Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

Transatlantic Antitrust and IPR Developments

Bimonthly Newsletter

Issue No. 5/2018 (November 2, 2018)

Contributors:

Gabriel M. Lentner, Jonathan Cardenas,
Kletia Noti, Marie-Andrée Weiss

Editor-in-chief: Juha Vesala

Contents

About the contributors

Gabriel M. Lentner is an Assistant Professor of Law at the Danube University Krems. He holds a Ph.D. in International Law and is a Lecturer in Law at the University of Vienna School of Law. Gabriel received a diploma with highest distinction in European Studies from the University of Vienna in 2010 and a diploma in Law & Logic from Harvard Law School and the European University Institute in Florence in 2013. His main research interests lie in international investment and EU Law, as well as public international law. As a TTLF Fellow, his current research focuses on the protection of intellectual property rights through international investment agreements. Gabriel wishes to acknowledge valuable research assistance by Filippo Faccin and Antonia Mathioudaki.

Jonathan Cardenas is a corporate associate in Crowell & Moring's Washington, D.C. office, and is a TTLF Fellow. Prior to joining Crowell & Moring, Jonathan served as a postdoctoral fellow with the Information Society Project at Yale Law School. Jonathan received a J.D. from New York University School of Law, where he was a Jacobson Leadership Program in Law & Business Scholar, and where he served as managing editor of the NYU Journal of Law & Business. He received an M.Phil. in international relations from the University of Cambridge and a B.A. in political science, summa cum laude, from the University of Pennsylvania.

Kletia Noti is an associate with Grimaldi Studio Legale, Brussels, where she joined the EU Law, Competition and Regulatory Department in 2015. Prior to this, she practiced EU Competition Law in the Brussels offices of Clifford Chance LLP and was an associate at Cleary, Gottlieb, Steen and Hamilton LLP. Kletia also worked for several years as an academic assistant in charge of the European Law and Economic Analysis (ELEA) program at the Department of Law and Economics of the College of Europe, Bruges. At the College of Europe, Kletia also taught tutorials in EU Competition Law and researched the intersection of intellectual property and antitrust law. Kletia holds an LLM from Columbia University School of Law and a Master's and Bachelor's degree summa cum laude from Bocconi University in Milan. During her studies at Bocconi University, Kletia was an exchange student at the University of California, Los Angeles, on a scholarship granted by Bocconi University. She has also been a visiting student at Harvard University. Kletia's community involvement includes her current role as an EU policy monitor for the IP Transactions & Licensing Committee at the Intellectual Property Section of the American Bar Association. Prior to this, she was a member of the editorial board of the *World Competition: Law and Economics Review*. Her previous work experience includes internships at the European Commission's Directorate-General for Competition, Clifford Chance LLP, and Studio Legale Monti in Milan.

Marie-Andrée Weiss is an attorney admitted in New York and in Strasbourg, France. Before becoming an attorney, she worked for several years in the fashion and cosmetics industry in New York as a buyer and a director of sales and marketing. She graduated from the

University of Strasbourg in France with an M.A. in Art History, a J.D. in Business Law, an LL.M. in Criminal Law, and an LL.M. in Multimedia Law. She also graduated from the Benjamin N. Cardozo School of Law in New York City with an LL.M. in Intellectual Property Law. She is an attorney in New York and her solo practice focuses on intellectual property, privacy, data protection, and social media law. As a TTLF Fellow, her fields of research are freedom of speech on social media sites and the use of consumers' likenesses in marketing and advertising.

Intellectual property

United States

A Study in Trademarked Characters

By Marie-Andrée Weiss

The characters created by Disney, Marvel, and LucasFilms are valuable intellectual property and are protected both by copyright and by trademark. However, a recently decided case in the Southern District of New York (SDNY), *Disney Inc. v. Sarelli*, 322 F.Supp.3d 413 (2018), demonstrates that preventing the unauthorized use of such characters may not be as easy as expected.

In this case, Plaintiffs are Disney Enterprises, Marvel Characters and LucasFilm, all of which own copyrights and trademarks in many of the most famous characters in the world, such as Mickey Mouse, Hulk, and Chewbacca. These characters were first featured in movies like *Frozen*, *The Avengers* or *Star Wars*, and are now licensed or featured in derivative products such as comic books, video games, or theme parks. Their exploitation is highly lucrative.

When visiting Plaintiffs' theme parks, one has a chance to meet the characters "in person." This experience is also offered by Characters for Hire, a New York company offering, as the name implies, character hiring services. The company's principal owner is Nick Sarelli (Defendant). Characters for Hire offers a service wherein actors dressed in costumes entertain guests during birthday parties or corporate events. For example, actors have allegedly dressed as Mickey, Elsa and Anna from *Frozen,* Captain America and Hulk from *The Avengers*, and Luke Skywalker and Darth Vader from *Star Wars*.

The contracts Defendants provided to their clients contained disclaimer language, stating, for example, that Defendants do not use trademarked and licensed characters. The contracts also warned clients that the costumes may differ from those seen in movies "for copyright reasons," adding that "[a]ny resemblance to nationally known copyright character is strictly coincidental."

These disclaimers did not appease Plaintiffs, who sent several cease and desist letters to Defendants before filing a federal copyright and trademark infringement suit and a New York trademark dilution suit.

While Judge Daniels from the SDNY granted Defendants' motion for summary judgment and dismissed Plaintiffs' claim for trademark infringement on August 9, 2018, he denied the motion to dismiss the copyright infringement claim and the trademark dilution claim.

The descriptive fair use defense failed

Plaintiffs claimed that the use of their trademarked characters to advertise and promote Defendants' business, along with their portrayal by costumed actors, was likely to confuse consumers as to the origin of the services.

Defendants argued that their use of Plaintiffs' characters was descriptive and nominative fair use, and that there was no likelyhood of confusion.

Descriptive fair use is an affirmative defense to a trademark infringement suit, as Section 33(b)(4) of the Trademark Act allows "use… of a term or device which is descriptive of and used fairly and in good faith [but] only to describe the goods or services of such party, or their geographic origin." In other words, a defendant can use plaintiffs' trademarks in a descriptive sense, or to describe an aspect of his own good or service.

For such a defense to succeed in the Second Circuit, a defendant must prove that the use was made (1) other than as a mark, (2) in a descriptive sense, and (3) in good faith (*Kelly-Brown v. Winfrey* at 308). This defense failed in the present case, as Defendants had not made a descriptive use of Plaintiffs' marks. Instead, Judge Daniels found that their ads "were specifically designed to evoke [Plaintiff's marks] in consumers' minds…"

The nominative fair use defense also failed

Defendants also claimed that they used Plaintiffs' marks to describe their own products. Such nominative fair use is a defense to a trademark infringement suit if such use "does not imply a false affiliation or endorsement by the plaintiff of the defendant" (*Tiffany v. eBay* at 102-103). But this nominative fair use defense also failed, as Defendants used Plaintiffs' marks to identify their own service, which is hiring out characters for parties, rather than Plaintiffs' trademarked characters.

Defendants' use of characters was not trademark infringement

Judge Daniels used the eight-factor *Polaroid* test used by the Second Circuit in trademark infringement cases to determine whether Defendants' use of Plaintiffs' marks were likely to confuse consumers.

While Plaintiffs' marks are undoubtedly strong (first factor), the similarity of the marks (second factor), weighed only slightly in Plaintiffs' favor because Defendants used different names for their characters than Plaintiffs' trademarked character names, e.g., "Big Green Guy," "Indian Princess," and "The Dark Lord" instead of Hulk, Pocahontas and Darth Vader.

The third and fourth *Polaroid* factors, the proximity of the goods and services, and the possibility that the senior user will enter

the market of the junior user, were found to weigh in Defendants' favor. There was no evidence that Plaintiff has plans to expand into the private entertainment service industry.

The fifth *Polaroid* factor, evidence of actual confusion, also weighed in Defendants' favor, as there was no evidence that Defendants' customers used the names of Plaintiffs' trademarked characters when referring to Defendants' services in online reviews or otherwise. Plaintiffs could not provide a survey proving customers' confusion either.

Judge Daniels found the sixth factor, Defendants' intent and evidence of bad faith, to also be in Defendants' favor, since Defendants had put customers on notice that their services were not sponsored by or affiliated with Plaintiffs by using altered versions of Plaintiffs' characters' names and by removing Plaintiffs' characters' names in their online reviews.

The seventh *Polaroid* factor, the quality of Defendants' products, was also in Defendants' favor, as Defendants' services, being of a lesser quality than Plaintiffs', makes it likely that consumers will not be confused as to the source of the services.

The eighth *Polaroid* factor, consumer sophistication, also was in favor of Defendants, as Plaintiffs did not prove the sophistication level of Defendants' relevant consumers.

Balancing these eight factors, the SDNY found no likelihood of consumer confusion and denied Plaintiffs' motion for summary judgment on their trademark infringement claim.

Trademark dilution

Plaintiffs chose to claim trademark dilution under New York trademark dilution law, Section 360-1 of New York Business Law, and not under the Federal Trademark Dilution Act. This choice may have been made because the New York law does not require a mark to be famous to be protected, and a plaintiff only needs to prove the mark's distinctiveness or secondary meaning.

Judge Daniels found that there was a genuine issue of fact as to whether Defendants' use of Plaintiffs' marks is likely to dilute Plaintiffs' marks by tarnishment. A court will have to determine if Defendants provide services of poor quality.

Copyright

Plaintiffs argued that Defendants had "copied and used the images, likenesses, personas, and names of Plaintiffs' characters…to promote and advertise its services online." Defendants argued in response that the characters in which Plaintiffs own copyrights are based on prior works that are part of the public domain.

Both parties will have more chances to pursue their arguments as Judge Daniels denied the motion for summary judgment on copyright infringement. He found that Plaintiffs had presented as evidence

screenshots from Defendants' website and videos allegedly published by Defendants which had not been properly authenticated. More specifically, they had not been authenticated by someone "with personal knowledge of reliability of the archive service from which the screenshots were retrieved," citing *Specht v. Google*, a 2014 Seventh Circuit case.

It is likely that the parties will settle out of court.

Intellectual property

United States

There is Such Thing as Bad (Right of) Publicity

By Marie-Andrée Weiss

Last June, the New York legislature failed, once again, to amend the state's right of publicity law. A similar bill, Assembly Bill A08155, had the same fate last year. New York Assembly Bill 8155-B had passed the assembly on June 18, 2018, but the Senate did not bring the bill to a vote before the legislature adjourned. This is fortunate, as the bill had several flaws.

The current New York right of publicity law

New York statutory right of privacy, Civil Rights Laws §§ 50 and 51, is a narrowly drafted law. The New York Court of Appeals recently described the legislative intent at passing this law as "slender" (*Lohan v. Take-Two Interactive Software, Inc*.). Indeed, the law does not provide an extensive right of publicity, but merely makes it a misdemeanor to use a living person's likeness, that is, her name, portrait or picture, "for advertising or trade purposes" without prior written consent. New York does not recognize any other privacy rights, not even at common law.

Identity as personal property

The bill clearly differentiated the "right of privacy" from the "right of publicity." During a person's lifetime, a person would have had a right to privacy and a right to publicity. Both rights would have prevented the unauthorized use of likenesses and names, but only the right of publicity would have provided the right to sell one's persona.

The "right of privacy" was defined as a "personal right, which protects against the unauthorized use of a living individual's name, portrait or picture, voice, or signature for advertising purposes or purposes of trade without written consent." This is essentially the right that is currently protected in New York. The bill would have also protected a person's signature, which is not currently protected. Moreover, under the bill, this right of privacy would have expired upon death, just as it does now.

