NEW MEDIA AND CIVIL LIABILITY

Katerina Dulčić
Polytechnics Nikola Tesla in Gospić

Abstract
The author considers the impact of the new media from the aspect of civil liability actions done on the internet. New technologies have become widely accessible for everyone. They allow easy and fast communication. Literally everybody can be a publisher on social networks, blogs or just comments on sites. In not such a long ago history, publishers were big companies with ability to pay damages. Today, the responsible person can be even a child. Therefore, the courts have made some decisions that declared intermediates responsible for their clients’ actions. To protect themselves, the internet service providers should not allow anonymous services or protect themselves with adequate measures. The legal cases explained in the article show which conducts results with liability or frees of responsibility in some jurisdictions.

Key words: Internet Service Provider, civil liability, damages, user generated content, author’s responsibility

Introduction
In their article, Warren and Brandeis (Warren, Samuel D., Brandeis, Louis, 1890) have criticized the media at their time. At the end of the XIXth century they said: “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers...". What would they say if they saw the technology today?

Today, media are responsible and liable for any damage they may cause by their publishing. The level and causes may be variable in different countries and legal system, but, professional journalist try to publish the truth, protects the minors all under the “treat” of potential damage reparation.

Social networks make anybody able to publish their own ideas, but the problem is: who is liable for eventual damages.

1. Variety of publishers
The “classic” paper media that have their on line editions are not much questionable. For them it is easy to apply the principle of internet analogy cases (Harpaz). But, there are many other, even anonymous, publishers that express their freedom of speech on the internet. There are free blog services, social networks and even comment sections on web sites that can cause the damage to people, but also to companies.

In 1998 there was a case of a member of a newsgroup that posted a massage that said: “Run away from the Bank X”! The Bank requested the removal of the massage, but the responsible of the newsgroup did not do that. They requested the removal and the damages of the writer, person responsible of the newsgroup and the company hosting the newsgroup. The court rejected their request on the bases of freedom of speech. (Tribunale di Roma, 1998).

The first type of user generated content website moderates (i.e., checks or vets) the user generated content before it goes online. The website owner or its employee or agent typically checks for potential legal issues (see below) and inappropriateness3 and makes a decision on what to upload and what to shelve. Sometimes, the user generated content will be edited before it goes online. The
advantage of such “pre-moderating” is that the website becomes a cleaner environment and the likelihood of any infringing content being uploaded onto the site is reduced. The main disadvantages are the probable delay before content goes live, and the potential liability of the website owner (as an editor or publisher) for the UCG, even if it did not create the material. In addition, moderation can be costly and time-consuming. Websites that do not moderate their user generated content may be able to rely on an intermediary defense, provided that the website was set up appropriately, the website owner was not aware of the problem, and the operator took reasonable care and acted promptly to remove the content once on notice. The European and UK intermediary exemptions from liability are relatively untested, so for now the website owner will have to take the risk that they will provide protection in the circumstances. In our view, the middle ground of “post-moderation,” that is, checking the user generated content after it has been uploaded, is risky from a legal perspective although it may be a sensible compromise in practice. If the website owner can prove that it had not reviewed and was not aware of the content until put on notice and adequate safeguards were in place, it may be in the same position as an unmoderated website. However, if the moderators noticed the infringing content but let it through, or ought to have noticed it, the website owner may legally be in the same position as an editor or publisher of the content. Further, a claimant could claim that the website’s moderators should have spotted the infringing content more quickly and by not removing the content, the website owner was not taking reasonable care. A claimant could also claim that if the website could postmoderate all content, then it should have pre-moderated it. These arguments are currently untested, at least in the UK. The worst of all worlds, from a European legal liability perspective, is to have strollers on the site. These are individuals who peruse the content and sometimes interact with the discussion. It may not be clear what they have seen and what they have not at any one time. If they fail to take down infringing content, the website is likely to be liable by virtue of the fact that it will be deemed to have known of the infringement. Similarly, if the strollers do not access a particular thread, then the claimant could argue that the website did not take reasonable care because the strollers should have checked the thread in question (Pinto et. al., p. 5-6).

