



OXFORD PRO
BONO PUBLICO

# Regulation of Digital Media and Intermediaries

**December 2021**

# CONTRIBUTORS

## Faculty Supervisor:

**Prof Jacob Rowbottom**
Professor of Law
Faculty of Law, University of Oxford

## Research Coordinators:

**Rupavardhini Balakrishnan Raju**
DPhil Candidate, University of Oxford

**Mihika Poddar**
MPhil Candidate, University of Oxford

## Researchers:

**Andrew Omond**
MSt Candidate, University of Oxford

**Austin Chan**
BCL Candidate, University of Oxford

**Ceara Tonna-Barthet**
BCL Candidate, University of Oxford

**Constance Hurton**
MSc Candidate, University of Oxford

**David Horvath-Franco**
BCL Candidate, University of Oxford

**Genki Kimura**
MJur Candidate, University of Oxford

**Glory Nwaugbala**
DPhil Candidate, University of Oxford

**Humadha Ahmed**
MPP Candidate, University of Oxford

**Katina Dorer**
MSc Candidate, University of Oxford

**Kwan Lui Victor**
MSc Candidate, University of Oxford

**Luz Orozco**
DPhil Candidate, University of Oxford

**Madeleine Lusted**
BCL Candidate, University of Oxford

**Marlies K. Hofmann**
MJur Candidate, University of Oxford

**Robert Stendel**
MJur Candidate, University of Oxford

In addition, the research team would like to thank:

- **Professor Mindy Chen-Wishart**, Dean of the Oxford Law Faculty, for her support of this project;
- Members of the Oxford Pro Bono Publico Executive Committee, **Dr Andrew Higgins, Professor Kate O'Regan, Dr Miles Jackson, Professor Sandra Fredman and Dr Shreya Atrey,** and members of the Student Committee, **Alvin Cheung, Ayban Elliott-Renhard, Chelsea Wallis, Gayathree Devi KT, Sameer Rashid Bhat, Swapnil Tripathi and Vandita Khanna** for their support and assistance with the project.

**Indemnity**

Oxford Pro Bono Publico (OPBP) is a programme run by the Law Faculty of the University of Oxford, an exempt charity (and a public authority for the purpose of the Freedom of Information Act 2000). The programme does not itself provide legal advice, represent clients or litigate in courts or tribunals. The University accepts no responsibility or liability for the work which its members carry out in this context. The onus is on those in receipt of the programme's assistance or submissions to establish the accuracy and relevance of whatever they receive from the programme; and they will indemnify the University against all losses, costs, claims, demands and liabilities which may arise out of or in consequence of the work done by the University and its members.

**Intellectual Property**

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

## A. INTRODUCTION

1. OPBP has been asked by the Internet Freedom Foundation (IFF) to prepare a report on the law relating to selected aspects of regulation of social media intermediaries, online news media, and over-the-top on-demand video streaming platforms ('OTT platforms'). IFF is a non-profit digital rights organisation operating in India with the stated aim of ensuring that technology respects and furthers the fundamental rights of internet users in India. It works across a broad spectrum of issues, with expertise in free speech, electronic surveillance, data protection, net neutrality, and innovation.

2. This report examines the position of law on the regulation of social media intermediaries, online news media, and OTT platforms in Argentina, Australia, Canada, Chile, the European Union, Germany, and the United States of America. It does this with a view to identifying how content on these online platforms is regulated and monitored by domestic laws, in order to understand the extent of regulatory control exercised by the State. In this backdrop, the report explores the following research questions:

### I. Social Media Intermediaries:

a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?

b) Can the government order that content be removed, and if so in what circumstances, and what types of content?

c) What is the nature of the content that a court can order to be taken down from a social media intermediary?

d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?

### II. Online News Media:

a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?

b) What are the tests or standards for determining whether an online news article/page needs to be removed?

c) Is the order of a court/tribunal a prerequisite for removal of online content?

**III. OTT Platforms:**

a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?

b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?

## B. RESEARCH FINDINGS

3. In general, the regulation of social media, online news media and OTT platforms is an emerging area, with countries across the world grappling with the need for regulation while also balancing free speech and expression concerns. In the absence of specific regulatory tools designed for online platforms, a patchwork of laws governing speech, media and information in the physical space have been extended to digital content. These may range from tort law, copyright law, regulation for publications and media to criminal laws prohibiting dissemination and/or publication of some kinds of content. Moreover, in many contexts, regulation aimed at internet service providers have been extended to social media platforms, for broadcasting media to OTT platforms, and print media to online news media. Increasingly, in light of the difficulties that extending these laws to different platforms raises, jurisdictions have been considering more targeted legislation. As this report was being written, laws in several jurisdictions remained in flux with new laws having been recently introduced or draft bills being considered. When considering regulating online platforms, governments are faced with the dilemma of striking the fine balance between the need to

exercise control and monitor content on these platforms for different regulatory goals vis-à-vis concerns of freedom of speech and the media and access to information.

4. In this context, the South American and European countries in particular are also influenced by the regional human rights jurisprudence. Where there is draft legislation, the report has also attempted to include the proposed provisions in addition to the existing position of law. Where there are regulatory bodies tasked with oversight over digital intermediaries, the report has attempted to discuss the extent of independence of these bodies.

## I. Social Media Intermediaries:

5. In jurisdictions where there is no targeted legislation, the liability for content is spread across a number of laws. In view of limitations of scope, the report does not cover *everything* online that attracts liability, or can be removed by executive or court order, but instead largely focuses on criminal liability, and liability for violation of intellectual property, and laws relating to defamation. The cross-cutting themes that emerge in the regulation of social media relate to whether liability for content posted is linked to knowledge of the unlawful nature or illegality of content, whether procedures for the removal of such content are detailed, and specification of timelines for response in taking down of content. Majority of the jurisdictions examined impose liability based on knowledge of unlawfulness of content, with removable content often linked to the country's criminal code. With respect to liability, many of the cases largely fall under intellectual property violations and defamation laws. Special attention is paid across jurisdictions to certain categories of unlawful content such as pornography especially those involving minors, offences threatening state security like terrorism related content, and decency laws which often have expeditious timelines attached for removal.

### a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?

6. In Argentina, the Constitution accords protection to the right to publish ideas without prior censorship, and the freedom of press. In addition, the Inter-American Human Rights standards have influenced the development of case law. The National Communications Entity ('ENACOM') is the main communications and media regulator. The position

regarding liability for content is drawn from Supreme Court rulings. Social media intermediaries cannot be held liable for 'content that they have not created themselves', except for the cases in which they had previous and actual knowledge of the illegality of the information and did not act diligently to remove it. In cases of content with 'manifest illegality' which have been enumerated by the Court, private notice by interested parties is sufficient to constitute knowledge of illegality and triggers an obligation to take down the content. For all other types of content, removal is subject to judicial order.

7. In Australia, the laws regulating social media intermediaries are currently undergoing change. The Online Safety Bill recently received royal assent and is scheduled to come into force in early 2022. In general, it is an 'actual knowledge' jurisdiction, whereby liability is imposed in line with awareness i.e., social media intermediaries are liable for the information they are deemed to have knowledge of (and therefore have the ability to remove). However, at present the liability for content is covered under various areas of law with differing thresholds. On the civil side, liability can fall under provisions relating to consumer protection, defamation, vilification, and copyright, subject to limitation of liability which prevents internet hosts from being held liable for content that they were not aware of, and prohibits rules that require an internet host or Internet Service Provider (ISP) to monitor, make inquiries about, or keep records of, content hosted or transmitted. In addition to the above, a further route to civil liability will come into force in 2022 under the forthcoming Online Safety Act. This will impose civil liability upon online intermediaries, including social media intermediaries, for several pre-defined categories of content, as enforced by the eSafety Commissioner – the statutory regulatory authority. These are: cyber bullying targeting an Australian child, cyber-abuse material targeting an Australian adult, non-consensually posted intimate images, posts containing Class 1 and 2 material (a classification scheme for content simplifying the existing Broadcasting Services Act, 1992), content breaching industry codes, and 'abhorrent violent material'. On the criminal side, social media platforms are criminally liable if they fail to 'ensure the expeditious removal of' or 'expeditiously cease hosting' 'abhorrent violent material' subject to exceptions including under the Constitutional right of political communication which can be used as defences by the social media intermediary.

8. In Canada, there are limited circumstances in which liability may be imposed upon social media intermediaries. Liability arises under copyright law only if a notice of infringement is

received and the intermediary does not pass on the notice. Under the law of defamation, judicial decisions suggest that knowledge of the defamatory statements is necessary, and some degree of negligence or non-action upon notification is required to attribute liability as a publisher. The Canadian has been considering new legislation to regulate five kinds of online harms - child sexual exploitation content, terrorist content, content that incites violence, hate speech, and non-consensual sharing of intimate images. As its last draft stood, it would increase the burden on platforms requiring active content monitoring and includes administrative and monetary penalties for non-compliance, including failure to block or remove content.

9. In Chile, liability for content rests with the original author. Tortious liability for intermediaries arises only when a service provider stores illegal content, has knowledge of its illegality and does not remove it within a reasonable time period. The copyright laws also exempt providers from liability if they meet certain conditions including lack of knowledge of the illegality of the content, absence of financial gain from the violation and ability and procedure to control and expeditious removal of infringing content. Criminal liability attaches to distribution of sexual content without the permission of the persons involved, or content that may violate another's honour, but it is unclear whether this would apply to social media intermediaries. There was a proposal to specify liability for site administrators for hosting and not removing pornographic material, although it has not yet become law.

10. In Germany, social media intermediaries are regulated under the Network Enforcement Act. The Network Enforcement Act, however, does not impose a general obligation to monitor content on its platform, but to maintain an effective complaints procedure for processing user complaints and imposes reporting obligations in the form of publication of specified details in the Federal Gazette and the platform's website. The Act defines what constitutes unlawful content drawing reference to the Criminal Code and stipulates a time period for removal. The liability mainly takes the form of regulatory fines prescribed by the Act. The administrative authority empowered to issue regulatory fines and to monitor compliance is the Federal Office of Justice. The Act provides for judicial appeal against the regulator's decision.

11. In the European Union (EU), social media regulation is currently largely governed by the E-Commerce Directive (ECD) with sector specific rules supplementing it. A Digital Services

Act (DSA) is currently under consideration which seeks to bring in greater regulation. At present under the safe harbour principle, social media intermediaries are immune from liability under the E-Commerce Directive if they do not have actual knowledge of illegal activity or information and, as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent; or upon obtaining such knowledge or awareness, act expeditiously to remove or to disable access to the information. Despite this general exemption, intermediaries are increasingly subject to transparency and risk-assessment obligations, and there are also sector specific rules relating to consumer protection and data protection provide for liability under specific circumstances. Liability under copyright laws arise when intermediaries fail to take proportionate measures to disable access to or remove the infringing contents expeditiously and make best efforts to stay down such contents. Moreover, liability may also arise if intermediaries fail to follow requirements under data protection law.

12. In USA, The Communications Decency Act 1996 provides immunity to intermediaries for user-generated content on the platform on two fronts – and does not attribute liability if there has been action in good faith to restrict access to objectionable material. There are some criminal and intellectual property based exceptions and also some judicially identified exceptions to this immunity, such as (i) if the provider or user of an interactive computer service induced or contributed to the development of the illegal content in question; (ii) if the plaintiff's claim does not arise from the defendant's publishing or content moderation decisions (the act only provides protection against liability arising from the defendant's role as a publisher); and (iii) if the provider or user of an interactive computer service fails to meet the good faith requirement.

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

13. In Argentina, there is no specific procedure for the government to order removal of content and the standards laid down by the Supreme Court as discussed above applies.

