The with no one to blame and pay

Business, E-Commerce

THE SCHOOL OF SCIENCES CybercrimeConcepts and Legal ConsiderationsCSC460 ISP liability obligations in European UnionFALL 2017 StefanosVasilaras F20131723Christos Liatsos F20151678 SofianosFialogiannos F20151559ISP liability obligations in European Union INTROTACTION No one can deny the enormous effectthe internet had on the way we communicate now days. Thousand kilometers can bereduced to a single mouse click exchanging information, ideas and knowledgearound the planet in just a couple of seconds. But because of the way the digital networkenvironment is built, we rarely have connections between sender and receiverswithout the use of a range of providers to act as go-betweens for contentcreators and consumers.

Such go-betweens are hosting service providers, communications or network providers, and access providers who play a role asintermediaries by providing the venues for internet users to download, uploadpost or transfer such materials. Also we have the Internet Service Providers(ISP) who provide internet access services to their subscribers in exchange fora fee and other internet services like data storage on servers. One of the key futures of the Internetis the anonymity it can provide.

This is giving the necessary encouragementsome people need to engage in illegal acts through the Internet as stealingcopyright materials. At many cases because of the anonymity of the Internet, the ones who conduct illegal acts are undetectable leaving the copyright ownerswith no one to blame and pay for they loses. As a result ISPs are seen aspotential targets to be sued in order to compensate the damages of copyrightstealing. As a mean to defend themselves, ESPs got the ability to supervisewhether illegal data are being

transmitted over their network and stored ontheir servers. Regardless of that, ISPs are regularly dragged in the middle ofcourt battles since they are seen as liable by copyrights owners for their loses. On the other hand, some defend ISPs because according to them, they should notbe responsible for the actions of others. Furthermore asking the ISPs to trackeverything all their subscribers are transmitting is task almost impossible toaccomplish.

This debatable issue has been discussedover the years with no final solution ever been found. As a result, manycountries try to find a compromise between the copyright owners' interest andthe limitations of liability for ISPs. On this matter the European Union hasenacted the E-Commerce Directive (ECD) which contains provisions concerning theliability of intermediaries. Because of the ECD, ISPs have a shelter to beexcluded from being held liable in certain conditions. It is important to notethat the liability exemptions provided by the ECD apply in a horizontal manner. This means that they cover all types of liability, including civil, administrative and criminal liability.

The exemption regime also covers a widevariety of activities initiated by third parties: defamation, unfair commercialpractices, piracy, etc. Not all intermediary services can benefit from anexemption regime though. The ECD has introduced specific liability exemptionsfor three distinct types of intermediary services: mere conduit, cashing andhosting.

Mereconduit: Mere conduitexist in two sorts of types. The primary comprises of the transmission in acorrespondence system of data gave by a beneficiary of the administration, andthe second comprises of the " arrangement of access to a correspondenceorganize". The first type is applicable to the

demonstration of ISPs as mereconduits of materials that are given by outsiders, by enabling such materialsto be transmitted through their systems. The latter immunizes ISPs from beingheld liable for providing the internet network. Moreover, the transmission andarrangement of access said above incorporates the automatic, transientstockpiling of the data for instance of transmission.

That is, information istransmitted in a network by being carried from one computer to anothercomputer. Information then is temporally stored for a short period of time onany of these computers, and this temporal storage is also seen as transmission. Additionally, this transmission must occur for the sole motivation behindcompleting the transmission for the necessary needs, and the data must not be heldfor any period longer than the specific time frame that is sensibly importantfor the transmission. However, when ISPs meets the conditions that they just goabout as mere conduit, there will be no obligation for ISPs as long as theydon’t start the transmission themselves, don’t choose the receiver of thetransmission and don’t choose or alter the data contained in the transmission, aside from controlling the technical nature of the transmission to enable it tohappen on the first place. Caching: Cachingbuilds up a limitation of risk for ISPs in the case that the data is naturally, transitionally, and temporary put away in their systems for the sole motivationbehind making more proficient the data’s forward transmission to differentbeneficiaries of the administration upon their requests. Themotivation of caching is to diminish the repetitive high demand of specificmaterials by locating the high demand materials on remote servers, then storingaway duplicates of those materials on local servers.

Along these lines, itenables materials to deliver to clients who are looking for those materials inthe quickest path since the information has less distance to travel. In any case, ISPs are not at risk when they perform storing exercises under the conditionsthat:(1) Theydon’t alter the data, then they can’t be considered as intermediaries.(2) theyagree to conditions on access to the data, this condition is important becauseat some point a man who puts the data on the system applies certain conditionsto make get to accessible, such as payments of fees. ISPs must guarantee thataccess to cache copies that is permitted only in case users conform to get toprerequisites. (3) Theydon’t interfere with rules in regards, to the refreshing of data, indicated ina way broadly perceived and utilized by industry in manner. ISPs must enabledata to be refreshed, particularly because of data needing constant updates, for example, individual data, logical or financial data.

(4) Theydon’t interfere with the legitimate utilization of innovation, broadlyperceived and utilized by industry, to acquire information on the utilizationof the data.(5) Theyshould act quickly to remove or to disable access to the data put away on theirsystems after acquiring real learning that the initial source of thetransmission has been remove from the system, or access to it has been disable. Court administrative authority has ordered such removal or disability. Itimplies that ISPs must guarantee that the data they give is as exact as couldbe expected under the circumstances. Hosting: Hostingbuilds up a restriction of obligation for ISPs where they give storage room onweb servers to outsider clients.