2. Permanent data on the internet

The risk of publishing on the internet and divulgation of data is major, especially if we deal with data interesting to a wider public. It is impossible to remove such data and protect the right to your own image. There are examples often cited in American legal literature known with names: “Star Wars Kid” and “Numa Numa Dance”.

The Star Wars Kid was a teenager that filmed himself with a video camera acting a character of the movie Star Wars, back in 2002. He was making the sound effects by himself, playing with a broomstick instead of the light sward. He was obese and clumsy. He made the video tape at the school studio and left it there. A year later, in 2003, a group of pupils found the tape and they thought it was so funny to deserve a wider public. So they digitalize it and posted at the local internet community, which porpoise was sharing digital files just among members. Even that was quite embarrassing for the boy that made the tape for himself and a small group of personally chosen members. But the divulgation didn’t stop at the local community; it went viral on the internet. Today, it is still possible to see the original version and many edited versions with animations added. Kid’s parents got an extrajudicial agreement with the guilty pupils, but they had to move. The most hurting part was the nasty comments that accompanied the video on many sites. (Solve, 2007; 46-47). The question is where this man can hide, today, as the video is viewable from every spot on the Earth that has internet access. His five minutes of having fun are object of fun to so many people he hasn’t ever met.

Similar case was the one that has as protagonist a Chinese child named Qian that has been photographed without his knowledge during a class on traffic safety. He had a round reddish face, he was looking on a side and had lips tightened together. The photographer posted the photo on the internet, and many liked his face. They inserted it in different photos from famous paintings like Mona Lisa, to movie posters and even newspapers photos, so poor child can see his own picture sitting with President Bush. When he was informed about it by his friends, he was shocked, but later get used to
his popularity, never searched. He was just attending a class, and a picture of him has been taken. (Solve, 2007; 43,44).

The case of “Numa Numa Dance” is different because it was self-published. The protagonist filmed himself singing a Romanian pop song, but he did not expect such wide publicity. At the moment he wanted to get back his private life, and be an anonymous again, it was impossible.

Almost anybody has the need to do some funny thing that he or she want to share just with a very restrict public. Everybody should be able to choose with whom to share own abilities, and who is not allowed to see something. Wide access to technology gives us the opportunity to memorize our precious moments in a simple way, but also gives the opportunity to others to take picture of us and also make videos. In the 70’ and 80’ cameras were big and not everybody was able to have them. If someone with a video camera entered a room, people would start to take care of their behavior, because it could be filmed. Today, we don’t notice a camera, almost everybody has a smartphone, able to take photographs, make videos, edit them and then share it on social networks. And it is impossible to notice whether someone is reading newspapers on their phone, working, or filming you falling on the wet floor in a restaurant. And social network group of the person you do not even know is watching and rewatching your fall within five minutes or less.

3. Control over the published materials

In old times, we had camera films, we brought them to a studio and we got photos and the film back. Our pictures were under our control all the time. Today, we mail digital files to be printed, and we cannot be shore whether the printing studio hasn’t sold copies to a photo bank (like: www.fotolia.com). But even if the protagonist is selling his own photos, they cannot be shore for the use of these photos. The agency does not know the porpoise for which they were brought. So they can end up clipped as the face of the Chinese boy Qian. Nevertheless, the Agency obliges it’s members not to use fotos in defamatory manner (see: download agreement art. 3 comma g, http://eu.fotolia.com/Info/Agreements/StandardLicense), the effective control is impossible. The photos can be downloaded anywhere in the world, and there is no obligation clause to inform the agency of the effective use of the downloaded photos. The majority of the license agreement covers the economic and retribution part of the sold art work.

4. Responsibility of the author

As in the real material word, on the internet, there is clear responsibility for the written words. The criteria vary from country to country, as it should be. Defamation and especially slander should be judged by the standards of the community where the offence took place. The same words have different meanings in different communities. But that is not the object of this article.

It was easy for Mr. Mark James to request damage reparation from Ms. Jaquelline Thompson for her blog posts. They were from the same community, and she signed her blog posts. Mr. James was Chief Executive of Carmarthenshire County Council and Ms. Thompson in her posts accused him of corruption. She did not have any proof of Mr. Jones corruption, so she was declared guilty for libel and had to pay for moral damages 25.000 £. (Thompson v. James, [2014] EWCA Civ 600).