The bill would have also created a "right of publicity," defined as "an independent property right, derived from and independent of the right of privacy, which protects the unauthorized use of a living or deceased individual's name, portrait or picture, voice, or signature for advertising purposes or purposes of trade without written consent."

The bill would have made an individual's persona his or her personal property, "freely transferable or descendible, in whole or in part by contract or by means of

any trust or testamentary instrument." The bill would, therefore, have made it possible to transfer one's persona, by selling it or licensing it, for a limited or unlimited time, and these contracts would have been able to survive death.

The dangers of making identity a transferable personal property

SAG-AFTRA, a performers' union, supported the bill. Its New York President urged its New York members to let their representatives know that they were in favor of passing the bill. However, the bill, as written, could have placed actors in danger of losing the right to use and profit financially from their personality.

The Fantine character, created by Victor Hugo in *Les Misérables*, sold her hair so she could send money to her daughter Cosette. One can imagine an actress, who once played Fantine in a *Les Mis* production, but who has since fallen on hard times, selling her entire persona in order to make ends meet. Hair can grow again, but under the bill, a persona could have been sold off for a long time, even forever. One could even imagine a persona becoming a commodity under the new law, with producers buying personas straight out of a 'central-casting' database. Representative Morelle noted during the debate that "[i]f someone looks like another person, that's not covered under this. You could go find someone who looks like Robert De Niro, or you could find someone that looks like another actor."

The bill would have thankfully forbidden parents or guardians from assigning the right of publicity of a minor and would have rendered such assignments unenforceable. Under this bill. Fantine could have sold her own persona, but not Cosette's.

A descendible right of publicity

Unlike other states, such as California, New York does not have a post-mortem right of publicity. The bill would have provided such a right for forty years after a person's death, whether she was famous or not. At the expiration of the forty-year period, the image of an individual would have been freely usable.

This right would have been descendible, either by testament or by intestate succession. Either way, the right would have been enforced by a person or persons possessing at least a fifty-one percent interest of the individual's right of publicity.

Persons claiming to be successors in the right of publicity of a deceased individual, or licensees of such rights, would have had to register their claim with the New York Secretary of State and pay a $100 fee. Thereafter, their claim would have been posted on a public web site specifically designed for that purpose. Parties interested in licensing or buying a particular right of publicity could have used this registry to find out who owns a particular right. Failure of a licensee or successor to register a persona would have been a defense for unauthorized use

of the deceased's persona. The sponsor of the bill, Representative Joseph Morelle, specified during the debate that the law would apply to anyone seeking damages in New York, provided that the interest had been registered in the New York registry.

The Electronic Frontier Foundation argued in a memorandum sent to the New York legislature that the law would pressure heirs to benefit commercially from the image of their deceased relatives, noting that in "a large estate, an inheritable and transferable right of publicity may add to the tax burden and thus lead heirs with no choice but to pursue advertising deals or some other commercial venture." Indeed, deceased artists such as Glenn Gould or Franck Zappa are back on the road performing as holograms.

Fake News, Deepfakes and the right to publicity

The bill addressed the issue of "*digital replica,*" which it defined as a "computer-generated or electronic reproduction" of the likeness or voice of a person, whether alive or dead. Representative Morelle explained that the bill aimed at codifying the recent *Lohan v. Take-Two Interactive Software* decision, where the court found that New York right of privacy law, which protects unauthorized use of a "portrait," encompasses the "graphical representation of a person in a video game or like media."

Use of such digital replicas would have been forbidden, without prior authorization, in expressive works such as a live performance, a dramatic work, or a musical performance "in a manner that is intended to create, and that does create, the clear impression that the individual represented by the digital replica is performing, the activity for which he or she is known." Athletes' digital replicas could not have been used in audiovisual works either, if doing so created "the clear impression that the athlete represented by the digital replica is engaging in an athletic activity for which he or she is known." This was probably aimed at protecting athletes against the unauthorized use of their likenesses in video games.

The dystopian movie *The Congress* featured actress Robyn Wright selling the right to her digital image to a studio, under an agreement which forbade her to ever act again. Even more sinister is the prospect of selling one's digital image for making pornographic movies. Indeed, Artificial Intelligence (AI) technology allows creation of "deepfakes" video where a person is depicted as performing sexual acts. Such technology can be used to seek revenge (so-called revenge porn) or simply to create porn movies featuring celebrities. The bill specifically addressed the issue of unauthorized use of digital replicas in a pornographic work and would have forbidden the use of digital replicas in a manner intended to create, or which did create "*the impression that the individual represented by the digital replica is performing* [*in such pornographic work*]".

Representative Morelle also mentioned during the debate that digital replicas can be used to create fake news, for instance, by making political figures look and sound

as if they are saying something they did not actually say, which brings us to the First Amendment issues this bill raised.

First Amendment Issues

New York courts found that the use of a person's likeness with respect to "newsworthy events or matters of public interest" is non-commercial and therefore not actionable under New York's right of publicity law (*Stephano v. News Group Publs.*).

Use of digital replicas would have been authorized for parody, satire, commentary or criticism purposes, or "in a work of political, public interest, or newsworthy value," or if the use was *de minimis* or incidental.

The bill would have explicitly provided a First Amendment defense to the use of a persona without prior consent, including use in a book, play or movie. This is in line with the recent California case, *Olivia de Havilland v. Fox Networks*, which had pitted the centenarian actress against the producer of *Feud: Bette and Joan*, an eight-part television show about the Joan Crawford/Bette Davis rivalry. Catherine Zeta-Jones portrayed Olivia de Havilland, and was shown in the movie giving an interview wherein she referred to her sister Joan Fontaine as a 'bitch', among a few more unsavory comments. Olivia de Havilland sued for infringement of her California right to publicity but lost because the use of her name and likeness in the movie was protected by the First Amendment. The case shows how public figures cannot always rely on their right of publicity to censor speech about themselves which they deem unsavory.

It has been reported that Olivia de Havilland plans to ask the Supreme Court to review the case, and the New York legislature is likely to introduce a new version of its right of publicity bill in the coming months. Right of publicity is developing, warts, holograms, and all.

Intellectual property

United States

What's New in the US-Mexico-Canada Agreement (USMCA)

By Gabriel M. Lentner and Antonia Mathioudaki

As readers know, NAFTA has been turned into the United States - Mexico - Canada Agreement (USMCA). Along with changes to minimize barriers in the automobile and dairy sectors, intellectual property rights, data protection, and dispute settlement have undergone considerable alterations. These changes are addressed here.

IP Protection Extended

As for intellectual property rights, the negotiations have resulted in enhanced protections, an outcome mainly desired by the US (and with considerable similarities with the 2015 TPP text).

In regard to copyrights, Art.20.H.7 of the USMCA stipulates that, following the author's death, his or her intellectual property rights shall be protected for 70 years onwards (thereby extending protection from the 50-year standard, by which Canada currently abides). In cases where no person's life is used as a basis for the copyright term, the minimum is now set to 75 years from the date of the first authorized publication. In NAFTA, the minimum was 50 years.

Biologics are a field which NAFTA did not specifically regulate. Under the USMCA Art.20.F.14, however, patent protection for new pharmaceutical products that are (or contain) biologics will last 10 years from the date of first marketing approval of that product in the Party concerned. Note that biologics protection in Canada is currently only 8 years. It is also important to highlight that the USMCA provides for a patent-term restoration system, enacted after request, in cases where the applicant's patent issuance has been 'unreasonably' delayed (Art.20.F.9).

IP Enforcement

Of utmost importance are the advanced enforcement provisions of IP rights protection. Under NAFTA, the competent authorities could act only after the filing of an application by the right holder (Art.1718). The USMCA provides for the *ex officio* authority of border officials to initiate border measures against suspected counterfeit trademark goods or pirated copyright goods which are imported, destined for export, in transit, or entering/exiting a free trade zone or a bonded warehouse; this is intended to combat the phenomenon of weak counterfeiting (Art.20.J.6). Further, the USMCA provides for the establishment of a new IP Committee, with the task of holding consultations on several cooperation

issues (Art.20.B.3).

Digital Trade Chapter

When the original NAFTA came into force in 1994, digital trade was not considered in the agreement. USMCA, however, dedicates a whole chapter to it (Chapter 19). Two key points in Chapter 19 should be emphasized. First, the rules on data localization restrict policies that require companies to store personal information within the local jurisdiction, which seems to conflict with what is provided for in the relevant EU regulations. The cross-border transfer, storage and processing of data is facilitated under the USMCA through, *inter alia*, the prohibition of custom duties on the transfer of digital products and the requirement that Parties do not (unnecessarily) restrict the cross-border transfer of personal information. Second, Art.20.J.11 introduces a safe-harbor provision for Internet Service Providers by requiring that parties limit the Providers' liability for monetary relief in instances of infringements where they merely maintain, transmit, or store unauthorized information, but do not control, initiate or direct the infringement.

Limitation of Investor-State Dispute Settlement

Reformation of the dispute settlement mechanism is another field of practical and legal interest. Chapter 11 of NAFTA provided for investor-state dispute settlement (ISDS) for protected investments. The foreign investor had recourse to an arbitral tribunal to challenge host State measures. Canada has now entirely withdrawn from the ISDS system. Thus, investor-state disputes are only permitted between the US and Mexico, and only under certain conditions. First, they are only available for alleged violations of the standards of national treatment and 'most-favored nation', as well as direct expropriation disputes. Furthermore, ISDS is only available after local remedies have been exhausted or after a time lapse of 30 months. As far as minimum standards of treatment (fair and equitable treatment) and indirect expropriation are concerned, the investors can only pursue a claim before domestic courts.

Notably, specific categories of US investors are permitted to initiate proceedings relating to oil, gas, transportation, infrastructure, and power generation concession contracts concluded between them and the Mexican government (USMCA Annex 14-E). Yet, the state-to-state dispute settlement mechanism of NAFTA's Chapter 19 has not undergone modification and remains in place.

Conclusion

The parties have chosen to maintain many of the original NAFTA principles, such as that bilateral and trilateral elements can coexist. The USMCA agreement, therefore, represents a compromise, bringing changes in some areas while leaving others untouched.

Other developments

United States

Olivia de Havilland Asks Supreme Court to Review Docudrama Right of Publicity Case

By Marie-Andrée Weiss

Actress Olivia de Havilland, DBE, is petitioning the Supreme Court of the United States for writ of certiorari for the following question:

"Are reckless or knowing false statements about a living public figure, published in docudrama format, entitled to absolute First Amendment protection from claims based on the victim's statutory and common law causes of action for defamation and right of publicity, so as to justify dismissal at the pleading stage?"

It all started with the television 'docudrama' series *Feud: Bette and Joan*, about the Bette Davis and Joan Crawford rivalry. In the docudrama, Catherine Zeta-Jones portrayed Olivia de Havilland calling her sister Joan Fontaine a 'bitch', implying that Frank Sinatra is an alcoholic, and generally enjoying good juicy gossip, even at the expense of her close friend Bette Davis.

This did not sit well with Miss de Havilland, who prides herself on having achieved success "without sacrificing her strong moral and personal commitment to truth… and plain old fashioned good manners." She found her portrayal in Feud to be false and damaging to her reputation, and filed a right of publicity and false light invasion of privacy suit against the producers of the show in June 2017.

Defendants filed a motion to strike the complaint under the California Strategic Lawsuits Against Public Participation (anti-SLAPP) statute, which provides defendants the right to dismiss cases which chill expression because Plaintiff engages in a costly and time-consuming litigation.

