "Lion" (But Can Pursue Using It)

On 12 September 2012, the Paris Court of Appeal, ruling in emergency proceedings, rendered an interesting decision regarding the use of the denomination "LION" in relation to Apple's famous operating system "Mac OS X".

It should be remembered that, for more than 10 years, successive versions of Apple's operating system "Mac OS X" (or "OS X") have always been named after big cats: *Cheetah* in 2001, *Jaguar* in 2002, *Panther* in 2003, *Tiger* in 2004, *Leopard* and *Snow Leopard* in 2007 and 2009.

Circus, a French company, applied on 6 April 2010, for the French trade mark "LION", notably in class 9 in relation to "software in the field of visual creation, of post-production, of special effects for theatre movies, videos or other visual presentations".

In 2011, Apple elected to name the new version of its operating system "*LION*" and, on 6 April 2011, applied for the Community trade mark "LION", also in class 9 for "computer software; computer software for authoring, downloading, transmitting, receiving, editing, extracting, encoding, decoding, displaying, storing and organizing text, graphics, images, and electronic publications".

Despite the cease and desist letter sent to Apple by Circus, Apple started using the "LION" trade mark on its website and related software products. In July 2011, Circus initiated trade mark infringement summary proceedings against Apple before the Paris Court of First Instance.

In defence, Apple relied upon a prior semi-figurative "LION" trade mark (consisting in the term "LION" associated with a paw print, filed in class 9) acquired in September 2011, and further contended that Circus had fraudulently applied for its "LION" trade mark, arguing that Circus was aware such sign would one day be used in relation to a new version of the operating system Mac OS X.

On 12 September 2012, the Paris Court of Appeal ruled that Apple's acquisition of the prior "LION" trade mark was fraudulent, on the basis that "the acquisition of a mark, in the course of litigation, for the sole purpose of defeating an action for infringement, characterises a fraudulent response". This solution is consistent with French case law which tends to consider that the acquisition of a trademark after the launch of a lawsuit is particularly suspicious. Apple was further sentenced for trade mark infringement of Circus' French "LION" trade mark.

It is, however, noteworthy that the Judges elected not to prohibit Apple from using the "LION" denomination. In the Judges' opinion, "prohibition [to use the mark] would be disproportionate in comparison with the damages suffered by Circus". That stance is further justified by the Court of Appeal, which ruled that Circus has not, at this stage, launched any product under the Lion trade mark, and that Circus has not shown evidence that "the filing of an application for the "LION" trade mark resulted in any influence on consumers' decision to purchasing the new version of Apple