14. In Australia, independent statutory authority – the eSafety Commissioner – has various powers under which they can issue a removal notice for online content. The types of content that can be removed include prohibited content defined in the Broadcasting Services Act,

1992 under which the eSafety Commissioner has the power to ban certain types of content from being hosted on sites located within Australia. Such content can either be referred to the commissioner through the complaints process and the Commissioner also has own powers of investigation. Other content that can be removed include cyber bullying material targeting an Australian child, and non-consensually shared intimate images under the Enhancing Online Safety Act, 2015. The forthcoming Online Safety Act due to come into force in 2022 updates the current take-down powers of the e-safety commissioner, both amending the removal process set out by the Enhanced Online Safety Act 2015 and conferring additional categories – namely, cyber-bullying scheme, adult cyber abuse scheme, image-based abuse scheme, online content scheme (which provides for a simplified classification system and removal of harmful material under certain circumstances), and abhorrent violent material blocking scheme. All these categories have prescribed timeline for compliance with the order for removal. It also provides for an appeals process whereby the commissioner's decisions can be referred to the Administrative Appeals Tribunal, which then performs an independent merits review.

15. In Canada, there currently does not exist any specific procedure empowering the government to order takedown of content. Even under the copyright law, the intermediary does not have to take down content to avoid liability. However, under the new law being considered by the government, any individual – governmental or otherwise – would be able to flag content as harmful, (as per five identified harms - child sexual exploitation content, terrorist content, content that incites violence, hate speech, and non-consensual sharing of intimate images). The social media platform would then be obliged to remove the content or respond by concluding that it is not harmful within 24 hours.

16. In Chile, there is no specific procedure that allows the government to remove content. However, a court when approached by a rightsholder could order an intermediary to take down content if it (a) is infringing a copyright or (b) amounts to a crime.

17. In Germany, there is a complaint mechanism that can be invoked by users for removal of content under the Network Enforcement Act. Apart from specified obligations to provide data based on requests for information from official authorities, there does not appear to be separate powers for the government to order removal of content. The type of content that

can be removed is unlawful content specified in the Network Enforcement Act which lists offences under particular provisions of the Criminal Code.

18. In EU law, neither of the relevant directives stipulate the power of the states to require social media intermediaries to take down specific contents, as they are considered to be a matter of national legislation. However, the EU-level sector-specific rules stipulate the entitlements of the competent authority of the member states to order the removal of specific contents such as child pornography, hate speech and violence, terrorist content etc.

19. In the USA, the Digital Millennium Copyright Act provides a notice and takedown process to have user-uploaded content which infringes copyright to be removed from websites. ISPs are provided with a wide immunity from liability if they comply with the notice-and-takedown procedures. However, the government takes substantial enforcement efforts directed at online intermediaries. Other than copyright law, the First Amendment jurisprudence subjects any content-based restrictions on speech to a 'strict scrutiny' analysis, resulting in most laws seeking to regulate content being invalidated. Consequently, users' ability to post speech on social media platforms and governments' ability to order for content to be removed is primarily secured through self-regulation by virtue of moderation policies, terms and conditions created and enforced by the intermediaries.

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

20. In general, the types of content that can be taken down have been outlined the previous two sections. Further details where applicable are discussed below.

21. In Argentina, the test is 'manifest illegality' and courts would consider as manifestly illegal content such as child pornography, data that facilitates or instructs the commission of crimes, that might endanger people's lives or physical integrity, that promotes genocide, racism or discrimination with incitement to violence, that disrupts ongoing crime investigations, that constitutes a serious offense to honour, notoriously faked pictures, or that entails a serious and grave invasion to privacy by publishing images that were intended to remain private. Apart from these intellectual property rights among others has also been found as grounds for removal of content.

22. In Australia, courts can order content which is deemed to be defamatory, infringing copyright, breaching consumer protection, and vilificatory to be taken down, and Illegal content under the criminal law such as content that incites or promotes suicide, child pornography or child abuse, or abhorrent violent material can be subject to a court-order of removal.

23. In Canada, courts have been reluctant to order take down of content from online platforms in light of free speech principles, and consider several factors to determine if such an order can be made in cases of defamation and even hate speech. This involves a delicate balance between freedom of expression and restrictions on speech on social media. However, building on existing law, under the new proposed law (Bill C-10 - An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts), the takedown powers will focus on five kinds of harms - child sexual exploitation content, terrorist content, content that incites violence, hate speech, and non-consensual sharing of intimate images.

24. In Chile, a court can order content to be removed when approached by a rightsholder if it (a) is infringing a copyright or (b) amounts to a crime.

25. In Germany, apart from intellectual property violations, the types of content that can be removed are mainly covered by the Network Enforcement Act as discussed in para 17.

26. Under EU law, there is no specific framework governing the take down of specific content at the EU level. EU law takes it for granted that the courts of each member state can offer injunctive relief in the case where it is proportionally appropriate to remove specific contents based on a rightsholder's legitimate claim. The Directive on Combatting Terrorism is one of the exceptions, which requires that intermediaries remove flagged terrorist content in all member states within an hour of receiving a removal order from the competent authority.

27. In USA, once a category of speech is considered by the Court as 'unprotected', it may be prohibited, although there are very few kinds of content that will amount to unprotected speech.

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

28. In Argentina, no specific procedure is provided by law to request or order a social media intermediary to 'unmask' an anonymous speaker or identify an originator of content.

29. In Australia, at present the courts are able to request unmasking information where necessary for enforcing legal regulations and ensuring justice. Under the forthcoming Online Safety Bill 2021, the statutory authority – the eSafety Commissioner will gain identificatory and investigatory powers where necessary in aiding its investigations. It allows the Commissioner to request information about the identity of the end-user of a social media service and their contact details. The Commissioner may also disclose this information to various other named bodies.

30. In Canada, the identity of anonymous wrongdoers can be unmasked by 'Norwich Pharmacal Orders' - a way to compel the release of information relevant to a potential claim before the action is commenced. If an innocent third party such as a website operator has enabled the perpetrator to commit a wrong, a Norwich Pharmacal Order can be sought, and may compel the service provider to disclose information about an anonymous poster's real name, IP address, email address, etc. Such an order will be issued only if these conditions are met - sufficient evidence of a valid, bona fide or reasonable claim against the wrongdoer, involvement of the third party from whom the information is sought in the wrongdoing, lack of other practicable source of the information, whether the third party can be indemnified for out-of-pocket costs to which it may be exposed because of disclosure, and whether the interests of justice favour disclosure.

31. In Chile, courts have been unwilling to cater to requests to 'unmask' anonymous users, but it may be allowed when necessary to impose civil or criminal liability on infringing/injurious content.

32. In Germany, amendments to the Network Enforcement Act which are in various stages of implementation greatly expand the access of the Federal Criminal Police (BKA) in cases of online hate crimes to personal user data. 'Personal data' includes usernames, internet protocol (IP) addresses, port numbers and, with a judicial order, passwords.

33. In EU law, there is no specific law on unmasking anonymous users. However, unmasking anonymous users may have human rights implications. Although the question is yet to be addressed whether an expectation of anonymity on the internet is an aspect of the right to the protection of personal data and the right to freedom of expression, the European Court of Human Rights has upheld the value of anonymity as a part of freedom of expression generally.

34. In USA, intermediaries may be asked to unmask anonymous users for issues like copyright infringement, defamation, harassment, etc. Other than under the copyright law, there is no uniform standard governing this, although generally, many cases have assessed two facotrs before making a determination – (a) ensuring the defendant has notice and opportunity to respond to the subpoena before his identity is exposed and (b) the strength of the plaintiff's underlying claim.

## II. Online News Media:

35. In the absence of specific legislation, the regulation of online news media in the majority of the jurisdictions covered is an extension of print media laws. In comparison to social media, in some jurisdictions the standard for intervention and removal appears to be the same, but in others it is higher due to the countervailing concerns regarding freedom of press. Removal or takedown of content is generally difficult except in cases of copyright.

### a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?

36. In Argentina, there is no special procedure for the government to order or request that an online news item must be removed from a website and the same standards regarding illegal content laid down by the Supreme Court that apply to social media intermediaries also apply to online news media.

37. In Australia, the law is the same as that governing social media content. The eSafety Commissioner is empowered under the Enhancing Online Safety Act 2015, and will be empowered under the Online Safety Bill 2021 to order that online news items

must be removed where the content is deemed to be - cyber-bullying targeting an Australian child, cyber-abuse of an Australian adult, non-consensual intimate images, class 1 and class 2 content, abhorrent violent material. The take-down process here is also the same as with regards to social media above. For news, however, there is a specific exemption under the Online Safety Bill 2021, with material exempt from removal where the material relates to a news report, or a current affairs report, that is in the public interest, and is made by a person working in a professional capacity as a journalist.

38. In Canada, there is no specific statutory provision allowing the government to order the removal of online news from any website in the absence of a court-issued removal order. Courts have generally been reluctant to grant such orders, favoring upholding freedom of the press. However, Bill C-10 in its current form would have given the government broad powers to ask Online Communication Service to take any action or refrain from doing certain things in furtherance of obligations imposed upon them under the Act.

39. In Chile, a court can order an online media platform to remove or rectify certain defamatory content, and failure to abide by it may attract fines for the director of the news media or even suspension of its operations. However, there is no specific regulation governing removal.

40. In Germany, online news media is subject to a rather complicated and piecemeal regulatory framework. This is due in part to a lack of specific regulation on online news media and in part to the federal structure of Germany because legislative powers concerning online news media are split between the federal level and the State level. The states have agreed on Inter-State treaties between them harmonizing the rules applicable to media. The Inter-State Treaty on Media and the Inter-State Treaty on Media and the Protection of Minors allow for content to be removed if they violate rules relating to advertisements or gambling or contain content that can be construed as fighting the liberal democratic order, glorifying Nazi crimes or war, inciting hatred against minority groups, or child pornography. An order to remove online content may be enforced without an additional court order according to the respective State's laws on enforcing acts of the administration subject to the requirement of proportionality. In relation to civil liability online news media are liable for their own content (or third-party content which they adopted as their own). Government agencies may also invoke these provisions to remove

content. Removing online news items under criminal law offences such as insult and defamation is possible as a consequences of criminal proceedings.

41. In the EU, in general regulations for online news media must be read with the fundamental right to freedom of expression. Under the European Charter for Human Rights (ECHR) jurisprudence, public authorities can order the removal of an online news item if 'prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.' The procedure for removal is regulated at the national level.

42. In USA, the First Amendment protects freedom of press and thus applies to online news media as well. Prior restraint is not permitted and the courts have held that the content on the internet is cannot by itself be the subject of greater regulation as it is not as invasive as broadcast media. Content-based removals of speech are presumptively unconstitutional and will be subject to strict scrutiny. There are only a few categories of unprotected speech where the protection does not apply – defamation, obscenity, incitement, fighting words, true threats, speech integral to criminal conduct, child pornography and speech harmful to minors, protection of intellectual property.

**b) What are the tests or standards for determining whether an online news article/page needs to be removed?**

43. In Argentina, courts have incorporated the Inter-American standard of 'public interest' and have considered the 'journalistic relevance' of allegedly infringing information when assessing whether a particular search result, thumbnail or page should be de-indexed or removed.

44. In Australia, the same standards as that which apply to content on social media as discussed earlier govern online news content.

45. In Canada, given the absence of legislative direction, courts have set a high bar to order removal of content. Requiring a party to remove content from the internet constitutes a "mandatory injunction". As this is burdensome, the test to issue it is more stringent. The plaintiff must show that they have a "strong prima facie case" and are very likely to succeed at trial.

46. In Chile, there is no specific regulation governing removal of content, and thereby no uniform standard governing this.