The facts in this case regarded a rather small community, and the fact that these libelous declarations were available for anybody with internet access; no one was interested in them. There was no massive sharing to social networks. It should be expected that the article on the blog has not been read out of the local British county it regarded.

4.1. When author is anonymous

Internet allows authors to be anonymous. It is not impossible to determinate IP address of a computer that was used to post “anonymously”, but first the service that hosts the post has to spend valuable
time to determine which Internet Service Provider was used to access their web site, than Internet Service Provider that assigns automatically IP addresses has to research to what physical address was that IP address assigned in particular lapse of time, and then it has to be determined who used that computer. It can be done for major crimes, but in libel cases it is impossible, for the costs and benefit calculation. It would be unjust to require this cost of an offender that is responsible just for slander or label.

In considering liability for user generated content, it is important to appreciate that there is a spectrum of intermediaries that are more or less involved in the dissemination of the content. At one end of the spectrum is the company that operates the cables and routers that make up the backbone of the Internet. These mere conduits, by analogy with a postal or telephone service, are generally immune from liability for the content passing through their systems. Then there are the pure internet service providers (ISPs), which do no more than enable the public to access the internet. Next are the entities that are technical hosts of websites, in the sense that they provide the servers on which the website is stored. Finally, there are those that control the user generated content websites onto which users upload content. A key issue in European law is the extent to which website owners of user generated content sites are immune from liability for actionable user generated content over which they had no knowledge and did not create. (Pinto et. al., p. 5)

On the Google blog service, based and managed in the USA, but available worldwide, known as Blogger.com, on the blog “London Muslim”, some posts appeared that Mr. Tamiz considered defamatory of him. They were in forms of anonymous comments. Mr. Tamiz wrote letters of complaint to Google. Google has not acted immediately, but after almost two months, when the complaints were forwarded to the blogger. The blogger reacted within three days, and voluntarily removed the comments from his blog. Google defended itself with its policy towards the content of blogs, that states: “Blogger.com is not involved with the creation of content that people post on their blogs. It does not create, select, solicit, vet or approve that content, which is published and controlled by the blog owners. ‘Blogger is a free service for communication, self-expression and freedom of speech. We believe that Blogger increases the availability of information, encourages healthy debate and makes possible new connections between people.

We respect our users’ ownership of and responsibility for the content they choose to share. It is our belief that censoring this content is contrary to a service that bases itself on freedom of expression.

In order to uphold these values, we need to curb abuses that threaten our ability to provide this service and the freedom of expression it encourages. As a result, there are some boundaries on the type of content that can be hosted with Blogger. The boundaries we have defined are those that both comply with legal requirements and that serve to enhance the service as a whole.” Google also has the service “Report Abuse” that offers eight grounds for reporting abuse, and users have to select one of these. If the user selects ‘Defamation/Libel/Slander’, which is what appears to have happened in this case, a second screen is displayed. The second screen makes clear that the Blogger.com service is operated in accordance with US law, and that defamatory material will only be taken down if it has been found to be libellous (i.e. unlawful) by a court. The reason for this policy is that under US law, Google Inc is not a publisher of third party content hosted on blogspot.com. US law works on the basis that claimants must raise their defamation issues directly with the author of the material, not third party service providers such as Blogger.com. Given the volume of content uploaded by users of the Blogger service, it is usually not practicable for Google Inc to remove content without first receiving the Court’s determination that the content is, in fact, libellous. Google is not in a position to adjudicate such disputes itself.