The Los Angeles Superior Court denied the motion, finding that *Feud* was not "transformative" under the *Comedy III Productions* 'transformative use' test and thus not protected by the First Amendment. In *Comedy III*, the California Supreme Court had found that an unauthorized use of likeness is protected by the First Amendment if it is transformative.

Defendants appealed. The California Court of Appeal reversed on March 26, 2018, finding that the way Plaintiff had been portrayed in Feud was not "highly offensive to a reasonable person" and that the First Amendment protected the portrayal of Plaintiff without her permission. Plaintiff then petitioned the California Supreme Court to review the case. The court declined to do so on July 11, 2018, and Miss de Havilland is now petitioning the Supreme Court for a writ of certiorari.

Is docudrama a knowing or recklessly false publication?

The scope of the question Petitioner is asking the Supreme Court is rather narrow and focuses of the issues of so-called docudramas, which mixes real life elements and dramatization. She argues that the court should review the case as it is "the right vehicle for [the court] to… clarify whether the First Amendment creates a special immunity for knowingly false statements **published in a docudrama** at a time when this genre is at an all-time high point" (emphasis my own).

Petitioner also argues, somewhat more broadly, that knowing or recklessly false statements in any form are not protected by the First Amendment and that "false factual statements possess no intrinsic First Amendment value," citing *United States v. Alvarez*.

False statements are not generally protected by the First Amendment. A docudrama is a fiction and fiction is, by essence, false. But concluding that fiction, because it is false, is not protected by the First Amendment would be a sophism.

The California right of publicity statute has an exception for matters of public interest if the use of the likeness of an individual has been made "in connection with any news, public affairs, or sports broadcast or account, or any political campaign." Miss de Havilland argues that this public interest exception does not protect knowing or reckless publication, and that if a fiction about a real person is knowing and recklessly false, the person thus portrayed should have the right to sue for defamation and unauthorized use of her likeness without being prevented to do so by the First Amendment.

It would be surprising if the Supreme Court accepts review of the case because the issue at stake – whether creators have the right to portray real persons in works of fiction without their permission – is well settled. The decision of the Los Angeles Superior Court appears to be only a fluke, and was reversed by the California Court of Appeal, which held that a person portrayed in a book, play, film or television show does not have the right to control "the creator's portrayal of actual people."

This dismissal of Miss de Havilland's claims was consistent with California case law. The Ninth Circuit held in the 2006 *Sarver v. Chartier* case that the right of publicity suit filed by an Army Sergeant allegedly portrayed in the *Hurt Locker* movie had been properly barred by the California anti-SLAPP statute. The film was based on an article published in *Playboy* magazine about Plaintiff's experience while he worked as an explosive technician in Iraq.

However, it can be argued that the *Sarver* case actually supports Miss de Havilland's argument. In *Sarver*, the Ninth Circuit did not use the *Comedy III* transformative test to reach the conclusion that the movie did not violate Plaintiff's right of publicity because it is transformative enough. Instead, it extensively quoted the only Supreme Court right of publicity decision, *Zacchini v. Scripps-Howard Broadcasting*, where the Supreme Court concluded that

the Ohio right of publicity statute could prevent broadcasting the entire performance of a "human cannonball" without violating the First Amendment, because petitioner had made significant economic investments in energy, talent and expense to prepare for his act.

The Ninth Circuit noted in *Sarver* that it interprets *Zacchini* as upholding a right of publicity "where the defendant appropriates the economic value that the plaintiff has built in an identity or performance" without considering whether defendant's use is transformative or not. This interpretation may lead a case such as this one to be decided in favor of the plaintiff, especially if one considers that the practice of securing a 'life rights agreement' before portraying a particular person in a movie or television show is prevalent in the business and is thus another way to profit from the economic value of one's identity.

Other developments

European Union

The UK House of Commons Treasury Committee Report on Crypto Assets

By Jonathan Cardenas[1]

On September 19, 2018, the UK House of Commons Treasury Committee (the "Committee") published a Report on Crypto-assets (the "Report"), which provides regulatory policy recommendations for the UK Government, the UK Financial Conduct Authority (the "FCA") and the Bank of England.[2] The Report forms part of the Committee's Digital Currencies Inquiry, which was launched in February 2018 to examine the potential impact of distributed ledger-based digital currencies on the UK financial system and to prepare a balanced regulatory response from the UK Government.[3] This article briefly summarizes the Committee's UK regulatory policy recommendations.

I. Crypto Asset Risk

The Committee's regulatory policy recommendations are structured around a variety of risks that crypto assets pose to crypto asset investors. These risks include: high price volatility; loss of investment due to fraud and/or third-party hacking of crypto asset exchanges; loss of access to crypto asset exchange accounts and/or digital wallets due to unrecoverable lost passwords; price manipulation due to poor market liquidity and relatively low trading volumes; potential facilitation of money laundering and terrorist financing; and, macro risk to UK financial stability. Mindful of these risks, the Committee notes that crypto assets presently fall outside the scope of FCA regulation merely because the "transferring, buying and selling of crypto assets, including the commercial operation of crypto asset exchanges"[4] do not meet legal definitional criteria to be considered as either a "specified investment" under the Financial Services and Markets Act 2000 (Regulated Activities) Order (the "Regulated Activities Order"), or as "funds" or "electronic money" under applicable payment services and electronic money regulation, as referenced

[1] Disclaimer: The views and opinions expressed in this article are those of the author alone. The material in this article has been prepared for informational purposes only and is not intended to serve as legal advice.

[2] UK House of Commons Treasury Committee, Crypto-assets, Twenty-Second Report of Session 2017-19, 19 September 2018. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf.

[3] UK House of Commons Treasury Committee, Digital Currencies inquiry: Scope of the inquiry, 2017. Available at: https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/inquiries1/parliament-2017/digital-currencies-17-19/.

[4] UK House of Commons Treasury Committee, Evidence - Financial Conduct Authority (DGC0028): Financial Conduct Authority's written submission on digital currencies, April 2018. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.pdf.

in expert witness reports provided to the Committee.[5]

1. Initial Coin Offerings

Consumer fraud in the context of initial coin offerings ("ICOs") is a topic of special concern to the Committee. The Committee recognizes that there is currently "little the FCA can do to protect individuals"[6] from fraudulent ICOs as a result of a regulatory loophole that permits ICOs to escape FCA jurisdiction. Since most ICOs do not directly promise financial returns, but rather, offer future access to a service or utility, they do not fall squarely within UK law definitions of "financial instrument,"[7] as referenced in expert witness reports provided to the Committee, and therefore are not FCA regulated.

The Committee concurs with the view of U.S. Securities and Exchange Commission Chairman Jay Clayton that ICOs should not escape the ambit of securities regulation merely because they change the form, and not the actual substance, of a securities offering.[8] The Committee also concurs with the view expressed in an FCA warning that consumers should be prepared to lose their entire investment in early stage ICO projects due to the FCA's lack of jurisdiction and consequent inability to protect consumers.[9] As a result, the Committee recommends that the Regulated Activities Order be updated, as a matter of urgency, in order to bring ICOs within the scope of FCA jurisdiction.

2. Crypto Asset Exchanges

The facilitation of money laundering and terrorist financing through crypto asset exchanges is another area of major concern addressed by the Committee. Crypto asset exchanges are not currently required to comply with anti-money laundering ("AML") rules under UK law because their activities are not specifically captured by the language of UK AML regulation, including, most notably, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.[10] Although current UK AML regulation does not target crypto asset exchange activity, crypto asset exchanges do fall within the scope of the European Union's 5th Anti-Money Laundering Directive (the "5th AML Directive").[11] As a consequence, the

[5] UK House of Commons Treasury Committee, Evidence - Financial Conduct Authority (DGC0028): Financial Conduct Authority's written submission on digital currencies, April 2018.

[6] UK House of Commons Treasury Committee, Crypto-assets, 19 September 2018, at para 87.

[7] UK House of Commons Treasury Committee, Oral evidence: Digital Currencies, Statement of David Geale, Q 193, HC 910, 4 July 2018. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/oral/86572.html.

[8] U.S. Securities and Exchange Commission, Statement on Cryptocurrencies and Initial Coin Offerings, December 11, 2017. Available at: https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

[9] Financial Conduct Authority, Consumer warning about the risks of Initial Coin Offerings ('ICOs'), 9 December 2017. Available at: https://www.fca.org.uk/news/statements/initial-coin-offerings.

[10] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (S.I. 2017/692), 26 June 2017. Available at: http://www.legislation.gov.uk/uksi/2017/692/made.

[11] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018

Committee recommends that the UK Government either (1) transpose the 5th AML Directive into UK law prior to the UK's planned exit from the EU, or (2) replicate relevant provisions of the 5th AML Directive in UK law as quickly as possible.

II. Regulatory Implementation

The Committee proposes two ways of introducing crypto asset regulation in the UK: (1) by amendment of existing financial services regulation or, (2) by adoption of new regulation tailored specifically to crypto assets.

Amending the existing financial services regulatory framework would involve classifying crypto asset activity as a regulated activity within the Regulated Activities Order. Doing so would enable the FCA to regulate crypto asset activities by, for example, mandating that licenses be obtained in order to carry out specified crypto activities in the UK. This approach has previously been used in the context of peer-to-peer lending,[12] and is regarded as the fastest way of providing the FCA with the powers needed to regulate crypto asset activities and protect UK consumers.

Adopting a new regulatory framework separate from pre-existing financial services rules would allow for a more flexible and tailored approach to crypto asset regulation, but would also require substantially more time to formulate and finalize.

Given the rapid growth of crypto asset markets and the expanding set of risks faced by UK consumers, the Committee recommends that the UK Government regulate crypto asset activities by expanding the scope of the Regulated Activities Order, rather than by adopting a separate body of rules. The Committee also recommends that the UK Government examine the exact type of crypto asset "activity" that would be included in an amended Regulated Activities Order, as well as the ramifications of doing so.

The Committee notes that although the global regulatory response to crypto assets is in early stages, the UK is in a position to learn from the experience of other jurisdictions given the fact that the UK has not yet introduced any specific type of crypto asset regulation. As a result, the Committee encourages UK regulators to engage with their international counterparts in order to ensure that best practices are applied in the UK.

---

amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, p. 43–74. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018L0843.

[12] *See* Financial Conduct Authority, The FCA's regulatory approach to crowdfunding (and similar activities), Consultation Paper 13/13, October 2013. Available at: https://www.fca.org.uk/publication/consultation/cp13-13.pdf.

The European Commission Wants to Reform the World Trade Organization

By Gabriel M. Lentner and Filippo Faccin

On September 18, 2018, the EU Commission issued a concept paper on WTO reform. In this paper, the EU Commission recognizes that the rules-based multilateral trading system faces its deepest crisis since its inception. Against this background, the Commission seeks to move the debate toward a focus on the reform of the WTO.

The concept paper covers 3 issues:

1) Rulemaking and development

2) Regular work and transparency

3) Dispute settlement

Rulemaking and Development

The first proposals in this area concern industrial subsidies and state-owned enterprises (SOEs).

Recognizing the low level of compliance with the Agreement on Subsidies and Countervailing Measures (SCM Agreement) the EU proposes, *inter alia*, the creation of a general rebuttable presumption according to which if a subsidy is not notified or is counter-notified, it would be presumed to be a subsidy or even a subsidy causing serious prejudice.

As regards SOEs, a clarification of what constitutes a public body is proposed that seeks to broaden the existing definition, which, according to the EU Commission does not capture many relevant SOEs. In addition, rules concerning enhanced transparency about the level and degree of state control in SOEs and other market-distorting support are proposed.