47. In Germany, the test of proportionality applies to the removal of content. Ordering the removal of a news item is only legal if there is no other and equally effective way to achieve the desired aim and any such measure must be restricted to parts of the content if this suffices to achieve the desired aim. Removal must not be disproportionate compared to the importance of the content for the provider or the general public.

48. In the EU, the test to determine whether an online news article or page was removed in accordance with the following standard - whether such removal is (1) prescribed by law, (2) in pursuit of a legitimate aim, and (3) necessary in a democratic society. This is subject to the requirement of proportionality and ensuring that the action does not amount to censorship.

49. In USA, as mentioned above, content-based removals of speech are presumptively unconstitutional and will be subject to strict scrutiny. Takedown will be authorised only if the speech can be categorised as unprotected.

**c) Is the order of a court/tribunal a prerequisite for removal of online content?**

50. In Argentina, in cases of 'manifest illegality' notice is sufficient to trigger the removal process. For all other cases a judicial order is necessary.

51. In Australia, a court order is not prerequisite for the removal of online content, as the eSafety Commissioner can order that content be removed where it falls under the content categories dictated under the Broadcasting Services Act 1992, Enhancing Online Safety Act 2015, Criminal Code Amendment (Abhorrent Violent Material) Act 2019, and

forthcoming Online Safety Bill 2021, subject to appeals to the Administrative Appeals Tribunal.

52. In Canada, only courts can order removal of online content. However, under the new proposed legislative framework, harmful content posted online could be addressed through a myriad of takedown requirements, content filtering, complaints mechanisms, and even website blocking, much of which can occur before the involvement of any court or tribunal.

53. In Chile, a court order is required to order removal of unlawful content.

54. In Germany, any removal of online content requires a court order. Removal on public law grounds remains subject to interpretation in the light of inadequate litigation on the matter. While a plain reading of statutory provisions does not mandate a judicial process, there could be countervailing claims on constitutional grounds.

55. At the EU level, there is no requirement for an order of the court / tribunal to remove online news content. Member States enjoy the freedom to order content to be removed if prescribed by law and is necessary in a democratic society. Individuals may, however, approach national courts alleging that an order to remove online content issued by the relevant authority infringed their freedom of expression.

56. In USA, a court order will be required for any take down, except through notice and takedown provisions under the copyright law.

## III. OTT Platforms:

57. The area appears to be broadly based on self-regulation or is unregulated. Though in some jurisdictions proposed regulation is in the offing.

### a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?

58. In Argentina, other than being required to register as film distributors and for tax purposes, OTT platforms are largely unregulated though specific legislation is under consideration.

59. In Australia, the OTT sector is largely governed by the Broadcasting Services Act 1992. This has a two-part approach, with different Schedules governing content hosted outside of Australia and content with an Australian connection. These set the standards for the kinds of content that can be hosted online, including both classified and unclassified content. There are various restricted categories under this. While the Australian Classification Board is responsible for content classification, Australia is moving towards a self-classification model with a major OTT platform receiving approval to self-classify content.

60. In Canada, proposed amendments to the Broadcasting Act will clarify that OTT services would be subject to the Act and could be required to contribute to the Canadian broadcasting system and highlight Canadian-created media under the same obligation as traditional broadcasters. This would give the regulator greater powers and flexibility to ensure online services contribute to the domestic funding system. Different services will consequently be subject to different levels of regulation depending on the nature of those services, depending on whether they are 'regulated' or 'not regulated'.

61. In Chile, there is no specific law regulating OTT platforms, but the general penal restrictions on exhibition of child pornography and materials contrary to 'good customs' may apply to content on such platforms. A Bill to regulate OTT Platforms in particular was tabled in September 2021, but has not been enacted yet. As per the draft bill, will only be liable for content that is unlawful, civilly libellous, slanderous, constituting threats or offences, if they do not act diligently to block or remove such content when they have actual knowledge of its unlawfulness. Platforms will also be obligated to take specific measures to protect the image and integrity of vulnerable persons.

62. In Germany, the Inter-State Treaty on Media provides the regulatory framework for OTT platforms. There are mandates obligating diversity of content and restrictions on discriminatory practices while hosting content. There are also regulations relating to user interface. OTT platforms do not require any prior licensing. The State Media Authority, a body independent from government authorities has regulatory oversight over OTT platforms.

63. In the EU, the general framework for regulation of OTT platforms is the Audiovisual Media Service Directive (AVMSD). The chief purpose of the AVMSD is to govern EU co-ordination of national legislation on all audio-visual media. Much of the regulation takes place in the form of voluntary measures adopted by OTT platform providers.

64. In USA, there is no specific regulation for OTT platforms. However, the regulatory authority, the Federal Communications Commission, has some standalone rules like requiring captioned programs shown on TV to be captioned when re-shown on the Internet, and general copyrights laws apply to them. The platforms are largely self-regulated.

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?**

65. In Argentina, there is no specific procedure under the law that allows the government to order an OTT platform to remove or modify content.

66. In Australia, the process for modifying and removing content hosted by an OTT platform is the same as discussed earlier in para 59 with regards to removing content from a social media host or online news item, with the eSafety Commissioner being accorded powers.

67. In Canada, there is no specific authority to order that content hosted by OTT platforms be modified or removed from any website. However, as Bill C-10 would bring OTT platforms into the potential regulatory purview of the CRTC, they would be legally obliged to address content hosted on their platforms that violate the Broadcasting Act's five online harms: child sexual exploitation, terrorist content, incitement to violence, hate speech, and non-consensual sharing of intimate images. In this way, OTT platforms would be subject to the same regulatory regime as social media and online news platforms: the obligation to undertake 'all reasonable measures to do whatever is within their power to monitor for the regulated categories of harmful content on their services, including through the use of automated systems based on algorithms' and restrict its visibility.

68. In Chile, as mentioned in the section above in para 61, there is no specific law regulating OTT platforms, but the general penal restrictions on exhibition of child pornography and materials contrary to 'good customs' may apply to content on such platforms. A Bill to

regulate OTT platforms was tabled but has not been adopted at the time of writing this report.

69. In Germany, the State Media Authorities may order the removal of content for violation of the Inter-State Treaty on Media subject to a proportionality test. However, the State Media Authorities are independent from government authorities.

70. In the EU, the AVMSD imposes an obligation on EU member states to ensure that appropriate measures are taken by video-sharing platforms under their jurisdiction to protect i) minors from content which may impair their physical, mental or moral development (ii) the general public from content containing incitement to violence or hate speech and iii) the latter from content the dissemination of which constitutes a criminal offence (i.e. public provocation to commit a terrorist offence, child pornography, and racism and xenophobia). This allows for potential regulation subject to the overarching standards imposed by the ECHR.

71. In USA, as mentioned above in para 64, there is no specific regulation for OTT platforms but their content may be subject to the general copyrights laws.

# ARGENTINA

## A. INTRODUCTION

72. Freedom of expression is protected under Argentina's National Constitution. Article 14 establishes the right to publish ideas without prior censorship and article 32 prohibits Congress from passing laws limiting press freedom. According to article 75.22, international human rights treaties ratified by the State enjoy constitutional status. Therefore, international human rights law has been instrumental for the development of the caselaw on the right to freedom of thought and expression. Particularly, the Inter-American human rights system – whose authority Argentina has legally and judicially recognised – has had a major influence in the interpretation of the state's obligations regarding 'the right to seek, receive and impart information of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice'.[1]

73. The Inter-American Court on Human Rights has reaffirmed that Article 13 of the American Convention protects not only inoffensive or innocuous expressions but also those that 'offend, shock or disturb the State or any other sector of the population', in the understanding that they are necessary in a democratic, open, plural and tolerant society.[2] According to the Inter-American legal framework, the right to freedom of expression also protects erroneous, mistaken, and false speech, without prejudice to the subsequent liability that may arise as a result.[3] Furthermore, the States have the primary obligation to remain neutral with respect to the content of speech, ensuring that there are no people, groups, ideas or means of expression that are excluded *a priori* from public discourse.[4]

74. As the Special Rapporteur for Freedom of Expression notes, the Inter-American case law emphasises three types of speech that are specially protected due to their importance in the exercise of all other human rights or the preservation of democracy: (a) political speech and

[1] Organisation of American States (OAS), American Convention on Human Rights ('Pact of San José'), Costa Rica, 22 November 1969, art 13.
[2] *Herrera-Ulloa v Costa Rica* (2004), Inter-Am Ct HR (Ser C) No 10, para 207; *La Última Tentación de Cristo* (2001), Inter-Am Ct HR (Ser C) No 73, para 69; *Ríos et al v Venezuela* Preliminary Objections, Merits, Reparations and Costs (2009), Inter-Am Ct HR (Ser C) No 194, [105]; *Perozo et al. v. Venezuela* Preliminary Objections, Merits, Reparations and Costs (2009), Inter-Am Ct HR (Ser C) No 195, [116].
[3] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Annual Report' Ch III (25 February 2009) OEA/Ser L/V/II.134, Doc 5 rev 1, [228].
[4] ibid [231].

speech involving matters of public interest; (b) speech regarding public officials in the performance of their duties and candidates for public office; and (c) speech that is an element of the identity or personal dignity of the person expressing him or herself.[5]

75. In addition, any limitation on freedom of expression to be permissible must be: (i) clearly and precisely defined in a law, both substantively and procedurally, and must serve compelling objectives authorised by the Convention; (ii) necessary and appropriate in a democratic society to accomplish the compelling objectives pursued; and (iii) strictly proportionate to the objective pursued.[6] Moreover, the subsequent liability arising from the abuse of freedom of expression must always be ordered by an independent and impartial judge or court authority, respecting due process guarantees. These measures must in all cases be proportionate and they must not be discriminatory or have discriminatory effects, and they cannot constitute censorship by indirect means, which is specifically prohibited by article 13.3 of the American Convention.[7]

76. Argentina has long recognised the prominent role of international human rights law and frequently incorporates its standards through law and jurisprudence. Notably, in *Kimel v. Argentina* the Inter-American Court analysed the conviction of a journalist for the crime of *calumnia* or false imputation of a publicly actionable crime after publishing a book questioning the judicial conduct of an investigation during the military dictatorship. The Inter-American Court held that the criminal and civil penalties imposed on the journalist were unnecessary and disproportionate – given that the journalist's criticism had evident public interest and that the law that serves as basis for the penalty was not consistent with the legality principle.[8] Therefore, it ordered the Argentinian State, among other things, to undertake a legislative reform of the criminal laws protecting honour and reputation.

77. In 2009, Argentina consequently enacted the 'Kimel law' that modified the legal descriptions in the codes for slander and insults by creating public interest exceptions.[9] However, it must be said that there is a recent legal trend identified by the Legislative Observatory of the Centre for Studies on Freedom of Expression and Access to Information where 19.5% of

[5] ibid [232].
[6] ibid [245].
[7] ibid [251].
[8] *Kimel v Argentina* (2008), Inter-Am Ct HR (Ser C) No 177.
[9] Centro de Estudios en Libertad de Expresión y Acceso a la Información, 'Trends in freedom of expression in Argentina' (March 2018) Universidad de Palermo 5.

the Argentine bills that in some way affect freedom speech criminalize expression, and 40% of them create new crimes (among them, cybercrimes such as 'virtual harassment' and 'non-consensual pornography' in digital format).[10]

78. There is no single, all-encompassing legislation to govern all aspects of cyberspace in Argentina. Since 1997, the State explicitly established protections for online freedom of expression through a presidential decree, which was eventually expanded by Congress in 2005 to include 'the search, reception, and dissemination of ideas and information of all kinds via internet services'. The Digital Law (N. 27.078) establishes the general framework for communications infrastructure, satellite services, telephone networks, mobile services, broadband connections and cable television. Notably, it explicitly excludes any type of content regulation and enshrines net neutrality, meaning that each user is guaranteed the right to access, use, send, receive or offer any content, application, service or protocol through the Internet with no restriction, discrimination, distinction, blocking, interference, obstruction or degradation.