Even by the European law Google was not found to be the publisher of anonymous comments, with arguments: “It is no doubt often true that the owner of a wall which has been festooned, overnight, with defamatory graffiti could acquire scaffolding and have it all deleted with whitewash. That is not necessarily to say, however, that the unfortunate owner must, unless and until this has been accomplished, be classified as a publisher.” But judges considered that existence of a contractual term about the content of blogs is not sufficient to give it “effective control” over the person who posted the defamatory comments. There was no basis for concluding in relation to that period that Google Inc
failed to take reasonable care in relation to publication of the comments or that it knew or had reason to believe that it caused or contributed to their publication. Greater difficulty aroused, however, in relation to the application of the conditions to continued publication of the comments after Google Inc had notice of their allegedly defamatory content. The Court found that the response was somewhat dilatory, but it was not considered in all the circumstances of this case, to be outside of the bounds of a reasonable response. (Tamiz v. Google Inc [2013] EWCA Civ 68)

As a conclusion of this case, the person that just hosts other materials, should adopt necessary measures for protection of liability. Once the host has become aware of any actionable content they should: immediately block and remove the content; inform the user; use search/filter software to identify, remove, and block contents “of the same kind,” i.e., identical and similar content by the same user; similar content by the same user; and identical content by other users; and manually review the results produced by the search/filter, if necessary.

5. Doctrine of appropriation of third–party content

Several German courts (including at the appellate level and confirmed to a significant degree by a November 2009 decision of the Federal Supreme Court - Federal Supreme Court, Decision of 12-11-2009–I ZR 166/07.) have developed a doctrine of appropriation of third-party content. The doctrine states that if the host has appropriated the UGC, it can be made liable for the appropriated content as for its own content.

This doctrine seems to contradict the Ecommerce Directive, but is nevertheless applied by a number of German courts. As a result of its recent confirmation by the Federal Supreme Court, the doctrine poses further threats to website operators who face claims in Germany. Whether there has been an appropriation, depends on the design of the website. In 2007, the Hamburg Court of Appeal (Court of Appeal Hamburg, Decision of 26-09-2007–5 U 165/06.) presumed the appropriation of user generated content because recipes uploaded to the website by users, including infringing photos, constituted the entire editorial content of the website. The Federal Supreme Court confirmed this decision on November 12, 2009 (Federal Supreme Court, Decision of 12-11-2009–I ZR 166/07.). Because the full reasoning of the court had not been published when this article was prepared, a thorough assessment cannot yet be made. However, according to the published press release, the court seems to have followed the reasoning of the Hamburg Court of Appeal, which found that the host reviewed the recipes before activating them, was granted comprehensive rights of exploitation of the accompanying photographs in the website’s terms of use, and affixed its logo to them. According to the court, the host at a minimum should have ensured that the photographer’s name was identified when the photographs were uploaded. If that name was not the name of the party uploading the content, the upload would have to be refused.

In another decision handed down in 2008, the Hamburg Court of Appeal (Court of Appeal Hamburg, Decision of 10-12-2008–5 U 224/06.) confirmed an appropriation of user generated content in the case of a host providing a platform for users to upload and share picture files. The users were able to register without identification and could then upload picture files and share them with third parties by sending or publishing links to their “public” album. Third parties were able to order prints of these picture files from the host for payment, while the uploading users did not receive any remuneration. The court argued that the host had appropriated the user generated content because the picture files constituted the only substantial content of the website, the host enabled users to purchase the photos from him, the host issued an invoice for the sale, every photo was made accessible under the website’s brand (as well as the user’s name), and the website terms granted the host comprehensive rights of exploitation.

In a 2002 case, the Cologne Court of Appeal (Court of Appeal Cologne, Decision of 28-02-2002–15 U 221/01.) found the host of a photo community website to be liable for the infringement of Steffi Graf’s personality rights by a photograph uploaded by a user. The court reasoned that the host had, primarily but not exclusively in an automated process, enabled users to activate communities about certain themes chosen by the users on its website by requesting a short description of the community and an
assessment of the target age group. In doing so, the host was found to have given the impression that it was vetting the third-party content beforehand and identifying itself with it.