Other proposals in this context are concerned with the expansion of the list of prohibited subsidies or the creation of a rebuttable presumption of serious prejudice. Non-insolvent companies without a credible restructuring plan or companies that use dual pricing will no longer have access to grants.

Establishing new rules to address barriers to services and investment, such as in the field of forced technology transfer are another priority.

The Commission also proposes to strengthen the procedural aspects of the WTO's rulemaking activities. It argues that the EU should maintain support for multilateral negotiations and full outcomes in areas where this is possible, and should also explore the feasibility of amending the WTO agreement so as to create a new Annex IV.b. This annex would contain a set of plurilateral agreements that are applied on an MFN-basis and which could be amended through a simplified process.

Furthermore, the EU seeks to strengthen the role of the WTO secretariat in support

of the various negotiation processes as well as the implementation and monitoring functions.

Regular Work and Transparency

The EU has consistently criticized the slow processes and the burdensome bureaucracy of the WTO, which paralyzes its regular work.

The solution that has been proposed is the development of rules that oblige members to provide substantive answers within specific deadlines and the increase of cross-committee coordination on issues related to market access.

The EU Commission concept paper defends the strengthening of the organization's monitoring powers to check whether countries are implementing multilateral agreements and transparent trade policies. In particular, the EU Commission wants the WTO to implement:

1) More effective committee-level monitoring
2) Incentives for improving notification compliance
3) Sanctions for willful and repeated non-compliance
4) Counter-notifications
5) A strengthening of the Trade Policy Review Mechanism (TPRM).

Dispute Settlement

The Commission paper states that the dispute settlement system is "at grave danger, and swift action by members is needed to preserve it".

A solution is necessary to end US blocking new appointments and to prevent the imminent stalemate of the appeal body.

The first stage of a general reform will be a comprehensive amendment of the provision of the Dispute Settlement Understanding (DSU) related to the functioning of the Appellate Body (AB). This amendment would:

- Narrow the 90-day limit to resolve a dispute
- Increase the number of members of the appeal body from 7 to 9 (This would help to increase the efficiency of the appeal body, while improving the geographical balance)
- Configure the membership of the appeal body to work full-time (currently, de jure, it is a part-time job)

Other developments

European Union

Injunctions and Article 15(I) of the E-Commerce Directive: The Pending *Glawischnig-Piesczek v. Facebook Ireland Limited* Preliminary Ruling

By Kletia Noti[1]

Introduction

Under EU law,[2] general monitoring obligations cannot be imposed by Member States upon intermediaries,[3] including hosting services providers.[4] At the same time, specific monitoring obligations are allowed, such as measures ordered *vis-à-vis* intermediaries by national judges in the context of national actions for injunctive relief.[5]

While the ECD does not preclude the granting of injunctions by national courts against a provider of hosting services, it does not precisely define their contours.[6] The compatibility with EU law of specific monitoring obligations contained in

[1]For their useful comments on an earlier draft, the author wishes to thank Dr. Irida Laci Lika, Counsellor, Embassy of the Republic of Albania to Germany; Harold Mousset, Digital Traffic Officer, Planet Parfum, Belgium; and Dr. Nicolo Zingales, Lecturer in Competition & information Law at Sussex Law School, Affiliate Scholar at the Stanford Center for Internet and Society.

[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, Official Journal L 178, 17/07/2000, P. 0001 – 0016 (hereinafter, "ECD"). Articles 12 to 14 ECD tackle the conditions under which intermediary service providers – namely, mere conduits (Article 12), caching (Article 13) and hosting services providers (Article 14) – are not liable for third-party illegal activities or information transmitted through or stored by them.

[3]Article 15(1) of the ECD provides that EU Member States are prohibited from imposing on providers of information society services providers (encompassing mere conduits, caching and hosting services providers) any general obligation to monitor the information which they transmit or store, or actively seek facts or circumstances indicating illegal activity.

[4]Article 14(1) of the ECD provides that hosting services providers can be exempted from liability for illegal activity or information stored at the request of third parties if the following conditions are met: (a) the provider must not have actual knowledge of illegal activity or information and, as regards claims for damages, must not be aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, must act expeditiously to remove or to disable access to the information. Under Article 14(2) ECD, the liability limitation shall not apply when the recipient of the service is acting under the authority or the control of the provider.

[5]Recital 47 of the ECD provides that "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation". Under Recital 48 of the ECD, Member States may require service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

[6] M. H. M. Schellekens, Liability of internet intermediaries: A slippery slope?, 2011, SCRIPTed, 8(2), pages 154-174.

injunctive measures ordered by Member States' national courts *vis-à-vis* intermediaries has led to a number of preliminary rulings before the Court of Justice of the European Union ("CJEU") in the context of third party illegal content consisting of intellectual property rights (IPRs) infringements. When it comes to such types of illegal content, in addition to primary EU law, other IPR-specific secondary EU law provisions provide for the possibility of national courts ordering injunctive relief measures against intermediaries when IPR-infringing content has been transmitted through or stored by third parties.[7] Such provisions have been subject to interpretation by the CJEU in several preliminary rulings.[8] In such rulings, the CJEU has, on the one hand, clarified the circumstances in which injunctions ordered by national judges concerning the implementation of general filtering systems infringe the general monitoring prohibition for EU Member States under Article 15(1) ECD.[9] In addition, the CJEU has also clarified when such filtering systems violate providers' and users' fundamental rights, as enshrined in the Charter of Fundamental Rights of the European Union (hereinafter, "Charter").[10] On the other hand, the CJEU has acknowledged that injunctions aimed at preventing further infringements "of the same kind" are allowed, provided certain conditions are met.[11]

[7]Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (hereinafter, "Enforcement Directive") and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (hereinafter, "Copyright Directive") lay down the possibility for Member States to order injunctions to prevent further infringements.

[8] According to the CJEU, "the jurisdiction conferred on national courts, in accordance with those provisions, must allow them to order those intermediaries to *take measures aimed not only at bringing to an end infringements already committed against intellectual-property rights using their information-society services, but also at preventing further infringements.*" (emphasis added) See Case C-324/09 L'Oréal and Others [2011] ECR I 0000, para. 131, Case C-70/10 Scarlet Extended [2011] ECLI:EU:C:2011:771, para. 31 and Case C-360/10 Sabam v Netlog [2012] 2 C.M.L.R., para. 29. The CJEU has acknowledged that the rules for the operation of such injunctions are a matter of national law (see Case C-324/09 L'Oréal and Others [2011] ECR I 0000, para. 32), subject to the limitations set in those Directives, Article 15 of the ECD (Case C-324/09 L'Oréal and Others [2011] ECR I 0000, para. 35) and primary EU law. Id.

[9]See Case C-70/10 Scarlet Extended [2011] ECLI:EU:C:2011:771, para. 40 (on internet access providers), and C-360/10 Sabam v Netlog [2012] 2 C.M.L.R, para. 38 (on hosting services providers, in particular, an online social networking platform). Also see Case C-484/14 Tobias McFadden v Sony, ECLI:EU:C:2016:689, where an injunction requiring its addressee, an internet access provider, to take measures encompassing examining all communications passing through an internet connection to prevent the recurrence of an infringement of a right related to copyright was considered by the CJEU to violate Article 15(1) ECD: id. at para. 87.

[10]The CJEU carries out a balancing exercise between the fundamental rights at stake. In Scarlet Extended, the CJEU considered the injunction imposed on an access provider as violating the provider's freedom to do business enshrined under Article 16 of the Charter (paras. 47 to 49); it was also found to violate the users' right to protection of their personal data and their freedom of information, enshrined respectively, under Articles 8 and 11 of the Charter (paras. 50 to 52). Such conclusions were also reached in Sabam v Netlog (see paras. 46 to 52). In McFadden, instead, a measure to secure a network was considered not to violate the provider and users' fundamental rights (paras. 99 to 101).

[11]In L'Oréal and Others, the CJEU acknowledged that injunctions aimed at preventing further infringements "of the same kind" (para. 144) can be ordered by national

More recently, at the EU Member State level, various national courts have ordered, *vis-à-vis* intermediaries, injunctions of a broad scope. Such case law developments have prompted doctrinal observations that the ban on general monitoring risks is being corroded.[12] At the same time, recent CJEU case law has interpreted the *L'Oréal* judgment on the scope of "injunctions" used to prevent further infringements as entailing a requirement of double identity of subject matter and agent (i.e., "avoiding new infringements of the same nature by the same market-trader").[13] In the light of such CJEU interpretation, concerns about the compatibility with EU law of monitoring obligations ordered by means of injunctions in several EU Member States may arise[14].

Yet, in the context of illegal content consisting of personality rights' infringements, the CJEU has not tackled the scope of specific monitoring obligations upon hosting services providers. On the other hand, prior rulings of the European Court of Human Rights (ECtHR) have dealt with intermediary liability for third-party illegal content.[15] This has led to uncertainty for national judges concerning the conditions when such obligations are compatible with Article 15(1) ECD.

One example of this uncertainty emerges in the context of the pending preliminary ruling in the matter of *Glawischnig-Pieszczek v Facebook Ireland Limited,*[16] which this article will now analyze. The preliminary questions reached the CJEU due to the Austrian Supreme Court (*Oberster Gerichtshof*) seeking a clarification on the scope of Article 15(1) of the ECD. In particular, the CJEU has been called upon to decide when the jurisdictional reach and scope of monitoring obligations contained in a

judges, and laid down the conditions under which these injunctions are compatible with EU law (see paras. 136 and 138 to 141). It did not specify what "of the same kind" means. See M. Husovec, Injunctions against Intermediaries in the European Union, 2017, Cambridge University Press. In Case C-494/15, Tommy Hilfiger and Others v Delta Center AS, ECLI:EU:C:2016:528, where at stake was an injunction against a physical intermediary, the CJEU narrowly interpreted L'Oréal and Others as allowing injunctions where "the intermediary may be forced to take measures which contribute to avoiding new infringements of the same nature by the same market-trader from taking place". (emphasis added) Id. para 34 and M. Husovec, Injunctions against Intermediaries in the European Union, 2017, Cambridge University Press. See also M. Brüß, Austria refers Facebook hate speech to the CJEU, 30 January 2018, available at: http://ipkitten.blogspot.be/2018/01/austria-refers-facebook-hate-speech.html.

[12]G. F. Frosio, The Death of 'No Monitoring Obligations': A Story of Untameable Monsters, 8 (2017) JIPITEC 199, who observes that: "In multiple jurisdictions, recent case law has imposed proactive monitoring obligations on intermediaries across the entire *spectrum* of intermediary liability subject matters".

[13] See Husovec, *supra,* note 11. Husovec points out that in Case C-494/15, Tommy Hilfiger and Others v Delta Center AS, ECLI:EU:C:2016:528, where at stake was an injunction against a physical intermediary, the CJEU narrowly interpreted *L'Oréal and Others* as allowing injunctions where "the intermediary may be forced to take measures which contribute to avoiding new infringements of the same nature by the same market-trader from taking place". (emphasis added). *Id*. para 34.

[14]See Husovec, *supra,* note 11.

[15]ECtHR's judgment in case 16. 6. 2015 No. 64569/09 [Delfi AS / Estonia] No. 137, ECtHR's judgment in case MTE and Index v Hungary [2016] ECHR 135.

[16]Case C-18/18: Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 10 January 2018 — Eva Glawischnig-Pieszczek v Facebook Ireland Limited. The questions pending before the CJEU were rendered public on 19 March 2018: see OJ C 104, 19.3.2018, p. 21–21.

national injunctive order *vis-à-vis* a hosting services provider in the context of a case involving hate speech against a national politician stored through the hosting provider's services may violate the ban on general monitoring enshrined under Article 15(1) ECD.