79. The Audiovisual Communication Services Law, as amended by Decree No. 267/2015, has set the regulatory framework for the media landscape. When the law was passed by Congress in 2009, it reserved a portion of the spectrum for non-profit civil society organisations, imposed public service obligations on private media, granted indigenous communities the right to receive radio and TV licenses, established limits to concentration and to broadcasting cross-ownership, and prohibited telephone companies from holding media licenses.[11] However, some scholars argue that the last government (2015-2019) undid many of the communication policies set out by this legislation by opening the possibility of large players providing the whole set of converged services (pay tv, mobile, fixed connectivity and telephony, open tv and radio), fostering concentration in an already highly centralised media market.[12]

80. The National Communications Entity ('ENACOM') is the main communications and media regulator. It was created by presidential decree in December 2015, and later validated by

[10] ibid.
[11] Open Society Foundations, *'Mapping Digital Media: Argentina'* (2012).
[12] Martín Becerra and Guillermo Mastrini, 'Economic and communication policies in Argentina: deregulation and concentration of media 2015-2019 (*Media@LSE blog*, 6 September 2019) <www.blogs.lse.ac.uk/medialse/2019/09/06/economic-and-communication-policies-in-argentina-deregulation-and-concentration-of-media-2015-2019/> accessed 24 September 2021.

Congress in April 2016. According to Freedom House, the body's composition has raised some concerns about its independence from the Executive.[13] The regulator ENACOM operates within the public innovation secretariat, under the chief of cabinet of ministers, and has a board comprised of four directors chosen by the president and three proposed by Congress (one by the majority or first minority party, one by the second minority party, and one by the third minority party).[14] ENACOM's decisions may be approved by a simple majority and its members may be removed by the president.

81. Currently, Argentina does not have a specific legislation regarding digital intermediaries' liability. In the absence of such law, recent court decisions have referred to the Civil and Commercial Code, the Civil Code (now revoked), and the Intellectual Property Law (N. 11.723) to adopt a negligence rule for intermediaries (versus strict liability) when reviewing online content controversies. Since 2014, caselaw establishes that digital intermediaries should not be liable for third-party content if they did not have knowledge of alleged third-party violations and that they must remove unlawful content *only* if notified by a judicial order, with the exception for cases of 'manifest illegality' (where a private notification to the intermediary is sufficient to generate the obligation to remove content).

82. There are no specific regulations or restrictions on encryption of communications or consumer data retention terms. Pursuant to Section 328 of the National Civil and Commercial Code, operators must continue to support accounting documents for 10 years. Regarding the interception of private communications under the National Intelligence Law (N. 25.520) and the Criminal Procedure Code, a warrant or judicial authorisation is required. While telecom operators must guarantee the confidentiality of communications, they must register users' identification information before selling them mobile phones or prepaid SIM cards. They are also bound by Data Protection Law (N. 25.326), which govern how personal data must be collected and the rights that are vested in consumers in this regard.

## B. SECTION 1: SOCIAL MEDIA INTERMEDIARIES

### a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?

[13] Freedom House, 'Freedom on the Net 2021' <www.freedomhouse.org/country/argentina/freedom-net/2021> accessed 24 September 2021.
[14] ibid.

83. In the landmark case of *María Belén Rodríguez v Google Inc*, the Argentinian Supreme Court addressed the liability of search engines for linking in search results to illegal third-party content and established the standards to take down or de-index information.[15] The Court ruled that search engines could not be held liable for 'content that they have not created themselves', except for the cases in which they had previous and actual knowledge of the illegality of the information and did not act diligently to remove it. Courts have applied the same standard to digital services different from search engines. In *Alberto Nakayama y otros* a Criminal Court ruled Taringa's stay of proceedings, a social networking site that hosts content uploaded by its users. The case involved a lawsuit against Taringa based on copyright.[16] According to the Criminal Court, Google and Taringa are both 'intermediaries whose main objective is to serve as a link'. Therefore, they have no obligation to verify third-party content ex ante, but are only responsible when they have actual knowledge of its illegality and do not act accordingly. Since Taringa removed the infringing content upon notice, it was not held liable.

*i) Previous and actual knowledge*

84. Specifically, the Supreme Court held in *María Belén Rodríguez v Google Inc* that search engines do not have a general obligation to proactively monitor the content uploaded by third parties and, therefore, there is no strict liability involved.[17] Instead, each author or creator should be responsible for the content provided. However, once a search engine acquires actual knowledge of the illegality of the content it becomes actively involved with the wrongdoing and may be held liable if it does not remove it promptly. In the absence of a specific legal provision, the Supreme Court set the standard that a distinction should be made between 'manifest illegal' content – where a breach of law is clear and a private notice from an interested party to the search engine generates actual knowledge - from the case where the allegedly harmful content requires interpretation or clarification - and, consequently, a judicial order is indispensable, as it will be further explained.[18]

[15] Corte de Justicia de la Nación [National Supreme Court] *Rodríguez, María Belén v Google Inc.*/daños y perjuicios [2014] CSJN Case no 337:1174 (Arg).
[16] Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala [National Criminal Chamber of Appeals] *Nakayama, Alberto y otros*/infracción a la Ley 11.723 [2015] Expte. N 21964/2014 May 5 2015 (Arg).
[17] ibid 15.
[18] Eduardo Bertoni, 'Right to be…Forgotten? Trends in Latin America after the Belén Rodríguez Case and the Impact of the New European rules', in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).

*ii) A reliable private notice for 'manifest illegal' content and the requirement of a judicial order for any other content*

85. The Court decided that, in the event of manifest or ostensible illegal content, a private notice to the search engine – not necessarily from the alleged victim – would suffice to trigger actual knowledge and the consequent duty to remove, delist or block the material. Manifest or ostensible illegal content would be: child pornography, data that facilitates or instructs the commission of crimes, that might endanger people's lives or physical integrity, that promotes genocide, racism or discrimination with incitement to violence, that disrupts ongoing crime investigations, that constitutes a serious offense to honour, notoriously faked pictures, or that entails a serious and grave invasion to privacy by publishing images that intended to remain private, even if not sexual.[19] The Court insisted on the 'explicit' and 'obvious' damage involved in these hypothesis to set off a reliable private notice to the search engine, where the illegal nature of the material should be beyond dispute.

86. For any other content, the Supreme Court held that a court or other competent authority should decide on its illegality and issue a notice to the search engine in order to generate the obligation to remove, delist, or block the material. The Court reasoned that, when clarification is needed, a search engine cannot and should not supply judicial adjudication. Therefore, in this second hypothesis, a private notice would not be enough to trigger actual knowledge. With this standard, Argentina favours a judicial takedown regime over a 'notice-and-takedown' system.[20]

*iii) Negligent response*

87. As explained, in cases of manifest illegality, search engines that receive a private notice are expected to remove, delist or block the harmful content promptly. In the rest of the cases, a judicial order is required to determine the illegal nature of the information and whether a notice to the digital intermediary is necessary. Only with proper notice, a plaintiff may be able to claim damages if the search engine negligently fails to act, as provided by the subjective liability rule established in Article 1109 of the Civil Code.

[19] ibid 506-507.
[20] Freedom House, 'Freedom on the Net 2021' <www.freedomhouse.org/country/argentina/freedom-net/2021> accessed 24 September 2021.

88. For instance, in *María Belén Rodríguez v Google Inc,* the plaintiff never notified the defendants – Google and Yahoo! – about the alleged infringing content. Therefore, the Supreme Court concluded that the search engines never acquired actual knowledge.

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

89. There is no special procedure for the government to order or request a social media intermediary to remove content. Government is bound by the general standards set by the Supreme Court in *María Belén Rodríguez v Google Inc,* which have been subsequently reaffirmed to date. Consequently, the government may either file a reliable notice to the social media intermediary for 'manifestly illegal content' as an interested party or obtain a judicial court order.

90. Notably, the regulator ENACOM publishes an online repository of websites that have been blocked or reinstated (or both) after judicial court orders.[21] The majority of website blocks concern copyright infringements and online gambling.

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

91. Courts have ordered social media intermediaries to remove content based on plaintiffs' rights to honour and privacy, guaranteed under the Civil and Commercial Code. However, when reviewing claims under the 'right to be forgotten', judges have considered journalistic relevance and public interest of the information as legitimate limitations of the right and consequently denied removals or deindexations. Courts have also ordered intermediaries to block content and websites to protect copyright, under the Intellectual Property Law.

92. Additionally, in line with *María Belén Rodríguez v Google Inc,* courts would consider as manifestly illegal content such as child pornography, data that facilitates or instructs the commission of crimes, that might endanger people's lives or physical integrity, that promotes genocide, racism or discrimination with incitement to violence, that disrupts ongoing crime

[21] ENACOM, 'Bloqueo de sitios web (Website blocking)' <www.enacom.gob.ar/bloqueo-de-sitios-web_p3286> accessed 5 September 2021.

investigations, that constitutes a serious offense to honour, notoriously faked pictures, or that entails a serious and grave invasion to privacy by publishing images that intended to remain private, even if not sexual.

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

93. Government does not impose restrictions on anonymity or encryption for internet users, but registration requirements are in place for obtaining a mobile phone or a domain name.[22] No specific procedure is provided by law to request or order a social media intermediary to 'unmask' an anonymous speaker or identify an originator of content.

94. However, while government agencies do not systematically collect or access internet users' metadata directly, they may request it from service providers with a warrant, which has been upheld by the Supreme Court regarding information like geolocation data.[23] According to Law 25.520, interception of private communications requires judicial authorisation.

95. The Criminal Procedure Code states that, provided a judicial order, communication service providers must be able to intercept data for a period of up to 30 days, with the possibility of an extension.

## C. SECTION 2: ONLINE NEWS MEDIA

**a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?**

96. There is no special procedure for the government to order or request that an online news item must be removed from a website. Therefore, the government is bound by the general standards set by the Supreme Court in María Belén Rodríguez v Google Inc, which have been subsequently reaffirmed to date. Consequently, the government must either file a

[22] Freedom House, 'Freedom on the Net 2021' <www.freedomhouse.org/country/argentina/freedom-net/2021> accessed 24 September 2021.
[23] Corte de Justicia de la Nación [National Supreme Court] *Halabi Ernesto v PEN Ley 28.873*/amparo ley 16.986 [2009] CSJN (Arg).

reliable notice to the website for 'manifestly illegal content' – understood as described lines above– or obtain a judicial court order.

97. The regulator ENACOM has repeatedly stated that it lacks both the authority and the technical capacity to block websites, whatever their content or profile. Consequently, upon a judicial court order, ENACOM communicates the judicial measures to the Internet Service Providers (ISPs), who must comply accordingly.