Other decisions of the Hamburg Court of Appeal show a more differentiated application of the appropriation doctrine in regard to discussion forums, although there are no signs that the doctrine is being abandoned. In February 2009, the court (Court of Appeal Hamburg; Decision of 04-02-2009–5 U 167/07.) ruled that copyrighted photographs uploaded by a user in an unmonitored discussion forum were not appropriated by the host, reasoning that the content was posted in a section of the website labeled “community,” as opposed to the editorial part of the website, and the host had not influenced user content in any way. The facts that the host had provided the themes and structure for the discussion forum and that the website was to a certain extent financed by advertising were not seen as sufficient for an appropriation of the user generated content. In another decision, the court (Court of Appeal Hamburg, Decision of 04-02-2009–5 U 180/07.) applied the same reasoning, ruling that the provision of themes, structures, or forum rules regarding prohibited content was not sufficient for an appropriation. In that decision, the court stated that the host of a discussion forum was not obligated to implement technical measures against uploading photos in the forum from the outset. This rule also applies even if the host had become aware of one case of infringement through the upload of a photo.

In any case, hosts of discussion forums should be careful to prevent any impression that might enable the appropriation doctrine to be applied. An appropriation could be implied if the host, as a result of specifying the topic, would expect infringing contributions (District Court Düsseldorf, Decision of 14-02-2002–2a O 312/01.). Generally, however, the host of a discussion forum is not obliged to monitor its content. Monitoring content may make matters even more difficult for the host, for instance, if the host reserves the right to examine or “approve” third-party content prior to its upload. This could be interpreted by the courts as appropriation, and therefore for the responsibility. (Pinto et al., p.8-9)

6. Intermediates and their activity

As a protection of anonymous comments, some people slandered on the internet tried even a more radical approach. So Mr. John Bunt sued the effective comments authors, but also their Internet Service Providers. The high point of Mr. Bunt’s case in this respect was to rely upon the fact that the corporate Defendants have provided a route as intermediaries, whereby third parties have access to the internet and have been able to pass an electronic communication from one computer to another resulting in a posting to the Usenet message board. The Usenet service is hosted by others, who were not parties to the proceedings, such as Google. It is not accepted that the relevant postings necessarily took place via the relevant ISP services, but that would be a matter for the Claimant to establish at trial.

The Court turned first to the Electronic Commerce (EC Directive) Regulations 2002, which came into force in August of that year. They define the circumstances in which internet intermediaries should be held accountable for material which is hosted, cached, or carried by them but which they did not create. The protection which these regulations afford is not confined to the publication of defamatory material. They embrace other illegal material, such as child pornography or the infringement of intellectual property rights. The plaintiffs explained the procedure of caching, and their impossibility to control what are their clients doing by using their internet connection. “The ability to view web pages quickly is an attractive attribute for users of the internet. The enormous volume of requests for web pages generated by internet users has led to the development of technical solutions by network providers and internet service providers to enable more efficient transmission of that information across the internet. Caching is one such solution. It is a technical process which enables internet providers to speed up the delivery of web pages to internet users by making a temporary copy of a web page that is requested by a user. When a subsequent request is made for the same page, the user can be provided with that content from the local ‘cached’ copy made by the internet service provider, rather than having to go back to the original web site which is the source of that page. This process enables the more efficient onward transmission of web pages to internet users. A web cache (including AOL’s) is not a copy of the internet – that is neither the purpose of a web cache, nor would it be commercially or technically feasible. In order for web caches not to have to expand in memory size indefinitely the actual content
in a web cache is designed to be overwritten in accordance with automatic defined rules ensuring that (i) cached content is up to date and (ii) cached content which is not being searched for (or has been removed or altered) is overwritten.” They explained that it was a merely technical procedure, done by computers without human interference, therefore impossible to select the content whether it is offensive of not to someone.

The mechanism of storage by the ISP web cache is completely automatic. Providers of web sites set automated ‘rules’ or conditions specifying; (1) whether a page may be cached; (2) if it may be cached, at what time that cached material should expire; and (3) whether the cache computers should revalidate with the original source web site as to whether a page sitting on AOL’s web cache has been updated or deleted. These rules are embedded in instructions which exist ‘behind’ web pages and the rules are applied by, and are readable by, web browser software in accordance with industry standards. This ensures that users of the internet reach the most up to date versions of web pages available. By way of example, for frequently updated pages like the BBC’s news home page (located at http://news.bbc.co.uk), the instructions behind that particular page will dictate that the page should not be cached. Each time that page is requested, those instructions state that it should be retrieved from the original source, not from a cached copy. By contrast, the messages hosted by Google Groups London contain instructions that allow caching but require that a web cache should revalidate the content with the original source for each subsequent request. So, if a particular message is cached, before the cache displays that content to a subsequent user requesting that page, the cache will check with Google as to whether that page has subsequently been removed or deleted. This entire process is entirely automatic and the only reason for it is to make the transmission of web pages more efficient. ISP does not modify the information contained on web pages in any way. ISP complies with any conditions embedded in such pages regarding access to the information (for example by preventing the caching of pages which contain instructions for them not to be cached) and does not interfere in any way with the lawful use of technology widely used by the industry to obtain data on the use of information (for example tracking how many times a source page has been accessed).