This article will now briefly analyze the issues the CJEU is expected to clarify in the current preliminary ruling. Part I recalls the facts underpinning the national proceedings that led the Austrian Supreme Court to refer the matter to the CJEU, seeking a clarification of EU law, and in particular, Article 15(1) ECD. Part II addresses the questions that the CJEU is faced with. First, the article will briefly focus on the extent of the jurisdictional reach of the injunctive orders by national judges. In particular, the CJEU has been asked to clarify whether Article 15(1) of the ECD allows a specific monitoring obligation compelling the hosting services provider to expeditiously remove not simply the reported illegal content, but also "identically worded items of information", or, "information with an equivalent meaning" (i) "globally" or "limited to the relevant Member State" only, regardless of the user who posts it; or (ii) directed against the information uploaded by the specific user having uploaded the illegal content, either limited to the relevant jurisdiction or regardless of where the user is located (**Part II.I**). Part II will also tackle the scope of the monitoring obligations to prevent further future infringements that the pending preliminary ruling is expected to clarify. Indeed, the national court also asks the CJEU to pronounce itself on whether Article 15(1) of the ECD can be interpreted as allowing a monitoring obligation *vis-à-vis* a hosting services provider which requires that hosting services provider to expeditiously remove, in accordance with Article 14(1)(a) of the ECD, not only the illegal information reported to it and identically worded items of information, but also information, differently worded but "of an equivalent meaning". The national court also seeks to know whether Article 15(1) of the ECD prohibits the hosting services provider from removing information of an equivalent meaning to the specifically reported illegal content solely after the hosting service provider is made aware of such information, or whether the hosting services provider is expected to actively seek out and remove such information on its own (**Part II.II**). Part III will draw conclusions.

I. Facts

In April 2016, Eva Glawischnig, Austrian politician and then leader of Die Grünen, the Austrian Green Party, was subjected to offensive comments posted through a fake Facebook account. [17] On July 7, 2016, in a letter addressed to Facebook, Glawischnig asked the company to delete the offensive comments and reveal the real identity and data of the person hiding behind the fake profile. Faced with Facebook's inaction and refusal to remove the posting or provide the identity of the profile user, Glawischnig, backed by the Austrian Green Party, brought an action against Facebook before

[17] The comments posted in the fake profile were insults against the politician, such as "wretched traitor", "corrupt clumsy oaf", "member of a fascist party". The posting also contained a picture of the politician.

the Vienna Commercial Court in autumn 2016.

Plaintiff claimed infringement of her right to the protection of her image, alleging that the posting violated Section 78 of Austrian copyright law. In addition, plaintiff also claimed that the posting violated Article 1330(1) and (2) of the Austrian Civil Code,[18] prohibiting defamation, and asked the court to issue an injunction compelling Facebook to remove the allegedly illegal material from its platform. Defendant argued it was not liable due to, *inter alia,* the application of the hosting services provider safe harbour principle enshrined under Article 16 of the Austrian E-Commerce Law, (transposing Article 14 of the ECD).[19] Defendant also argued that the action should have been brought before courts in Ireland, where Facebook's EU headquarters were, or in the United States, rather than in Austrian courts. In its judgment of December 7, 2016, the Vienna Commercial Court rejected defendant's jurisdiction arguments, upholding that it had jurisdiction over the case. The Vienna Commercial Court also sided with the plaintiff on the substance, considering the hosting service provider to be "an aide to the infringement". According to the court, plaintiff had awareness of the illegality of the comments, considering that, from their context, such illegality was obvious to a non-lawyer without further examination.[20] Therefore, since plaintiff did not expeditiously remove such illegal content, it could not avail of the safe harbour defence enshrined under Article 16 of the Austrian E-Commerce Law. As a remedy, the Vienna Commercial Court ordered a preliminary injunction against Facebook compelling it to remove the illegal content targeting Mrs. Glawischnig.

Only after being served with such injunction did defendant remove the posting within the geographical boundaries of Austria.[21] Mrs. Glawischnig and the Green Party claimed that, since the posting was accessible online from jurisdictions other than Austria, Facebook rendering access to the comments impossible only from Austria was not sufficient to do away with the harm that the posting caused to plaintiff's reputation. The matter reached the Vienna Court of Appeal, which rendered judgment in April 2017. First, similarly to the lower court, the Appeal Court rejected the defendant's claims that the matter should have been brought before Irish or US courts and established jurisdiction upon the defendant. Second, the appeal court agreed with the Vienna Commercial Court on the illegality of the comments, which was obvious to a non-lawyer without further examination, thus meaning that defendant had "awareness" of the illegal content. Indeed, the context

[18] Article 1330 of the Austrian Civil Code (Allgemeines Bürgerliches Gesetzbuch) provides as follows: "(1) Everyone who has suffered material damage or loss of profit because of an insult may claim compensation. (2) The same applies if anyone disseminates statements of fact which jeopardise another person's credit, income or livelihood and if the untruth of the statement was known or must have been known to him. In such a case the public retraction of the statement may also be requested (…)".

[19] Federal Act governing certain legal aspects of electronic commercial and legal transactions (E-Commerce Act) [E-Commerce-Gesetz] (ECG), January 1, 2002, which incorporates the ECD safe harbours into Austrian national law.

[20] It is worth recalling that, in Austria, courts have construed "awareness" or "knowledge" of the illegal material as "illegality being obvious to a non-lawyer without further examination."

[21] Vienna Commercial Court, judgment of 7 December 2016 in case 11 CG 65/16 w – 17.

showed that the comments contained excessive and violent wording that went beyond permissible political debate. Hence, the Appeal Court also upheld the lower court's finding that the hosting services provider was not covered by the safe harbour defense since it failed to expeditiously remove the posting after having become aware of it. Therefore, it considered Facebook to be an aide to the infringement.

The Vienna Court of Appeal ordered Facebook to remove – worldwide – both the posting at issue and all postings identical to it, but not necessarily similar ones.[22] One of the arguments Facebook raised was that, under Article 18(1) of the Austrian E-Commerce Act, which transposes Article 15 ECD, it could not be required to undertake *ex ante* monitoring. In this respect, the Appeal Court first recalled the prior jurisprudence of the Austrian Supreme Court concerning personality rights' infringements.[23] The Vienna Court of Appeal acknowledged that a balancing exercise must be carried out between the fundamental freedom of expression, on the one hand, and the right to one's honour and reputation, on the other hand. The Court held that when the duty to monitor only covers identical comments, even when worldwide, such an obligation is not tantamount to an *ex ante* general monitoring obligation; therefore, it is not prohibited under Article 18(1) of the Austrian E-Commerce Act and Article 15(1) of the ECD. Indeed, the Vienna Court of Appeal concluded that imposing such an obligation upon defendant was reasonable. In this respect, the Court made reference to the automatic tools that Facebook has to ensure removal of comments which are identical to the notified comment. By contrast, according to the Vienna Court of Appeal, compelling Facebook to remove similar postings to the notified content would have been an unreasonable burden for the hosting services provider. Unlike for identical comments, such an assessment could not be carried out via an automatic tool. Therefore, the Vienna Court of Appeal concluded that for comments similar in meaning to the notified comment, the harmed party must each time submit a notice to the hosting services provider asking it to remove this content.

Both parties appealed the Vienna Court of Appeal's judgment before the Austrian Supreme Court. In its judgment on October 25, 2017,[24] the Supreme Court recalled its previous case law concerning personality rights' infringements. In such case law, the Supreme Court considered that a balancing act must be carried out between the conflicting fundamental rights of freedom of expression, on the one hand, and the right to a person's honor and reputation, on the other. It considered that, if an operator has been informed by a user of an infringement and there is a concrete risk of further violations, the defendant's "special duty to take measures to prevent the infringement from continuing is reasonable". The Austrian Supreme Court went on to highlight that this special duty has been interpreted by Austrian courts, in

[22] OLG Wien Court of Appeal, Az.: 5 R 5/17t, 26.04.2017.

[23] Austrian Supreme Court, case 178/04a, Zankl, ECG² [2016] Rz 265. According to the Supreme Court, an injunction imposing upon a hosting services provider – in this case a blog – the obligation to continuously monitor newly posted comments following an infringement was reasonable and did not infringe Article 18 of the E-Commerce Act.

[24] OGH, case number 6Ob116/17b, decision of 25 October 2017.

the context of personality rights' violations, as requiring the hosting services provider to remove content similar in meaning to the identified content and not merely content identical to it.[25]

The Austrian Supreme Court opined that whether the imposition of such a monitoring obligation with regard to a personality rights violation is compatible with Article 15 (1) of the ECD (see, in detail, Hoffmann in Spindler / Schuster, Electronic Media Law [2015] § 7 TMG Rz 36 ff) was not *acte clair* under EU law.[26] Therefore, deeming an interpretation of Article 15(1) of the ECD to be necessary to reach a conclusion, the Austrian Supreme Court stayed proceedings and asked the CJEU to answer the following questions[27]:

"1. Does Article 15(1) of 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 ('Directive on electronic commerce') (1) generally preclude any of the obligations listed below of a host provider which has not expeditiously removed illegal information, specifically not just this illegal information within the meaning of Article 14(1)(a) of the Directive, but also other identically worded items of information:

a. worldwide?

b. in the relevant Member State?

c. of the relevant user worldwide?

d. of the relevant user in the relevant Member State?

2. In so far as Question 1 is answered in the negative: does this also apply in each case for information with an equivalent meaning?

3. Does this also apply for information with an equivalent meaning as soon as the operator has become aware of this circumstance?"

II. Implications of the pending judgment

II.I The jurisdictional issue

The first clarification sought by the CJEU concerns the jurisdictional scope of the national injunctive relief order allowed under Article 15 of the ECD.

In particular, the CJEU is asked to clarify whether an injunction containing a specific monitoring obligation compelling the hosting services provider to remove not simply the reported illegal content, but also "identically worded items of information" without violating Article 15 ECD: (i) of "global reach" or "limited to the relevant Member State" only, regardless of the user who posts it; or (ii) directed against the

[25] Austrian Supreme Court, case 178/04a, Zankl, ECG² [2016] Rz 265, *supra,* note 22.
[26] Id. At the same time, the Austrian Supreme Court considered case C-484/14, McFadden v Sony, not to be applicable since it concerned an access provider, and recalled the Sabam v Netlog, Scarlet Extended and L'Oréal and Others CJEU judgments. Interestingly, the Supreme Court also considered that the applicant had acknowledged the non-active nature of the intermediary. The CJEU also cited Article 8 ECHR and the ECtHR's judgment in case 16. 6. 2015 No. 64569/09 [Delfi AS / Estonia] No. 137.
[27] Case C-18/18, *supra*, note 16, OJ C 104, 19.3.2018, p. 21.

information uploaded by the specific user having uploaded the illegal content, either limited to the relevant jurisdiction or regardless of where the user is located. Further, the CJEU is asked to pronounce itself whether Article 15(1) ECD does not preclude the above, does this also apply in each case when "information with an equivalent meaning" is at stake.

As explained above, the Vienna Court of Appeal considered a global order to remove not only the complained about content but also items of information identical to such content not to violate the ban on general monitoring under Article 18 of the Austrian E-Commerce Act. It remains to be seen whether the CJEU will agree with such conclusions.

The pending questions before the CJEU exemplify the challenge that the Internet represents for private international law.[28] The CJEU is called upon to shed light on whether a domestic court enjoining activity on the Internet globally complies with the ECD, and in particular, Article 15 thereof.