**b) What are the tests or standards for determining whether an online news article/page needs to be removed?**

98. As noted above, the Inter-American case law underscores that political speech, speech involving matters of public interest, and speech regarding public officials in the performance of their duties and candidates for public office are specially protected due to their importance in the exercise of all other human rights or for the consolidation, operation, and preservation of democracy.[24] Remarkably, the Inter-American Commission on Human Rights has considered that media digital platforms are public sources of information and dissemination of opinions and ideas on matters of public interest, and therefore cannot be subject to a de-indexing order nor to the suppression of online content regarding matters of public interest.[25]

99. In its decision in the case of Newspaper La Nación (Mauricio Herrera Ulloa) v Costa Rica, the Inter-American Commission on Human Rights determined that by ordering the removal of a series of critical articles regarding a public official from a newspaper's website, the State violated Article 13 of the American Convention. The Commission understood that such measures are prohibited 'even if it is supposed to prevent by that means a possible abuse of freedom of expression', and held that the judicial order for removal violated both the journalist's freedom of expression as well as 'the right of everyone to be well informed'.[26]

[24] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Annual Report' Ch III (25 February 2009) OEA/Ser L/V/II.134, Doc 5 rev 1 [232].
[25] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open, and Inclusive Internet' (15 March 2017) OEA/Ser L/V/II, [138].
[26] *Complaint before the Inter-American Court on Human rights against Costa Rica,* Case No 12.367 'La Nación' Mauricio Herrera Ulloa and Fernán Vargas Rohrmoser (28 January 2002) Inter-Am Commission, [97].

100. Argentinian courts have incorporated the Inter-American standard of 'public interest' and considered the 'journalistic relevance' of allegedly infringing information when assessing whether a particular search result, thumbnail or page should be de-indexed or removed.[27] Considering the authority of the Inter-American system in the Argentinean legal system, it is probable that the above-mentioned standards would be taken into account in the context of online news media.

### c) Is the order of a court/tribunal a prerequisite for removal of online content?

101. According to the Supreme Court's decision in *María Belén Rodríguez v Google,* if the content involves 'manifest illegality', a private notification to the intermediary is sufficient. Such manifestly illegal material would be child pornography, data that facilitates or instructs the commission of crimes, that might endanger people's lives or physical integrity, that promotes genocide, racism or discrimination with incitement to violence, that disrupts ongoing crime investigations, that constitutes a serious offense to honour, notoriously faked pictures, or that entails a serious and grave invasion to privacy by publishing images that intended to remain private, even if not sexual.

102. Any other content which is not ostensibly or patently illegal requires a judicial order.

## D. SECTION 3: OTT PLATFORMS

### a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?

103. Other than being required to register as film distributors and for tax purposes, OTT platforms are largely unregulated. The Argentine Digital Law (N. 27.078), which establishes the general framework for information and communication technologies, explicitly excludes any type of content regulation, while the Audiovisual Communication Services Law, as amended by Decree No. 267/2015, does not refer to OTT platforms. However, the government is currently considering various online video regulatory frameworks. Some of the bills include the provision of a minimum quota for local content and tax incentives to

[27] See also Corte Suprema [Supreme Court], *Páquez, José v Google Inc s/ medidas precautorias*, CIV 23410 / 2014. / 3 /RH2; Juzgado Nacional de Primera Instancia en lo Civil [First Instance Court], *Natalia Ruth Denegri v Google Inc s/ derechos personalísimos*, Expte N 50.016/2016.

promote national productions. If passed, the proposals would allow the regulator ENACOM to determine how local content must be included.

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?**

104. There is no specific procedure under the law that allows the government to order an OTT platform to remove or modified content. Considering the constitutional framework and caselaw, a judicial order would probably be required.

# AUSTRALIA

## A. SECTION 1: SOCIAL MEDIA INTERMEDIARIES

105. Australia's laws regulating social media intermediaries – and online content more widely – are currently undergoing change. The Online Safety Bill recently received royal assent and is scheduled to come into force in early 2022. This will significantly affect regulation of online content in Australia, increasing government regulatory powers, reach, and scope. Prior to implementation, there are various regulatory laws and frameworks currently governing this area, including the Enhancing Online Safety Act 2015, the Broadcasting Services Act 1992, and the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019. The following sections will encompass both the present and forthcoming situations.

### a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?

106. There are various circumstances in which social media intermediaries may be held liable under Australian law for content posted by their users. Different areas of the law have developed their own rules and thresholds for intermediary liability independently here, resulting in a confusing landscape.[28] As a general rule, Australia is classed as an 'actual knowledge' jurisdiction, whereby liability is imposed in line with awareness: i.e., social media intermediaries are liable for the information they are deemed to have knowledge of (and therefore have the ability to remove). However, how such 'knowledge' or 'awareness' is defined in practice is complex and multifaceted, differing both across and within different areas of the law. This section will outline the areas of the law in which intermediaries can be held liable and the corresponding thresholds of liability that they must meet for this to occur.

#### 1) Civil Liability

107. Civil liability has been imposed on grounds of consumer protection, defamation, vilification, and copyright infringement:[29]

[28] Kyle Pappalardo and Nicholas Suzor, 'The Liability of Australian Online Intermediaries' in Giancarlo Frosio (ed), *Oxford Handbook of Intermediary Liability* (OUP 2020) 236.
[29] ibid.

*i) Consumer Protection*

108. Under consumer protection law, online intermediaries can be held liable for content published by site users where it contains misleading or deceptive information. The key case determining liability in this area is *Google Inc. v ACCC*.[30] Here, the Australian High Court held that intermediaries are only liable for content they have 'endorsed', ruling that Google could not be held liable for misleading advertisements appearing in their search result pages as merely providing an advertisement hosting system did not in itself class as endorsing the content of said adverts. In holding that the content host must 'itself engage in misleading or deceptive conduct, or endorse or adopt the representations which it displayed on behalf of advertisers', the High Court here set a high threshold for liability: requiring actual wrongful conduct on the part of the defendant, rather than just awareness of said conduct.[31] This therefore goes beyond an actual knowledge approach, requiring an active fault element from the intermediary.

109. However, other parts of the judgment in ACCC were less conclusive on this requirement, leaving it difficult to pinpoint exactly when liability will be imposed. This is because much of the judgment focused on the specific arguments made in the case: ACCC made a narrow case, pleading that Google itself made the misleading representations and so suing them on these grounds. However, had they argued that Google had misled the public by publishing said representations (through developing the advertising system and so providing a platform by which the misleading content could be created and reproduced), members of the court noted that liability might well have been imposed.[32]

*ii) Defamation*

110. Social media intermediary liability for defamation is covered by the same regulatory framework as governs other forms of mass media. This means that social media intermediaries are held liable for defamatory content posted on their sites if they are deemed to have 'published' it.[33] As with consumer protection, this requires the host site to have an

[30] *Google Inc. v Australian Competition and Consumer Commission* (2013) 249 CLR 435.
[31] ibid 73 (French CJ, Crennan and Kiefel JJ).
[32] ibid 117 (Hayne J).
[33] Kyle Pappalardo and Nicholas Suzor, 'The Liability of Australian Online Intermediaries' in Giancarlo Frosio (ed), *Oxford Handbook of Intermediary Liability* (OUP 2020) 240.

active role with regards to the content. For example, under *Bleyer v Google*, merely producing search results through an algorithm did not make Google a publisher of said results.[34]

111. However, publication by omission is possible if the secondary actor is deemed to have 'consented to, or approved of, or adopted, or promoted, or in some way ratified, the continued presence of that statement … in other words … [if there is] an acceptance by the defendant of a responsibility for the continued publication of that statement'.[35] In practice, this has required something in addition to mere hosting of content. For example, in *Visscher v Maritime Union* the host's use of the words 'read full story' in conjunction with a defamatory account was deemed to imply that the defamatory content was true;[36] while in *Duffy v Google Inc.*, the South Australian Supreme Court held Google liable for defamatory content contained within brief lines of information posted alongside search result links.[37]

112. Hosts sued for defamation may be able to defend against intermediary liability here if they are deemed to have innocently disseminated the content in question. This defence applies to those deemed to lack actual or constructive knowledge of the content of the defamatory material.[38]

*iii) Vilification*

113. The law on intermediary liability for online vilification is set out under the Racial Discrimination Act 1975. Under Section 18C, this makes it unlawful to 'do an act' that is reasonably likely to 'offend, insult, humiliate or intimidate' a person or group where that act is motivated by 'race, colour or national or ethnic origin'. For a social media host to be held liable under this, they must be deemed to have published the vilificatory content in question. Again, the case law here is ambiguous as to what exactly this means. The Court in *Silberberg* made it clear that it is possible to publish by omission, i.e., by hosting facilities that allow others to post vilificatory comments and then failing to remove said comments, but that this requires actual knowledge on the part of the host regarding the existence of the offensive content, and then that the failure to remove said content is motivated by discrimination.[39]

---

[34] *Bleyer v Googe Inc.* (2014) NSWSC 897.
[35] *Urbanchich v Drummoyne Municipal Council* (1991) Aust. Torts Rep. 81 [7] (Hunt J).
[36] *Visscher v Maritime Union of Australia* (No. 6) NSWSC 350, 30.
[37] *Duffy v Google Inc.* [2015] SASC 170.
[38] Kyle Pappalardo and Nicholas Suzor, 'The Liability of Australian Online Intermediaries' in Giancarlo Frosio (ed), *Oxford Handbook of Intermediary Liability* (OUP 2020) 240.
[39] *Silberberg v Builders Collective of Australia Inc.* (2007) 164 FCR 475.

114. There is some confusion in the case law as to in what circumstances exactly this motivation will be found. The Court in *Silberberg* seemed to require explicit evidence, holding on the facts that there was insufficient evidence that the failure to remove said comments was 'because of the race, colour or national or ethnic origin', as it might instead have been caused by a lack of due diligence or inattention, and therefore finding the intermediary not liable.[40] In contrast, in *Clarke v Nationwide News* the Court allowed a greater degree of imputation, finding that there was such evidence on the facts as, where the intermediary 'actively solicits and moderates contributions from readers', the 'offence will be given as much by the respondent in publishing the offensive comment as by the original author in writing it', thereby inferring the intention from the overall operating procedures, even without evidence for the specific content in question.[41]

115. Specifying the exact circumstances under which liability will be founded here is therefore difficult: Social media intermediaries will be held liable for vilificatory content posted on their sites, but only where the failure to remove it is deemed to be due to their own discriminatory intent. Important in deciding this would seem would be the strength of moderation. As social media intermediaries tend not to actively solicit and moderate contributions to content in the same way as news providers like Nationwide – but rather provide a platform upon which others to do so – it seems unlikely that they would meet this presumption, leaving them likely instead to fall under *Silberberg* and so requiring actual evidence that the failure to remove is due to discriminatory intent.

*iv) Copyright*

116. This is governed by the Copyright Act 1968. Under Sections 36(1) and 101(1), intermediary liability for copyright breach requires the social media host to have 'authorised' the breaching content. This is assessed as a question of fact, according to all of the circumstances. In *UNSW v Moorhouse*, authorise was defined as 'sanction', 'approve' or 'countenance', with Justice Gibbs setting out a three-fold test requiring the host to:[42]

a) have control over the means by which the copyright infringement is committed, and make it available to other persons,

[40] ibid 486 (Gyles J).
[41] *Clarke v Nationwide News Pty Ltd* (2012) 289 ALR 345.
[42] *University of New South Wales v Moorhouse and Angus & Robertson (Publishers) Pty Ltd* (1975) 133 CLR 1 [14] (Gibbs J).

b) know (or have reason to suspect) that said means are likely to be used for the purposes of an infringement, and
c) fail to take reasonable steps to limit its use to legitimate purposes.

117. Sections 39B and 112E provide an exception to this for intermediaries that are deemed to be a 'mere conduit', whereby they will not be held to have authorised infringement of copyright purely by having provided the facilities by which the copyright infringement communication was made.

*v) Online Safety Bill 2021*

118. In addition to the above, a further route to civil liability will come into force in 2022 under the forthcoming Online Safety Act.[43] This will impose civil liability upon online intermediaries, including social media intermediaries, for several pre-defined categories of content, as enforced by the eSafety Commissioner. These are: cyber bullying media targeting an Australian child, cyber-abuse material targeting an Australian adult, non-consensually posted intimate images, posts containing Class 1 and 2 material, content breaching industry codes, and 'abhorrent violent material'. The liability standard here is one of actual knowledge, whereby social media intermediaries will be liable for any content in the above categories regarding which they have received a notice from the eSafety Commissioner and then failed to remove within the statutory time limit. Other evidence of content being brought to the intermediary's attention, such as a user complaint, are also sufficient here in proving actual knowledge.