Based on this technical information, the judge did not consider the Internet Service Providers responsible as publishers or editors. (Bunt v. Tilley, Hancox, Stevens, AOL UK Ltd, Tiscali UK Ltd, British Telecommunications plc, [2006] EWHC 407 (QB)).

7. Comparison with the USA

The USA is the mother land for internet. It started there, and majority of services are hosted in the USA.

In the United States, the broad protection provided by section 230 of the Communications Decency Act of 1996 means that websites generally do not have to face many of these issues. Section 230 provides that “no provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” Interactive computer service is broadly defined as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server.” The most common interactive computer services are websites.

The immunity is lost to the extent that the publisher is an information content provider, which is defined as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet.” As the Ninth Circuit Court of Appeals explained in Fair Housing Council of San Fernando Valley v. Roommates.com: A website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is “responsible, in whole or in part” for creating or developing, the website is also a content provider. Thus, a website may be immune from liability for some of the content it displays to the public but be subject to liability for other content. In some very limited situations, therefore, a website may be potentially liable if it helped create the content at issue, as happened in Roommates.com. The website in Roommates.com had been designed to match individuals looking to rent a room with users
who were renting out a room. The website required users to select options from drop-down and checkbox menus about their age, sex, and sexual orientation, and whether children live in the household, and about users’ preferences on these subjects. The majority of the Roommates.com court held that, by “requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others.” (Fair Housing Council of San Fernando Valley v. Roommates.com, L.L.C., 489 F.3d 921 (9th Cir. 2007), rev’d in part, vacated in part, aff’d in part, 521 F.3d 1157 (9th Cir. 2008)) Thus, the defendant could not claim immunity from alleged violations of the Fair Housing Act as a mere “provider . . . of an interactive computer service,” as defined by Section 230.

On the other hand, and in stark contrast to the EU, under Section 230 immunity is not lost once the publisher is on notice of the allegedly defamatory content.52 As a result, failure to take down a post, even one that gives rise to liability for the individual who posted it, does not take away the safe harbor for the website owner. (Pinto et. al., p. 12)

8. Conclusion

The responsibility of the individual author that uses the new media as an expression of own freedom of speech is out of question. The author is liable for every offence he or she can do. The problem is that they have to be identified. And there lies the responsibility of Internet Service Providers.

The internet service providers should consider their position very carefully at the moment they set up their service. The service has to be careful of what is provided, and if they control the user generated content, they are responsible. Maybe, the best way is to avoid the control of the content and allow the requests for removal, or abuse complaints. That is a reasonable cost and benefit solution for free content. Otherwise, hosts should have a great amount of polyglots able to control in real time given content. The control over posted material, or posting upon approval is possible only on small community websites. In cases of many requests for posting, the service would be slow and therefore not interesting for the clients.

Another thing should be taken in consideration: the amount of damages. Considering the inability of removal of certain content (because they have been already copied by users or other sites), the amount of remuneration should be higher than the one for the offences published in “classic” media.

On the other hand, the publishers of “classic” media are big companies, with financial ability of paying the damages. The publishers on the new media are often individuals, unable to pay for the damages they can cause. Sometimes, they are even underage. Therefore, the legislators started converting the responsibility towards Internet Service Providers, which are the persons to get profit from the offensive activities of individuals. There is still not objective liability without the guilt, but, as we can see, in some cases it is pretty close, especially in Germany.

Bibliography:


6. Thompson v. James [2014] EWCA Civ 600, The Court of Appeal (Civil division), Case No: A2/2013/1768,