Article 15(1) of the ECD has as its *rationale* the upholding of fundamental freedoms protected by the Charter (including freedom of expression and information[29]) and the European Convention of Human Rights.[30] In this respect, the ECtHR has clarified that "justified and proportionate restrictions" upon freedom of speech can be imposed by the ECHR signatory States.[31] At the same time, the CJEU has also considered that "where several fundamental rights are at issue, the Member States must, when transposing a directive, ensure that they rely on an interpretation of the directive which allows a fair balance to be struck between the applicable fundamental rights protected by the European Union legal order. Then, when implementing the measures transposing that directive, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with that directive but *also ensure that they do not rely on an interpretation of it which would be in conflict with those fundamental rights or with the other general principles of EU law, such as the principle of proportionality*".[32] (emphasis added)

Against this background, this article will briefly mention some developments concerning both Member State and extra-EU case law. It will additionally refer to some pending EU preliminary rulings where injunctions of global reach *vis-à-vis* search engines have been at stake in the context of the "right to be forgotten" (**II.I.I**).

Subsequently, the article will analyse whether, given the territoriality of defamation laws (and in general, personality rights' infringement laws), a conflict of laws argument can prevent the upholding of an injunction of global reach. In the past, this argument has been used by non-EU courts to deny global orders. (**II.I.II**)

II.I.I Case law involving injunctions of global reach in national Member States, in

[28] M. Douglas, A global injunction against Google, 2018, 134 (Apr),The Law Quarterly Review 181.
[29] Article 17 of the Charter.
[30] Article 10 of the ECHR.
[31] See Delfi AS v. Estonia (2015) ECtHR 64669/09, Grand Chambers judgment.
[32] Case C-314/12, UPC Telekabel Wien, ECLI:EU:C:2014:192, para. 46.

the EU and outside the EU

The below case law concerns de-listing or blocking of access to illegal content, rather than injunctions to remove content. However, since their jurisdictional scope is at stake, they will be briefly referred at.

A. EU Member State case law: the *Max Mosley v Google* saga

As the saga of *Max Mosley v Google* shows, injunctions of global reach against intermediary services providers are not a novel issue in Member State case law.

In 2008, a prostitute took video footage of Mosley, a UK individual, on a concealed camera provided to her by a journalist of News of the World while he was engaged in private sexual activity in a flat in Chelsea. Images from the footage were published prominently in the News of the World newspaper and on its website in 2008. Mosley sued the newspaper[33] and brought the matter before the European Court of Human Rights.[34] He also argued that the posting of the images, which were uploaded on websites accessible by search engines on the internet, violated his right to privacy. Therefore, Mosley brought proceedings in various jurisdictions in an effort to get Google to block access to the photos from its search results.

The case reached courts in various EU Member States. In France[35] and Germany,[36] the issue of their compatibility with Article 15(1) ECD did not arise. In the United Kingdom, the court considered whether the monitoring and screening obligations imposed upon Google by the national judges could violate Article 15(1) ECD, but did not conclude whether this was the case [37]

More specifically, in France, Google was ordered to remove the nine photos and, furthermore, to ensure they would not be displayed for five years on its engine worldwide (including on the domain google.com) under penalty of € 1,000 per day of delay.[38]

In Germany, the Landgericht Berlin concluded that Google's publication of the images clearly violated Mosley's privacy rights and, furthermore, that Google had not been responsive to the "notice and takedown" attempts made for four years by Mosley's attorneys. Since Google knew that the images were defamatory, the Landgericht Berlin argued that the company had "a duty to take all reasonable steps to prevent future defamation".[39] Such steps could include developing software that would "delete and detect or block such content", which Mosley showed that Google could develop. The court noted that the use of this kind of software would not violate European or German national law.

[33] Mosley v News Group Newspapers [2008] EWHC 1777 (QB).
[34] Judgment by the European Court of Human Rights (Fourth Section), case of Mosley v. United Kingdom, No. 48009/08 of 10 May 2011.
[35] Case No. 11/07970, Tribunal de Grand Instance de Paris, decision of November 6, 2013.
[36] Hamburg District Court, 324 O 264/11, 24 January 2014, Max Mosley/Google.
[37] Max Mosley v. Google, [2015] EWHC 59 (QB).
[38] Case No. 11/07970, Tribunal de Grand Instance de Paris, decision of November 6, 2013.
[39] Hamburg District Court, 324 O 264/11, 24 January 2014, Max Mosley/Google. Also see LG Hamburg Google judgment, available at: https://globalfreedomofexpression.columbia.edu/cases/lg-hamburg-google-judgment/

Google's defense that the existing software could not reach such a wide scope was rejected,[40] and Google's concerns that this could lead to over-removal were considered as not sufficiently demonstrated.

In the United Kingdom, Mr. Justice Mitting, who wrote the opinion on behalf of the majority, clarified that injunctions encompassing the prevention of further infringements "of that kind", provided that they are "effective, proportionate, dissuasive and do not create barriers to trade"[41] can be employed in upholding the rights of individuals to have sensitive personal information lawfully processed. The judge concluded that "the evidence which I have is not such as to permit a judgment to be made on whether or not the steps required by the claimant would involve monitoring in breach of Article 15(1) of the E-Commerce Directive".[42] According to him, it was "common ground that existing technology permits Google, without disproportionate effort or expense, to block access to individual images", similarly to what it can do with child sexual abuse imagery. Hence, according to Justice Mitting, the evidence "may well satisfy a trial judge that it can be done without impermissible monitoring."[43] The judge did not explicitly express himself whether such monitoring would comply with the ECD, and considered the claim to be "viable".

However, unlike in the current case, at stake was imagery and, furthermore, only the images that the plaintiff had notified Google about.

In the current case, instead, text-based content filters are involved. Their accuracy, as doctrine points out, is questionable.[44]

B. Case law pending before the CJEU: the pending *Google v Commission nationale de l'informatique et des libertés* (CNIL) preliminary ruling and jurisdictional issues in the context of the "right to be forgotten"

Jurisdictional issues in the context of privacy matters are not novel to EU law either. Indeed, another preliminary ruling is pending before the CJEU. That case concerns the jurisdictional reach of an order to de-list certain results that violate a judge-made creation, the "right to be forgotten"[45], currently codified in EU law under the General Data Protection Regulation.[46]

In particular, as a result of the reference lodged by the French *Conseil d'État* on

[40] For a criticism that this is an example of erosion of the no monitoring obligation, see Frosio, Giancarlo, From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe (March 1, 2017), 12 Oxford Journal of Intellectual Property and Practice 565 (2017); Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2017-05, available at SSRN: https://ssrn.com/abstract=3009156 or http://dx.doi.org/10.2139/ssrn.3009156

[41] See Max Mosley v. Google, [2015] EWHC 59 (QB), para. 52, citing L'Oréal v eBay, para. 144.

[42] Max Mosley v. Google, [2015] EWHC 59 (QB), para. 53.

[43] Id., para. 54.

[44] D. Keller, Twitter, 24 May 2018, Oh, man. Text-based content filters fail again, available at: https://twitter.com/daphnehk/status/999819966697259008

[45] Case C-131/12, Google Spain and Google.

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88.

August 21, 2017, the CJEU is now faced with the question whether the 'right to de-referencing', as established by the CJEU in its judgment of May 13, 2014 in case C-131/12, Google Spain and Google, requires Google to globally de-list search results that violate French privacy laws.[47]

The case concerns a dispute between the French privacy watchdog, *Commission nationale de l'informatique et des libertés* (CNIL) and Google. The matter reached the French Supreme Administrative Court further to Google's challenge of an order issued by the CNIL requiring Google to de-list certain articles from its search results on Google domains worldwide. CNIL argued that, in order to be effective, the de-listing must be carried out on all extensions of the search engine. Google argued that each jurisdiction should be able to determine what information can be accessed by its citizens online, and that there must be a balance between people's right to privacy and freedom of expression.

Doctrine provides several arguments why a global implementation can be problematic.[48] Indeed, global implementation is "arguably the most contentious from the perspective of public international law, as it implies the greatest interference with the territorial sovereignty of other States".[49] Because of this concern, case law in various EU Member States supports geographic filtering.

In 2016, Google also started de-listing results across all its domains, including Google.com, when accessed from the country where the request came from, thus upholding the geographic filtering mechanism that some doctrine advocates for as striking the right balance; geographic filtering has now become standard practice.[50]

The CJEU is not expected to issue a ruling before 2019.

C. Non-EU case law: Global de-listing orders against innocent third parties

The judicial approach favouring global injunctions finds a precedent in the context of the Canadian *Google v Equustek* ruling.[51] In this ruling, Canada's Supreme Court upheld a British Columbia court ruling that ordered Google to de-list entire domains and websites from its global search index. Google's arguments that the order violated the principle of comity and users' freedom of expression were rejected by the national court as merely theoretical.

[47] Pending preliminary ruling before the CJEU in Case C-507/17 Google Inc. v Commission nationale de l'informatique et des libertés (CNIL).

[48] B. van Alsenoy, and K. Marieke, The Extra-Territorial Reach of the EU's 'Right to Be Forgotten', CiTiP Working Paper 20/2015, Available at SSRN: https://ssrn.com/abstract=2551838, pages 22-24, and Fomperosa Rivero, Álvaro, Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality, Stanford-Vienna European Union Law Working Paper No. 19 (2017), available at SSRN: https://ssrn.com/abstract=2916608 or http://dx.doi.org/10.2139/ssrn.2916608. But see, *a contrario,* Frosio, Giancarlo, Right to Be Forgotten: Much Ado About Nothing (January 31, 2017). 15(2) Colorado Technology Law Journal 307 (2017). Available at SSRN: https://ssrn.com/abstract=2908993.

[49] B. van Alsenoy, and K. Marieke, note 52, page 22.

[50] G. Vermeulen, E. Lievens, Data Protection and Privacy under Pressure. Translantic tensions, EU surveillance and big data, 2017, Maklu Press.

[51] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, [2017] 1 S.C.R. 824.

The ruling has been criticised, mostly in the US. In particular, authoritative scholars[52] and several platforms[53] have argued against the extra-territorial application of the injunction upheld by the Canadian Supreme Court. This doctrine has highlighted how such rulings could clash with fundamental rights, namely users' fundamental freedom of expression and information.[54] In light of the global nature of the Internet, the argument goes, this could lead to authoritarian regimes also enforcing their laws beyond their territory; in turn, this would render it impossible for the rest of the world to learn about the human rights' violations of such regimes.

In a nutshell, injunctions of a global reach ordered by a national court could launch a race to the bottom, whereby countries with different values than the democratic world would enact stricter rules that could, in turn, jeopardise online freedom of expression.[55] The view is, however, not shared by all, with some authors arguing that the Google v Equustek precedent does not jeopardise freedom of speech online.[56]

Recently, an Australian court has acknowledged that its jurisdiction *ad personam* upon defendant, Twitter,[57] has a global reach. Many authors have also criticized this outcome.[58]

II.I.II Implications for the current pending preliminary ruling

Much has been written on the actions to be undertaken by social media platforms to combat and prevent hate speech or fake news. This analysis does not tackle these points.

The several separate, but intertwined, questions are:

1. Can national courts apply their law injunctions ordering the removal of content

[52] Arguing against injunctions of extra-jurisdictional scope since they could constitute serious rule of law issues and give rise to concerns about respect for freedom of speech should they be ordered by an authoritarian jurisdiction; insofar as the Google v Equustek Canadian Supreme Court ruling (2017 SCC 34) is concerned, see A. Katz, Google v Equustek: Unnecessarily Hard Cases Make Unnecessarily Bad Law, June 29, 2017, available at https://arielkatz.org/google-v-equustek-unnecessarily-hard-cases-make-unnecessarily-bad-law/ and D. Keller, Ominous: Canadian Court orders Google to remove search results globally, 28 June 2017, available at: http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally.