*vi) Limitations to liability*

119. Liability in this area is however limited under Clause 91(1) of Schedule 5 of the Broadcasting Services Act 1992, which renders any State or Territory legislation and any rule of common law or equity invalid to the extent that it:

a) subjects internet hosts or ISPs to criminal or civil liability for hosting or transmitting content where the host is not aware of the nature of the content; or
b) requires an internet host or ISP to monitor, make inquiries about, or keep records of, content hosted or transmitted.

[43] Online Safety Bill 2021.

120. In practice, this provision is as yet generally untested, and it is therefore difficult to say for certain how much of a limitation of liability it poses.

121. Overall then, there is no uniform standard according to which civil liability will be imposed. Rather, it varies according to the action in question, with the lowest threshold requiring that the intermediary is simply aware of something on their platform, as under the Online Safety Bill, and the highest requiring an active intentional fault element on behalf of the intermediary, as under the law on vilification.

### 2) Criminal Liability

*i) Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*

122. Passed in response to the live Facebook streaming of the Christchurch attack, this created new offences and categories of liability for social media hosts who fail to remove abhorrent violent material quickly enough after it is posted.[44] Of relevance here is Section 474.34, which leaves social media platforms criminally liable if they fail to 'ensure the expeditious removal of' or 'expeditiously cease hosting' 'abhorrent violent material' (although the timeframe for 'expeditious' is not specified).

123. Abhorrent violent material is defined as audio, visual, or audio-visual material that records or streams abhorrent violent conduct that reasonable persons would regard as being offensive, where that material is produced by a person engaged in the abhorrent violent conduct.[45] Abhorrent violent conduct is exhaustively defined as covering terrorist acts, murder or attempted murder, torture, rape, or kidnapping.[46] The Act requires the written consent of the Attorney-General before proceedings for an offence against these provisions can be initiated.[47] The offence attracts penalties of up to 3 years imprisonment and $2.1 million for individuals and up to $10.5 million or 10% of the annual turnover of a body corporate.[48]

---

[44] Robyn Chatwood, 'Australia suddenly passes new laws regulating streaming of abhorrent violent material by ISPs and other content providers' (*Dentons,* 15 April 2019) <www.dentons.com/en/insights/alerts/2019/april/15/australia-suddenly-passes-new-laws-regulating-streaming-of-abhorrent-violent-material#fn13> accessed 16 September 2021.
[45] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, s 474.31.
[46] ibid s 474.32.
[47] ibid s 474.42.
[48] ibid s 474.34.

124. There are defences to this under Section 474.37 where the material is:

a) required for enforcing or complying with the law
b) needed for proceedings in a court or tribunal
c) necessary for conducting scientific, medical, academic or historical research, or news or current affairs reporting that is 'in the public interest' and is made by a person working in a professional capacity as a journalist
d) needed for a public official's duties; or
e) related to the development, performance, exhibition or distribution in good faith of an artistic work.

125. In establishing such a defence, the social media host bears the evidential burden.[49] The Act also includes an exception under the Constitutional right of political communication, whereby the new offences do not apply to the extent (if any) that they would infringe any constitutional doctrine of implied freedom of political communication.[50]

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

126. Under the Enhancing Online Safety Act 2015, the Australian government established the office of the eSafety Commissioner.[51] This is an independent statutory office supported by the Australian Communications and Media Authority (ACMA) which is responsible for keeping Australians safe online, and is therefore free from government direction. The Commissioner has various statutory powers under which they can issue a removal notice for online content.

*i) The Broadcasting Services Act 1992:*

127. Under Schedule 5 and Schedule 7, the eSafety Commissioner has the power to ban certain types of content from being hosted on sites located within Australia. Such content can either be referred to the commissioner through the complaints process (which places the Commissioner under an obligation to investigate the content in question and determine whether it does in fact pertain to prohibited content), or it can be found and investigated by

[49] Criminal Code Act 1995, s 13.3.
[50] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, s 474.38.
[51] Enhancing Online Safety Act 2015, s 13.

the Commissioner using their own initiative. Prohibited content is defined under Schedule 7 of the Broadcasting Services Act to cover that which is:

a) RC (i.e., refused classification by the Classification Board under the Classification (Publications, Films and Computer Games) Act 1995): In practice this covers content that is 'very high in impact and falls outside generally-accepted community standards'.[52] The full details for this, and the standards for different categories of content, are set out in the National Classification Code, as enforced under Section 6 of the Classification (Publications, Films and Computer Games) Act 1995). In general, for content to be refused classification, it must:
    i. Depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that offends against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified;
    ii. or describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not);
    iii. or promote, incite or instruct crime or violence
b) Classified X18+: This covers material that involves non-violent sexually explicit content including actual sexual intercourse or other sexual activity between consenting adults.
c) Classified R18+: This includes any content not in the above category that is deemed unsuitable for a minor to see where the showing system is not protected by an adult verification system.
d) Classified MA15+: This contains elements such as sex scenes and drug use that could have a strong impact on the viewer, where the users has paid to access the content and it is not protected by an adult verification system.

128. If the investigated content fits these criteria (i.e., is prohibited), then the Commissioner will issue a removal notice that the content be taken down.[53] If it is not yet classified as such, but the Commissioner deems that were it classified it would fall under one of these

[52] Department of Infrastructure, Transport, Regional Development and Communications, 'What do the ratings mean?' (Australian Classification) <www.classification.gov.au/classification-ratings/what-do-ratings-mean> accessed 30 August 2021.
[53] Broadcasting Services Act 1992, sch 7.

categories, they will issue an interim notice that the content be taken down and further send a classification request to the Classification Board, then sending a final take-down notice post-classification.[54] Upon receiving such a notice, the content must be removed by 6pm the next business day. If the host is outside of Australia, they are instead added to a blocklist of banned URLs which are then added to filtering software that must be offered to all consumers by their internet service providers.[55]

*ii) Enhancing Online Safety Act 2015*

129. Under this, the eSafety Commissioner can issue a removal notice for certain types of content:

a) Cyber-bullying material targeting an Australian child: To qualify under this, two conditions must be met.[56] Firstly, the material to be taken down must be of such a nature that 'an ordinary person would conclude that it is likely that the material was intended to have an effect on a particular Australian child'. Secondly, it must be such that 'an ordinary person would conclude that … the material would likely have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child'. If these conditions are fulfilled, the process of removal then depends on the tier under which the social media host is classified. Tier 1 services are generally smaller services, Tier 2 are generally either larger services, or smaller services that have had their Tier 1 status revoked through non-compliance with previous removal requests.[57]

    i. Tier 1 services participate in the scheme on a cooperative basis and so are served removal requests with which they have the choice whether or not to comply with (although, if they repeatedly fail to comply with such requests over a 12-month period, they may have their Tier 1 status revoked and instead be classified as Tier 2.[58]

    ii. Tier 2 services are also served removal requests from the Commissioner. However, they have a legally binding duty to comply and may be subject to civil penalties if they fail to do so.[59]

[54] ibid.
[55] ibid sch 5.
[56] Enhancing Online Safety Act 2015, s 5.
[57] eSafety Commissioner, 'Social media Tier Scheme' (eSafety Commissioner, date unknown) <www.esafety.gov.au/about-us/who-we-are/social-media-tier-scheme> accessed 30 August 2021.
[58] Enhancing Online Safety Act 2015, s 18.
[59] ibid.

b) Non-consensually shared intimate images: Under Division 3, this covers any post, or threat to post, of an intimate image without the consent of the party depicted in said image. Intimate image is defined as any still or moving visual image either depicting or appearing to depict the party's genital or anal area (whether bare or covered by underwear), breasts (for female or transgender/intersex individuals identifying as female); or the party performing a private activity (exhaustively covering: being in a state of undress, using the toilet, showering, having a bath, engaged in a private sexual act, or engaging in any other like activity), in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.[60] These must be removed within 48 hours after a removal notice, regardless of tier status.[61]

130. These categories will be added to, and the removal process amended, by the forthcoming Online Safety Act:

*iii) Online Safety Act – Forthcoming*

131. As explained above, this will come into force in 2022. It updates the current take-down powers, both amending the removal process set out by the Enhanced Online Safety Act and conferring additional categories:

a) Cyber-bullying Scheme: As with the above provisions under the EOSA, this provides for the removal of material that is harmful to Australian children. In this, the material is defined in the same way as under the EOSA, but the take-down time is decreased from 48 to 24-hours and the scheme is extended to more services.[62]
b) Adult Cyber-abuse Scheme: This provides for the removal of material that seriously harms Australian adults. It aims extend similar protections as in the child cyber-bullying scheme to adults but sets a higher threshold of harm by virtue of their deemed higher level of resilience. Here, content is deemed to qualify as cyber-abuse (and therefore may warrant a removal notice) where it fits two conditions.[63] Firstly, that an ordinary person would conclude that it is likely that the material was intended to have the effect of causing serious harm to a particular adult. Serious harm here is defined as serious physical harm or serious harm to a person's mental health (including serious

[60] ibid s 9B.
[61] ibid s 44D.
[62] Online Safety Bill 2021, s 65.
[63] ibid s 7.

psychological harm and serious distress), whether temporary or permanent.[64] Secondly, that an ordinary reasonable person in the position of the Australian adult would regard the material as being, in all the circumstances, menacing, harassing or offensive.

c) Image-based Abuse Scheme: This provides for the removal of intimate images shared without the depicted person's consent. This scheme reflects the current regime in the EOSA with regards to the nature of the content covered, but it reduces the take-down time for such material from 48 to 24 hours.[65]

d) Online Content Scheme: This provides for the removal of harmful material in certain circumstances. This scheme reflects and simplifies the current regime in Schedules 5 and 7 of the Broadcasting Services Act, with some clarifications of the material and providers of services captured by the scheme. Content covered by this scheme must be removed within 24-hours of the Commissioner making a removal notice.[66] The content covered by this is:

    i. Class 1 Material: This covers that which is:
        a. Classified as RC (as defined at [23.a] above)
        b. or if not yet classified, likely to be classified as RC.
    ii. Class 2 Material. This covers that which is:
        c. Classified X 18 + material (as defined at [23.b])
        d. or if not yet classified, likely to be classified as X 18 +.
        e. Classified R18+ material (as defined as [23.c])
        f. or if not yet classified, likely to be classified as R18+.

e) Abhorrent Violent Material Blocking Scheme: This provides for the blocking of abhorrent violent material This scheme is new, but mirrors existing legislation in the Criminal Code Act 1995. The content covered under this is abhorrent violent material.

132. These standards are governed by the eSafety Commisioner's Office. There is however a right to appeal, under Section 220, whereby the Commissioner's decisions can be referred to the Administrative Appeals Tribunal, which then performs an independent merits review.

*iv) Criminal Code Amendment Sharing of Abhorrent Violent Material Bill*

133. Mirroring the Abhorrent Violent Material Blocking Scheme in the Online Safety Act, this gives the Commissioner the power to issue written notice regarding abhorrent violent

[64] ibid s 5.
[65] ibid s 77.
[66] ibid s 109, s 119.

material. This places content hosts 'on notice', creating a presumption against the host in any later court case, and so effectively leaving them criminally liable if they fail to remove it.[67]

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

134. Australian Courts can order content falling under the categories outlined in Section 1, part a) of this report to be removed: i.e., that which is deemed to be defamatory, infringing copyright, breaching consumer protection, and vilificatory.