In this manner facilitating characterizes theadministration that ISPs offer to people, organizations, and associations tolease space and consolidate any sort of information on the space. ISPs won't beheld subject for the outsider's data put away on their servers under theconditions that: (1) Theydon't have real learning of unlawful exercises or encroaching data of theirclients. (2) They maynot know about actualities or conditions from which the unlawful action or datais apparent, else they are obligated for claim and damages. As indicatedby those conditions, they are separated amongst civil and criminal liability. The first point, sets up a rule for criminal risk, implying that, ISPs won't beheld responsible under criminal law for hosting infringing third party's data unlessthey have genuine knowledge of unlawful exercises or infringing data. It isalong these lines clear that ISPs won't be held criminally at risk on the offchance that they have only constructive knowledge.

The second point isn'tsignificant to criminal obligation, however rather concerns civil liability fordamages. Under this condition, ISPs won't be held subject of breaking the lawunless they know about actualities or conditions of infringing data or unlawfulexercises. Hence, the standard to hold ISPs liable for civil liability isconstructive knowledge. Nevertheless, regardless of whether ISPs have genuinelearning or valuable knowledge of infringing data or unlawful exercises, theycan still be excluded from being liable in the case that they immediatelyremove and delete the infringing data and disable access to it once theyreceive the knowledge or awareness.

In addition, it additionally expresses thatthe conditions said above won't be applied when the recipient is acting underthe authority or the control of the

ISP. Cyprus: In Cyprusaccording to the Law Providing for Certain Aspects of Information SocietyServices and Particularly Electronic Commerce, Law 156(I) of 2004, as amended(Law 156(I)/04) for an ISP to be considered legal in Cyprus must be one havingtheir headquarters and main base of activities in Cyprus, however it does notmatter if their technological infrastructure is located in Cyprus or not. As for thelegal part of their liability obligations, they are not considered liable forthe information transmitted, on condition that the ISP: a) does not initiate the transmissionb) does not select the receiver of thetransmissionc) does not select or modify theinformation contained in the transmission Regardingthe provision of an information society service is provided that consists ofthe transmission in a communication network of information provided by arecipient of the service, the ISP shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the solepurpose of making more efficient the information’s onward transmission to otherrecipients of the service upon their request, on condition that:(a) The ISPdoes not modify the information;(b) The ISPcomplies with conditions on access to the information; (c) The ISPcomplies with rules regarding the updating of the information, specified in amanner widely recognized and used by industry;(d) The ISPdoes not interfere with the lawful use of technology, widely recognized andused by industry, to obtain data on the use of the information; and(e) The ISPacts expeditiously to remove or to disable access to the information it hasstored upon obtaining actual knowledge of the fact that the information at theinitial source of the transmission has been removed from the network, or accessto it has been disabled, or that a court or an administrative authority

hasordered such removal or disablement. Regarding aninformation society service that consists of the storage of informationprovided by a recipient of the service, the ISP, subject to the recipient ofthe service not acting under the control of the ISP, shall not be liable forthe information stored at the request of a recipient of the service, oncondition that: (a) The ISPdoes not have actual knowledge of illegal activity or information and, asregards claims for damages, is not aware of facts or circumstances from whichthe illegal activity or information is apparent; or(b) The ISP, upon obtaining such knowledge or awareness, acts expeditiously to remove or todisable access to the information. (4)Regarding the monitoring of information transmitted or stored under anyinformation society services provided within the context of any of s.

s. 15, 16and/or 17 of Law 156(I)/04, there shall be no general obligation on ISPs tomonitor the information which they transmit or store, nor a general obligationactively to seek facts or circumstances indicating illegal activity. Conclusion: TheECD has answered the question that to what extend ISPs should be responsiblefor online copyright infringement by establishing a set of rules concerning thelimitations of intermediary liability. The ECD provides theprotection for ISPs who perform certain activities and comply with theconditions set forth in the ECD. Moreover, the ECD harmonized the laws amongMember States, and therefore it can enhance the development of the internal market. However, Member States apply the ECD to their national legislation differently. Moreover The ECD does not affect the possibility for Member States to deal withISP liability issue in accordance with

their national laws, meaning thatnational legislations remain intact. Nevertheless, the ECD falls shot in some areas.

The main areas that the ECD does not coverare that it does not provide protection for information location tool providers. Hence, in this regard it depends on the national law of each Member State whetherISPs are liable where they provide information location tool services. Moreover, the ECD does not establish the notice and take down regime, andtherefore problems arise regarding the knowledge standard, freedom of expressionand unfair competition as explained above. Reference: 1) https://www. linkedin. com/pulse/20140723161608-20092204-eu-and-cyprus-law-on-electronic-commerce-and-online-services/ 2) https://books. google. com. cy/books? id= 1HcH18cqJh0C= notice+and+notice+canada= gbs_navlinks_s= y 3) http://ec. europa. eu/internal_market/e-commerce/directive_en. htm 4) https://ec. europa. eu/commission/priorities/digital-single-market_en#documents 5) http://digitalcommons. law. scu. edu/cgi/viewcontent. cgi? article= 1315= chtlj