[53] I. Fashola, Facebook, Microsoft Say Content Laws Should Stay Local, 7 March 2018, available at: https://esq-law.com/facebook-microsoft-say-content-laws-should-stay-local/

[54] See Keller, *supra,* note 57.

[55] See Keller, *supra,* note 57 and Kent Walker, A Principle That Should Not Be Forgotten, Google In Europe (May 16, 2016), https://www.blog.google/topics/google-europe/a-principle-that-should-not-be-forgotten/.

[56] See, for an opinion that the Court in Equustek struck the right balance, Neil Turkewitz, Why the Canadian Supreme Court's Equustek decision is a good thing for freedom — even on the Internet, 8 July 2017, available at: https://laweconcenter.org/resource/why-the-canadian-supreme-courts-equustek-decision-is-a-good-thing-for-freedom-even-on-the-internet/, B. Sookman, Worldwide de-indexing order against Google upheld by Supreme Court of Canada, 29 June 2017, available at: https://www.mccarthy.ca/en/insights/blogs/snipits/worldwide-de-indexing-order-against-google-upheld-supreme-court-canada.

[57] [2017] NSWSC 1300 X v Twitter.

[58] G. Van Calster, Global Twinjunctions. X v Twitter, 10 October 2017, available at: https://gavclaw.com/2017/10/10/global-twinjunctions-x-v-twitter/ and M. Douglas, The Exorbitant Injunction in X v Twitter [2017] NSWSC 1300.

– illegal in their jurisdiction - extra-territorially?

2. To what extent does this impinge upon the provider's freedom to conduct a business, recognized by the Charter of Fundamental Rights of the European Union?[59]

3. To what extent does this impact users' freedom to impart information, recognized by the Charter and the ECHR and acknowledged by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression?

In short, there are many grey areas and freedom of expression concerns that such ruling is expected to clarify.

In soft law EU-wide documents (such as the Code of conduct on countering illegal hate speech online), a definition of "illegal hate speech" is provided with reference to the Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law and national laws.[60] The argument that the plaintiff made in the Austrian proceedings was that the content posted was defamatory; some authors have also framed the illegal content as "fake news",[61] since it contained an untruthful statement about the politician.

It is worth recalling that Framework Decisions concerning the EU's competence in police and judicial cooperation in criminal proceedings did not go far toward harmonising Member States' laws on defamation. Laws tackling personality rights' infringements are territorial.

In the Austrian proceedings that gave rise to the preliminary ruling, the facts of the case were content (and jurisdiction) specific. It is worth clarifying that the Austrian judges – both the Vienna Commercial Court and the Vienna Court of Appeal – considered the content at stake to violate, *inter alia,* Article 1330(1) and (2) of the Austrian Civil Code. Such provisions allow victims of defamation to be compensated for the damages suffered as a result of insults.

Indeed, "hate speech" in Austria or Germany may not have the same scope (as interpreted by the case law) as in other jurisdictions. An extraterritorial application of the injunction could mean that conflicts of laws may occur, especially when the scope of the specific monitoring obligation is not limited to "wording" identical to the content at issue. In this case, content may erroneously be taken down. This may lead to legal uncertainty for the cross-jurisdictional operations of the hosting services provider and may have an impact on the providers' freedom to conduct a business.[62] In addition, as the CJEU has held, the providers' freedom to provide to society information services must be taken into account: albeit with respect to another ECD provision, the CJEU has held that while the ECD does not create a choice of

[59] Article 16 of the Charter.

[60] Under this Framework Decision "illegal hate speech" means "all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin".

[61] K. Niklewicz: Weeding out Fake News: An Approach to Social Media Regulation, Brussels, Wilfried Martens Centre for European Studies, 2017.

[62] See case law cited *supra,* note 9.

law rule, and host Member States "are in principle free to designate, pursuant to their private international law, the substantive rules which are applicable", this must not result in a "restriction of the freedom to provide electronic commerce services."[63]

However, extra-EU courts where the global reach of an injunction has been accepted are not satisfied with a conflict of laws argument being raised by a defendant in the abstract.[64] At the same time, a conflict of laws argument has led non-EU courts to actually use their discretion to reject injunctions of reach beyond the jurisdiction of the court.[65]

While in the facts of the Austrian case, the comments were obviously illegal, there may be other grey areas where, in order to assess illegality, context matters, and where, as such, cross-border removal of similarly worded content may entail legal uncertainty for the intermediary.[66]

Some recent case law illustrates the difficulties intermediaries face should they take down content that is later found to be legal by a national judge. For example, in April 2018, a German court (Berlin Regional District Court) issued a preliminary injunction against Facebook arguing that Facebook had acted unlawfully by deleting a user's comment on the grounds of an alleged breach of its Terms of Service.[67] Earlier in 2018, Facebook had blocked the user, identified only as Gabor B., and deleted his posting on the platform – a comment under a newspaper article that questioned Germany's practice of aiding the influx of refugees in Europe. After the user complained, the account was unblocked but the user's posting was not, on the grounds that it violated the Terms of Service the user had agreed to. The user sought a preliminary injunction against the intermediary. According to scholar Christina Etteldorf, "since such proceedings include a weighing up of the opposing interests of both the applicant and the respondent, taking into account the lawfulness or otherwise of the disputed measure, the ruling at least suggests that the court found that there was at least a possibility that the deletion of the comment had been illegal and that, in any case, the user's interests were predominant."[68] Namely, the court itself tempered the

[63]See CJEU Judgment in Joined Cases C-509/09 and C-161/10, eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited, ECLI:EU:C:2011:685, para. 62: "Secondly, Article 3(2) of the Directive prohibits Member States from restricting, for reasons falling within the coordinated field, the freedom to provide information society services from another Member State. By contrast, it is apparent from Article 1(4) of the Directive, read in the light of recital 23 in the preamble thereto, that host Member States are in principle free to designate, pursuant to their private international law, the substantive rules which are applicable so long as this does not result in a restriction of the freedom to provide electronic commerce services."

[64]See Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, [2017] 1 S.C.R. 824.

[65]Macquarie Bank Limited and Anor v Berg [1999] NSWSC 526 (2 June 1999). See also M. Douglas, The Exorbitant Injunction in X v Twitter [2017] NSWSC 1300.

[66] See Opinion of Advocate General Szpunar in Case C-484/14 Tobias McFadden v Sony, ECLI:EU:C:2016:170, para. 118.

[67] LG Berlin 31 O 21/18.

[68]Christina Etteldorf, Facebook should not have deleted content, available at: https://merlin.obs.coe.int/iris/2018/6/article12.en.html.

application of the Act to Improve Enforcement of the Law in Social Networks NetzDG[69].

Indeed, in the national proceedings leading to the current preliminary ruling, the Vienna Court of Appeal accepted that the content at stake was illegal hate speech based on the context. According to this Court, the wording contained insults which entailed violence and did not stay within the limits of reasonable political debate. Therefore, the posting violated specific provisions of the Austrian Civil Code,[70] causing damage to the politician. The Austrian Supreme Court recognized these comments' illegal character. While it could be argued that the underlying facts of this case point to the content being obviously illegal in Austria, what is "obviously illegal" is not defined under the ECD. In addition, in the context of personality rights infringements, there may well be areas where assessing the illegality of the content is more complex than in the current Austrian dispute, or where the harmed party is not precisely defined. For example, content may still be illegal, even if there is no individually injured party.

The abovementioned Facebook case in Germany exemplifies the freedom of expression concerns at stake in defamatory speech cases due to the risk of over-removal, which in turn touches upon users' fundamental rights of information. In that case, Facebook had considered the content to be in violation of its Terms of Service, but the court did not agree with this assessment.[71]

II.I.II.I. May the territorial scope of defamation laws lead to conflict of law considerations for the CJEU?

It may be argued, as the Austrian Supreme Court did in its referral, that courts' divergent approaches may benefit from a clarification by the CJEU. At the same time, an injunction that includes the worldwide removal of information that is similar in meaning to the content already found illegal means that a conflict of laws issue is not merely hypothetical.[72]

This circumstance renders the current case different from the abovementioned *Google v Equustek* case. In that case, Google's argument that a global injunction would violate international comity, or that to comply with it would result in Google violating the laws of a foreign jurisdiction, was rejected as merely abstract. The Canadian Supreme Court still went on to accept that a balance of the factors required the search engine to de-list certain results from its search engine globally. According to that court, a global injunction against Google (a non-party to the infringement) was necessary to provide plaintiff with an effective remedy in equity. Additionally, that court opined that IPRs should be protected across other jurisdictions. The majority of the judges did not ask whether Equustek was, as a matter of Canadian law, entitled to the injunction it

[69] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG), available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

[70] See § 1330 Abs 1 of the Austrian Civil Code.

[71] See Christina Etteldorf, note 74.

[72] See, for an article concerning conflict of laws in IPRs infringements in the context of intermediaries' liability, P.A. De Miguel, "Internet Intermediaries and the Law Applicable to Intellectual Property Infringements", JIPITEC, 2012.

sought;[73] additionally, the territorial nature of trademark law was not sufficiently addressed by the Canadian judges.[74] Finally, Equustek's IPRs rights were not global in scope[75].

Likewise, personality rights' infringements are territorial. Requiring the hosting services provider to remove content which is equivalent in meaning to the illegal content beyond the jurisdiction in question would force it to make a judgment call as to whether this content would even be a violation of the law elsewhere. If a doubt exists, will the platform – to prevent such an injunction from being ordered – err on the side of caution and remove the content? To what extent may this have a negative repercussion on users' freedom of expression and information?[76]

Additionally, how can the platform comply with such an injunction without this inquiry also entailing *ex ante* filtering (if the judge answers Question 2 in the affirmative)? Would this injunction abide by the principle of proportionality, one of the principles enshrined in primary EU law? What about about the inaccuracy of content-based filters?[77]

In conclusion, laws tackling personality rights have a territorial nature. In the past, this has prompted non-EU courts to argue against global injunctions. It remains to be seen how the CJEU will tackle the issue of territoriality.

II.II. The scope issue

The pending preliminary ruling presents the CJEU with the possibility of determining to what extent a national order asking a hosting services provider to find and remove postings "with an equivalent meaning" to the posting at issue or to carry out the removal of such postings upon become aware of them, would be compatible with EU law and the ECD.

In this respect, the CJEU will be faced with a delicate balancing of fundamental rights (freedom of expression and freedom to do business for the hosting services provider), on the one hand, and fighting illegal content (in the specific case, hate speech), on the other.[78]

The thorny question becomes whether the platform (in this case, Facebook) needs to actively look for posts with an equivalent meaning to the reported content, instead of just reposts that are identical to such content. In the original language of the preliminary questions, the German wording for "information with an equivalent meaning" is "sinngleiche" which is composed of two parts: "sinn" which can be translated as "meaning" and "gleiche" which can be translated as "of the same". Therefore, while the official English

[73] See Katz, *supra,* note 57.
[74] Id.
[75]See R. Stobbe, Canada's Top Court and the Google Injunction, 26 October 2017, available at: http://www.ipblog.ca/?p=1406
[76] Namely, illegal content does have a territorial nature (in that it violates the laws of the territory) and, as D. Keller opines, when a global injunction is ordered by a judge in a country where content is illegal in the jurisdiction as defined under laws of the state, this clashes with values of democracy and freedom of speech. See D. Keller, note 57.
[77] D. Keller, note 57.
[78] See M.Schmid, "CJEU hate speech case: Should Facebook process more personal data?", 24 January, 2018, available at: https://edri.org/cjeu-hate-speech-case-should-facebook-process-more-personal-data/.

translation on the CJEU's website refers to content "of equivalent meaning", the German wording appears to be broader than its English translation. Indeed, the German wording encompasses information of "the same meaning" as the content that has been reported. Much like in *L'Oréal v eBay*, where the court declined to specify the meaning of "of the same kind", the CJEU is here faced with clarifying how far the scope of the injunction can go before it violates the ECD's ban on general monitoring.