135. Similarly, illegal content under the Criminal Law – be it inciting or promoting suicide under the Suicide Related Materials Offences Act 2006, child pornography or child abuse under the Criminal Code Act 1995 or abhorrent violent material under Criminal Code Amendment Sharing of Abhorrent Violent Material Bill – can be subject to a court-order of removal.

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

136. The courts are able to request unmasking information where necessary for enforcing legal regulations and ensuring justice. For example, in the 2020 *Kabbabe v Google* case, the Australian Federal Court ordered Google to unmask a defamatory anonymous online reviewer so as to allow Kabbabe to pursue a defamatory case against said reviewer.[68] Similarly, under copyright law, the Federal Court in 2015 made an order to iiNet and five other Australian ISPs requesting the information of 4,726 account holders of IP addresses believed to have infringed copyright of the film 'Dallas Buyers Club', so as to allow for compensation for the infringement to be recovered from them.[69]

137. Further, under the Online Safety Bill 2021, the eSafety Commissioner will gain identificatory and investigatory powers where necessary in aiding its investigations. In particular, Part 13 allows the Commissioner to request information about the identity of the end-user of a social media service and their contact details. Meanwhile, under Part 14, the Commissioner

[67] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, s 474.35.
[68] *Kabbabe v Google LLC* [2020] FCA 126.
[69] *Dallas Buyers Club LLC v iiNet Limited* [2015] FCA 317.

is able to summon witnesses to attend before them and produce documents and information regarding inquiries, which may also reveal identifying information about anonymous speakers and content originators. The Commissioner may also disclose this information to various other named bodies, including staff of ACMA, Royal Commissions, and the Federal Police, under Part 15.

## B. SECTION 2: ONLINE NEWS MEDIA

### a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?

138. The law here is the same as that governing social media content outlined above: the eSafety Commissioner is empowered under the Enhancing Online Safety Act 2015 and (will be empowered under the) Online Safety Bill 2021 to order that online news items must be removed where the content is deemed to be:

a) Cyber-bullying targeting an Australian child
b) Cyber-abuse of an Australian adult
c) Non-consensual intimate images
d) Class 1 and Class 2 content
e) Abhorrent Violent Material

139. The take-down process here is also the same as explained with regards to social media above. For news, however, there is a specific exemption under Article 104 of the Online Safety Bill 2021, with material exempt from removal where the material relates to a news report, or a current affairs report, that:

a) is in the public interest; and
b) is made by a person working in a professional capacity as a journalist

### b) What are the tests or standards for determining whether an online news article/page needs to be removed?

140. The standards here are the same as delineated above in Section 1 with regards to content on social media, i.e., as governed by the Broadcasting Services Act 1992, Enhancing Online Safety Act 2015, Criminal Code Amendment (Abhorrent Violent Material) Act 2019, and forthcoming Online Safety Bill 2021.

**c) Is the order of a court/tribunal a prerequisite for removal of online content?**

141. A court order is not prerequisite for the removal of online content, as the eSafety Commissioner can order that content be removed where it falls under the content categories dictated under the Broadcasting Services Act 1992, Enhancing Online Safety Act 2015, Criminal Code Amendment (Abhorrent Violent Material) Act 2019, and forthcoming Online Safety Bill 2021, subject to the Administrative Appeals Tribunal, as outlined above in Section 1.

## C. SECTION 3: OTT PLATFORMS

**a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?**

142. The Australian OTT sector is largely governed by the Broadcasting Services Act 1992. This has a two-part approach, with Schedule 5 governing content hosted outside of Australia and Schedule 7 content with an Australian connection. Combined, these set the standards for the kinds of content that can be hosted online, including both classified and unclassified content (the latter of which is treated on par with the rating it would be likely to get, were it classified). There are various restricted categories under this:

a) RC (or refused classification) which cannot be sold, advertised or imported in Australia
b) X 18+ which is restricted to adult viewing only due to its sexual nature
c) R 18+ which is restricted to adult viewing only due to its high impact nature
d) MA 15+ which is restricted to viewers over the age of 15 due to its high impact nature

143. Historically, the Australian Classification Board, in conjunction with ACMA, have been responsible for classifying content under these. However, this is currently an area of the law undergoing change, with Netflix receiving approval to self-classify its content using its own

tools, following a two-year pilot scheme. The (ongoing) monitoring program assessing this process found that Netflix's tool assesses and classifies content with 89% accuracy.[70] This then enables quicker and more efficient classification, allowing for content to be premiered in Australia without delay.

144. While other OTT platforms technically remain governed by the Board, many appear to have moved to a self-classification model in practice, with platforms including Stan, Disney+, Amazon, and free-to-air catchup TV services, all self-classifying at least some of their content.[71] While classification of online content is therefore technically in line with that of physical content, no action has been taken so far in response to this non-compliance (likely due to the massive practical difficulties for the Board that classifying such large amounts of content would pose).[72]

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?**

145. The process for modifying and removing content hosted by an OTT platform is the same as explained above with regards to removing content from a social media host or online news item, with the eSafety Commissioner also governing this area.

[70] Kurt Bryant, 'Submission to the Review of Australian classification regulation' (Communications AU, 19 February 2020) <www.communications.gov.au/sites/default/files/submissions/kurt-bryant.pdf> accessed 30 August 2021.
[71] ibid.
[72] ibid.

# CANADA

## A. SECTION 1: SOCIAL MEDIA INTERMEDIARIES

146. The Canadian government is currently considering a suite of new legislation to regulate how social media platforms moderate potentially harmful user-generated content. While recognising the benefits of social media, the government of Canada is seeking to amend its regulatory framework to tackle five types of harmful online content:
    a) child sexual exploitation content,
    a) terrorist content,
    b) content that incites violence,
    c) hate speech, and
    d) non-consensual sharing of intimate images.

147. The definitions of these terms draw upon existing Canadian law, including current offences and definitions in its Criminal Code, but are due to be modified in order to tailor them to a regulatory – as opposed to criminal – context. The government has stated that there are other online harms that could also be examined and possibly addressed through future programming activities or legislative action. It has also stated that any such activities will be balanced against considerations regarding freedom of expression, privacy protections, and the open exchange of ideas and debate online, as enshrined as fundamental rights in the Canadian Charter of Rights and Freedoms.[73]

148. In June 2021, the Canadian government passed Bill C-10 - a major component of its drive to update its regulatory regime for the social media era, and which thus receives attention in this section. Portrayed as the first significant update to the foundational Broadcasting Act in 30 years,[74] the Bill made headlines in May 2021 when a clause known as the social media exemption was removed, leading many to question whether Canada would soon be regulating user-generated content and social media platforms — for example, to require

[73] Government of Canada, 'Discussion page - The Government's proposed approach to address harmful content online', <https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html> accessed 9 October 2021.
[74] Parliamentary Secretary to the Minister of Canadian Heritage Julie Dabrusin, 'Debates of June 21st, 2021', <https://openparliament.ca/debates/2021/6/21/julie-dabrusin-3/> accessed 17 August 2021.

them to showcase Canadian content on their platforms. The Bill was passed in the House of Commons in June 2021 and thereafter moved on to the Senate.

149. It should be noted that after this section of the report was authored, the Bill died on the Order Paper when Canada's Parliament dissolved in mid-August prompting a snap election. Given that the bill may be reintroduced, the report still describes provisions of the bill. If reintroduced, however, the Bill will need to restart the full review cycle through Parliament.[75] It is likely that it will be reintroduced.

150. Bill C-10 aims to regulate programming distributed by media streaming services and social media platforms by adding 'broadcast undertakings' conducted over the internet to the regulatory scope of the Canadian Radio-television and Telecommunications Commission (CRTC).[76] The regulations will apply to services such as Crave, Tou.TV, Netflix, Amazon Prime, and Spotify,[77] but not to 'the content that people upload on social media … [which] won't be considered as programming under the Broadcasting Act and that … won't be regulated by the CRTC',[78] as clarified during the Bill's third reading:

> A person who uses a social media service to upload programs for transmission over the Internet and reception by other users of the service — and who is not the provider of the service or the provider's affiliate, or the agent or mandatary of either of them — does not, by the fact of that use, carry on a broadcasting undertaking for the purposes of this Act.[79]

151. The CRTC is Canada's regulatory agency for broadcasting and telecommunications. It acts as an 'administrative tribunal that operates at arm's length from the federal government' to

---

[75] Alexandra Lewis, 'Online Broadcasting Regulation in Canada: What will the future hold?', <https://www.lexology.com/library/detail.aspx?g=7653086c-db35-4db3-9ba5-f9431ee9c7b9> accessed 9 October 2021.

[76] Parliament of Canada, 'Legislative Summary of Bill C-10: An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts' <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/432C10E#a1> accessed 16 August 2021.

[77] Parliament of Canada, 'Legislative Summary of Bill C-10: An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts' <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/432C10E#a2> accessed 18 August 2021.

[78] Steven Guilbeault, Twitter post <https://twitter.com/s_guilbeault/status/1389314082088624134> accessed 18 August 2021.

[79] Parliament of Canada, 'Bill C-10 – Third reading' <https://parl.ca/DocumentViewer/en/43-2/bill/C-10/third-reading#ID0ENBBA> accessed 18 August 2021.

implement the laws and regulations set by Canada's parliament.[80] The CRTC has been described as notably less partisan than its American equivalent, the Federal Communications Commission (FCC), whose five commissioners are all presidential appointees. By contrast, in Canada, although CRTC commissioners are appointed by the government, the agency operates as more of an arm's-length judiciary and makes decisions based on evidence submitted during public consultations, rather than along political party lines.[81]

**a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?**

152. In Canada, there are limited circumstances where intermediaries are liable for user-posted content.

153. The Copyright Act 1985 was amended in 2012 by the Copyright Modernization Act to include a 'notice and notice' system, by which the host must pass on to its subscriber a notice of infringement received from a copyright owner. However, no other action is required, and immunity from liability is not contingent on taking down the infringing content. It is only liable if it does not pass on the notice.[82]

154. In the context of defamation, the relevant standards are those in common law, where the definition of publication has generally been broad and based on strict liability, allowing some intermediaries to be considered publishers.[83] However, increasingly, courts have been construing publication in a more limited way, indicating that some awareness of the nature of posts will be necessary to attribute liability. The Canadian Supreme Court in *Crookes v Newton*[84] argued that publication only occurs where the defendant performs a deliberate act that makes defamatory content 'readily available to a third party in a comprehensible form.' Moreover, the common law doctrine of publication by omission deals with cases where the defendant may be liable if despite not authoring a communication, the defendant can control

[80] Government of Canada, 'Canadian Radio-television and Telecommunications Commission', <https://crtc.gc.ca/eng/home-accueil.htm> accessed 16 August 2021.
[81] Matthew Braga, 'Why Canada's net neutrality fight hasn't been as fierce as the one in the U.S.', <https://www.cbc.ca/news/science/us-canada-net-neutrality-party-politics-fcc-crtc-fight-1.4447558> accessed 25 September 2021.
[82] Copyright Act 1985, ss. 41.25, 41.26 and 41.27(3).
[83] Emily Laidlaw and Hilary Young, 'Internet Intermediary Liability in Defamation' (2018) 56 Osgoode Hall Law Journal 112.
[84] [2011] 3 SCR 269.

it, refuses to remove it, and can be interpreted as endorsing it.[85] Another doctrine that allows an intermediary to claim immunity is the doctrine of innocent publication, which is available when (ii) there is no evidence that the service provider ought to have been aware of the alleged libel on their service, and (iii) committed no negligence in failing to find out about the libel in question.[86] In *Baglow v Smith*[87] (a case wherein the plaintiff sued a poster in an online forum in addition to the forum's administrators over an alleged defamatory statement), the Court held that the administrators could be held liable as publishers of the post as the plaintiff had alerted the administrators to the defamatory nature of the statement, and that the administrators chose not to remove it even though it violated the forum's rules against 'abusive' and slanderous material (although ultimately the defence of 'fair comment' was applicable and no liability was imposed).