The bulk of the commentary below will concern this question. The privacy-related implications of such clarification will not be tackled.[79] The scope of the debate will be narrowed down to the *rationae materiae* scope of the injunction, in relation to which a clarification is sought before the CJEU.

First, a pending issue is whether the judgment may have repercussions beyond the specific context of the illegal content at stake. In other words, it may also touch upon other types of illegal content (such as IPR-based infringements); this is in the light of the CJEU's express reference to "infringements of the same kind" in *L'Oréal v eBay* (**II.II.I**). Second, it is also necessary to analyse the extent to which the CJEU will take into account its own precedent (**II.II.I**).

II.II.I A welcome clarification of *L'Oréal v eBay* or a content-specific ruling?

It is worth recalling, again, that in *L'Oréal v eBay* the CJEU did not say what it meant by the wording "of the same kind."[80] Advocate General Jääskinen opined that injunctions to prevent further infringements are compatible with EU law only when they are directed against the same party and in relation to the same infringement.[81] However, the CJEU did neither follow his view in *L'Oréal v eBay* nor did it clarify, in its subsequent case law, what "of the same kind" means exactly. It also neglected to make this clarification in the *Tommy Hilfiger* ruling, where the CJEU interpreted *L'Oréal* as allowing injunctions "which contribute to avoiding new infringements of the same nature by the same market-trader from taking place".

It is also worth recalling that, in contrast to the current matter, both those judgments concerned orders against online (in *L'Oréal*, the eBay marketplace) or offline (in *Tommy Hilfiger*, Delta *a.s.*) intermediaries in the context of IPRs violations by third party users.

The CJEU is now asked to pronounce whether an injunction which covers the prohibition of information "equivalent in meaning" is compatible with the ECD, or whether EU law only allows injunctions which require the hosting services provider to prevent content which is "identical in wording" to the posting at issue. In its decision to refer the matter to the CJEU, the Austrian Supreme Court mentions *L'Oréal v eBay*, and it presumably considers such ruling as not providing a

[79] For an overview, see Schmid, note 85.
[80] M. Husovec, *supra,* note 11.
[81] In L'Oréal v eBay, AG Jääskinen said that: "EU law does not go so far so as to require the possibility of issuing an injunction against an infringer so as to prevent further infringements which might take place in the future" and opined that a sufficient safeguard is a double requirement of identity (same party and same IP infringement). See Advocate General Jääskinen's Opinion of 9 December 2010 in C-324/09 *L'Oréal/eBay.*

clear answer to the question before it.[82] It also recalls that the *L'Oréal* ruling concerned the scope of injunctions ordered under the Enforcement Directive, and another type of content, a trademark infringement[83].

When it comes to illegal content which constitutes a breach of personality rights, as seen above, the CJEU has not yet clarified the scope of the specific monitoring obligations allowed under EU law.

Under this lens, some authors argue that the current judgment may be a welcome clarification of previous case law and may have repercussions beyond the specific type of illegal content at stake, including intellectual property law infringement ramifications.[84]

It remains to be seen whether the CJEU will consider a clarification of *L'Oréal v eBay* to be necessary, or whether the court will frame the issue in more content-specific terms.

It appears that the way the questions are drafted suggests that only text-based illegal content that amounts to a violation of a user's personality rights will be caught by the clarification. While, in its request, the Austrian Supreme Court cites the ECtHR's judgment in *Delfi v Estonia*, a case concerning defamation, the questions asked to the CJEU do not specifically mention personality rights' infringements. The Austrian Supreme Court merely speaks about "other identically worded items of information" or "information with an equivalent meaning". If the court decides to further clarify *L'Oréal v eBay*, it will likely be in the form of the CJEU giving criterion to national courts by which they can judge whether their injunctions are ECD-compliant. In such a case, it remains to be seen what standard, applicable across various types of illegal content, will be given by the CJEU. Again, this possibility is remote. It is much more likely that the ruling will instead deal only with the specific type of illegal content at hand.

II.II.II Does an injunction to remove postings with "equivalent meaning" require filtering of all content stored? The *Scarlet* and the *Sabam/Netlog* CJEU rulings

Were the CJEU to accept that Article 15(1) of the ECD allows injunctions imposing on the intermediary an obligation to remove illegal content also encompassing "information with an equivalent meaning", it is unclear how this can be done without filtering all content stored (including legal and illegal content). In the Code of Conduct on countering illegal online hate speech, the adhering platforms commit "to review the majority of valid notifications for

[82] In particular, in L'Oréal v eBay, the CJEU has considered that the intermediary may not be required to "exercise general and permanent oversight over its customers".

[83] Under Article 11 of the Enforcement Directive: "Member States shall ensure that, where a judicial decision is taken finding an infringement of intellectual property rights, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rights-holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC."

[84] See Brüß, *supra*, note 11.

removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary". At the same time, the Code does not specify whether the scope of such removal or disabling of access should also stretch to include content "equivalent in meaning" to the content reported. Is this because "equivalence" is in the eyes of the beholder? Are there tools in place that allow such an obligation to be carried out? How should companies deal with the risk of 'false positives'?

On the one hand, platforms must not see the hosting services liability safe harbour principle enshrined under the ECD as a means to shield themselves from their responsibility to combat the spread of hateful speech and other pernicious illegal content on the web. Content that has been re-phrased can still be in violation of the personality rights of individuals. Would it be too cumbersome to ask the injured party to report it again? Must the platform seek out such content actively or need it only wait to gain awareness of such content before taking action?[85]

When addressing the issue of scope, the CJEU must also take into account its prior jurisprudence, even though it mainly deals with other types of illegal content, namely copyright infringements.[86] According to past case law, an injunction imposed on the hosting service provider requiring it to install the contested filtering system – a system that requires filtering of information which is stored on its servers by its service users;– which applies indiscriminately to all of those users;– as a preventative measure;– exclusively at the hosting services provider expense; and– for an unlimited period – would oblige "it to actively monitor almost all the data relating to all of its service users in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the hosting service provider to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31 (see, by analogy, Scarlet Extended, paragraph 40)".[87]

Were the CJEU to interpret the injunctive order as also encompassing information that is equivalent in meaning to the reported content, the concerns raised by the Austrian Supreme Court are justified. Were the *Netlog/Sabam* judgment clear on the matter, there would have been no need for the Austrian Supreme Court to refer the matter to the CJEU. Some scholars argue that an expansion of the injunction to also encompass content which is similar in meaning – and the requirement to actively look for such content – would risk contradicting the abovementioned case law precedent;[88] broad filtering of all content by the hosting services provider would be required for such prevention to be technically feasible.[89] In turn, this would risk violating not only Article 15(1) of the ECD, but also primary EU law (namely, the user's privacy and the user's freedom of speech and information enshrined in the Charter of Fundamental Rights of the European Union)[90].

[85] In *L'Oréal v eBay* awareness can be gained often – but not always – by means of a notice.
[86] See Sabam and Netlog, *supra,* note 9- Scarlet Extended, supra, note 9.
[87] Sabam and Netlog, note 9, para. 38.
[88] See Sabam and Netlog, paras. 37 and 38.
[89] See Schmid, supra, note 76, and Brüß, *supra*, note 11.
[90] See Sabam, para. 48.

Finally, it remains to be seen how this injunction can be complied with and whether the issue of costs for the intermediary will have an impact on the reasoning of the court. In Netlog's filtering mechanism, one condition was that the monitoring would be entirely at the expense of the hosting services provider.

Here, the Vienna Court of Appeal considered the costs of such a measure – removing content that was similar in meaning regardless of a notice but in the relevant jurisdiction only – as unreasonable.

In this respect, it is worth mentioning that the implementation methods of a broader scope injunction matter for two reasons: first, inaccuracy of content based filters, and second, the impact on innovation in terms of costs for smaller platforms.

In respect to the first point, precisely because context matters[91], automatic tools that allow the removal of illegal comments "which are equivalent in wording" to the reported illegal content are insufficient to assess such context.[92] In this sense, were the injunction to be implemented by automatic tools that provide for filtering (up to the present, such tools have not been considered excessively costly for defendants), the negative impact on the users' freedom of speech and information must be taken into account, as over-removal may occur[93].

In addition, if human review were to be implemented when the injunction also covers "information equivalent in meaning to the reported content", how can this be done without it being excessively costly for the hosting services providers[94], or without this leading to legal uncertainty for the intermediary?[95]

While major platforms have human staff addressing notices, the wording of the question asked to the CJEU is framed in general terms; the Austrian Supreme Court speaks about "hosting services providers" in general. Therefore, depending on how the CJEU will address the matter, the ruling may also have an impact on hosting services providers which are not necessarily big social media, but rather small and innovative platforms. Such platforms nevertheless deal with content posted by their users, which may be violating users' rights. The Internet is not only Facebook and Google. The impact on innovation for all providers needs to be kept in mind.

III. Conclusions

Under Article 15(1) of the ECD, EU Member States are prohibited from imposing on intermediary services providers any general obligation to monitor information, which they transmit or store, or to actively seek facts or circumstances indicating illegal activity. At the same time, the ECD allows national judges to impose on intermediaries measures containing specific monitoring obligations. Case law from the CJEU has not shed light on the exact scope and jurisdictional reach of

[91] See Keller, note 57 and Schmid, note 85.
[92] See D. Keller, note 57.
[93] See Schmid, note 85-

[94] See the reasoning of the Vienna Court of Appeal. See also Opinion of AG Szpunar in McFadden v Sony, where the AG considered in depth issues with "injunctions formulated in general terms." Id. paras. 116 to 124.
[95] See Opinion of AG Szpunar in McFadden v Sony, paras. 77 to 80.

Article 15 of the ECD in regard to illegal content violating users' personality rights.

On March 19, 2018, the Official Journal of the European Union published the formal questions asked by the Austrian Supreme Court (*Oberster Gerichtshof*) to the CJEU in the context of the pending request for a preliminary ruling in the matter of *Glawischnig-Piesczek v Facebook Ireland Limited*.[96] In essence, the request, lodged by the Austrian Supreme Court at the beginning of 2018, will allow the CJEU to clarify the scope of Article 15(1) of the ECD. This article attempted to address some clarifications that the CJEU is expected to carry out and the very important issues that they raise, given the global nature of the Internet, where fundamental rights are at stake.

No matter which direction the CJEU will take, the pending ruling will allow the court to shed light on the scope of Article 15(1) of the ECD as it pertains to national injunctions, specifically when such injunctions contain specific monitoring obligations. Since broad injunctions may *de facto* risk rendering Article 15(1) ECD an empty shell,[97] the CJEU is faced with an opportunity to define the limits of such injunctions. The judges must balance the need to prevent hosting services providers from shielding themselves from their responsibilities to not become platforms for hate, on the one hand, and users' fundamental rights, as enshrined in the Charter of Fundamental Rights of the European Union, on the other. How the CJEU will strike the balance of the fundamental rights at stake remains to be seen.

[96] Case C-18/18: Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 10 January 2018 — Eva Glawischnig-Piesczek v Facebook Ireland Limited, OJ C 104, 19.3.2018, p. 21–21.
[97] See Frosio, note 12.