155. Based on an assessment of common law principles of publication, Friends of Canadian Broadcasting argues that social media intermediaries like Facebook and YouTube are arguably publishers even before they are notified of the defamatory content, as their algorithms exercise control over content and the way they operate means that they have knowledge of the content before notified.[88]

156. Criminal wrongs relating to content are contained in the provisions of the Canadian Criminal Code that criminalize hate speech (Sections 319.1, 319.2) and defamation (Sections 297-315). However, it is difficult to attribute liability under these to intermediaries. Regarding online child sexual abuse material, a specific law (Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, 2011) applies to online platforms. It requires that they report to the Canadian Centre for Child Protection any tip-offs they receive regarding websites where child pornography may be publicly available, to notify police and to safeguard evidence if they believe that a child pornography offence has been committed using an Internet service that they provide.

157. As noted above, the proposed law, Bill C-10 would not consider the content that individual users post to online social media as a 'broadcast undertaking'. But the online platforms themselves would be required to proactively monitor all user speech and evaluate its

[85] *Byrne v Deane* [1937] 2 All ER 204.
[86] *Crookes v Newton* [2011] 3 SCR 269.
[87] 2015 O.N.S.C. 1175.
[88] Friends of Canadian Broadcasting, 'Platform for harm - Internet intermediary liability in Canadian law', September 2020, <platform-for-harm-2020-friends.pdf> accessed 9 October 2021.

potential for harm. Online communication service providers would need to take 'all reasonable measures to do whatever is within their power to monitor for the regulated categories of harmful content on their services, including through the use of automated systems based on algorithms',[89] and restrict its visibility.

158. The regulations will apply 'to any company operating in Canada, regardless of where they are registered, where their head offices are located or where their servers exist'. The proposed legislation includes administrative and monetary penalties for non-compliance, including failure to block or remove content. Regulators would have the power to impose 'very hefty fines' on companies deemed in violation.[90]

159. Under the proposed legislation, a reasonable suspicion of illegal activity would not be necessary for a service provider, acting on the government's behalf, to conduct a search of posted content; all content posted online would be searched. Potentially harmful content would be stored by the service provider and transmitted, in secret, to the government for criminal prosecution.

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

160. Currently, there is no specific procedure for the removal of content by the government. As discussed above, even under the copyright law, the intermediary does not have to take down content to avoid liability.

161. The new proposed legislation would apply to online communication service providers. The concept of online communication service provider is intended to capture major platforms, (e.g., Facebook, Instagram, Twitter, YouTube, TikTok, Pornhub), and exclude products and services that would not qualify as online communication services, such as fitness applications or travel review websites. The legislation would not cover private communications, nor telecommunications service providers or certain technical operators.

---

[89] Government of Canada, 'Discussion page - The Government's proposed approach to address harmful content online', <https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html> accessed 9 October 2021.

[90] Karen Pauls, Canadian Broadcasting Corporation, 'New rules on removal of illegal online content could help in battle against child pornography', <https://www.cbc.ca/news/canada/manitoba/canada-illegal-online-content-child-porn-1.5847695> accessed 17 August 2021.

162. Any individual (governmental or otherwise) would be able to flag content as harmful. The social media platform would then have 24 hours from initial flagging to evaluate whether the content is harmful, as per the five harms listed previously (child sexual exploitation content, terrorist content, content that incites violence, hate speech, and non-consensual sharing of intimate images). The social media platform would then be obliged to remove the content or respond by concluding that it is not harmful. However, previous research has shown that even in more lenient notice-and-takedown systems, platforms systematically err on the side of taking down *lawful* content in order to avoid risk to themselves, engendering a risk of 'over-compliance' and legally unnecessary removal of lawful content.[91]

163. Regulated entities would also be required to establish robust flagging, notice, and appeal systems for both authors of content and those who flag content. Once a regulated entity makes a determination on whether to make content inaccessible in Canada, they would be required to notify both the author of that content and the flagger of their decision, and give each party an opportunity to appeal that decision to the regulated entity. Regulated entities would also be compelled to be more transparent in their operations. Regulated entities would be required to publish information that they do not currently publish, with baseline transparency requirements set out in statute and further specified in regulation.[92]

164. The Digital Safety Commissioner of Canada would administer, oversee, and enforce the new legislated requirements noted above. It would also be mandated to lead and participate in research and programming, convene and collaborate with relevant stakeholders, and support regulated entities in reducing the five forms of harmful content falling under the new legislation on their services. The government envisions pro-active monitoring and reporting requirements, including a role for artificial intelligence (AI). For example, it calls for pro-active content monitoring of the aforementioned online harms, granting the Digital Safety Commissioner the power to assess whether the AI tools used are sufficient. The Commissioner would have powers to:

---

[91] Daphne Keller, 'Empirical evidence of over-removal by internet companies under intermediary liability laws: an updated list', <http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws> accessed 10 October 2021.

[92] Government of Canada, 'Discussion page - The Government's proposed approach to address harmful content online', <https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html> accessed 9 October 2021.

a) intake complaints from users,
b) proactively inspect for compliance, including compliance with decisions of the Digital Recourse Council of Canada, which would provide people in Canada with independent recourse for the content moderation decisions of regulated entities like social media platforms,
c) inspect cases of non-responsiveness and non-collaboration,
d) issue public reports on levels of compliance,
e) issue compliance orders,
f) in specific instances of non-compliance with legislative and regulatory obligations, recommend Administrative Monetary Penalties up to 10 million dollars, or 3% of an entity's gross global revenue, whichever is higher, for non-compliance to the Personal Information and Data Protection Tribunal proposed in the Digital Charter Implementation Act, 2020 (Bill C-11),
g) refer offences for non-compliance with certain statutory obligations to prosecutors with fines of up to $25 million, or 5% of an entity's gross global revenue, whichever is higher,
h) as an exceptional recourse, apply to the Federal Court to seek an order to require Telecommunications Service Providers to implement a blocking or filtering mechanism to prevent access to all or part of a service in Canada that has repeatedly refused to remove child sexual exploitation and/or terrorist content; and
i) collect and share information with other Government departments and agencies for the purposes of administering this and other Acts of Parliament.[93]

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

165. Making orders restricting speech on social media requires courts to undertake a delicate balancing of constitutional considerations. If the order is being made pursuant to legislation, courts must assess whether the activity in question is covered by a guarantee under the Canadian Charter of Rights and Freedoms. The assessment must be conducted in light of section 1 (reasonable limits on expression) to balance freedom of expression considerations with other constitutional values important in these cases, including *inter alia* those of privacy and protection of reputation. If the order is made pursuant to common law or equity (i.e.,

[93] ibid.

injunction), courts must ensure that the development and application of the common law and equity, and the exercise of discretion, comply with constitutional values.

166. Some attempts by courts to balance freedom of expression with restrictions on speech on social media are listed below:

a) *R v Lucas*, in which the Supreme Court of Canada considered whether the offence of publishing a libel known to be false violated section 2 of the *Charter*.[94] In doing so, it considered at length the importance of the protection of reputation in its section 1 analysis.

b) In 2015, the Supreme Court of Nova Scotia struck down the provincial Cyber Safety Act (CSA), intended to suppress cyber-bullying, on the grounds that it violated the Charter. In *Crouch v Snell,*[95] the respondent had engaged in a smear campaign over social media and was subsequently ordered to stop the behaviour, take down the offending posts, and refrain from contact with the claimant. The respondent's lawyers successfully challenged the order on the basis that the behaviour fell within section 2(b) of the Charter to the extent that it was non-violent, and the CSA restricted freedom of expression.

c) In *Callon v Callon,*[96] an interim order was made pursuant to s. 46(1) of the Family Law Act restraining a wife from sending letters to third parties containing scurrilous allegations against her husband. The wife appealed, arguing that the court exercised its discretion in a manner that violated freedom of expression. The court held that the order violated section 2(b) of the Charter, but that this was justified under section 1, as it considered the limited scope of the order and the important objective of the restriction of ensuring reasonable conduct of the litigation.[97]

167. Analysis by the Canadian Civil Liberties Association pointed to 'a somewhat restrained role for the law in addressing many of the harms that flow from communication, regardless of where or how that communication takes place'. Canada's courts have affirmed numerous times that the price of free expression is an obligation to tolerate expression that may be

[94] *R v. Lucas* [1998] 1 S.C.R. 439.
[95] *Crouch v. Snell*, 2015 NSSC 340 (S.C.) McDougall J.
[96] *Callon v. Callon*, (1999), 68 C.R.R. (2d) 350 (Ont. Div. Ct.).
[97] Deborah Chappel, 'Orders Referring to Social Media: The Positives and the Pitfalls, 2019 CanLIIDocs 3943', <https://www.canlii.org/en/commentary/doc/2019CanLIIDocs3943> accessed 9 October 2021.

offensive and even harmful.[98] In 2013, the Supreme Court held that publication of hate speech was not *ipso facto* unlawful: 'Hate speech legislation is not aimed at discouraging repugnant or offensive ideas. It does not, for example, prohibit expression which debates the merits of reducing the rights of vulnerable groups in society. It only restricts the use of expression exposing them to hatred as a part of that debate. It does not target the ideas, but their mode of expression in public and the effect that this mode of expression may have'.[99]

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

168. In Canada's legal system, the identity of anonymous wrongdoers can be unmasked by 'Norwich Orders'. A Norwich Order is an order for pre-action discovery: it is a way to compel the release of information before a claim is commenced. If an innocent third party such as a website has enabled the perpetrator to commit the wrong, a Norwich Order can be sought, and may compel the service provider to disclose information about an anonymous poster's real name, IP address, email address, etc. In Canada, applications for Norwich Orders are often unopposed. While most websites will not provide the identifying information of a wrongdoer in the absence of a court order, they will often choose not to oppose the order.

169. To grant a Norwich Order, the court must be satisfied that all of the following conditions are met:

a) Is there sufficient evidence of a valid, bona fide or reasonable claim against the wrongdoer?
b) Is the third party from whom the information is sought somehow involved in the acts complained of?
c) Is the third party the only practicable source of the information available?
d) Can the third party be indemnified for out-of-pocket costs to which it may be exposed because of disclosure? And

[98] Canadian Civil Liberties Association, 'Regulating social media: Into the unknown', <https://ccla.org/social-media-regulation/> accessed 16 August 2021.
[99] *Saskatchewan (Human Rights Commission) v. Whatcott* [2013] SCC 11, para 51.

e) Do the interests of justice favour disclosure?[100]

170. Norwich Orders are most commonly sought in cases where internet anonymity has facilitated the commission of wrongful acts, including defamation, cyber-bullying, copyright infringement, and fraud.[101] Once only rarely used, these types of orders are gaining traction in Canada and worldwide, as lawyers and litigants use them to locate and ultimately freeze flows of money across borders, to identify importers of patent infringing goods, and to put a name to an ISP address that may be involved in online activity that is tortious or fraudulent.[102]

171. The Investigating and Preventing Criminal Electronic Communications Act obliges telecommunications service providers to provide, under appropriate circumstances, Canadian law enforcement with users' subscriber information (name, address, telephone number, international mobile equipment identity number, etc.) when:

a) the officer believes on reasonable grounds that the urgency of the situation is such that the request cannot, with reasonable diligence, be made under subsection 16(1);
b) the officer believes on reasonable grounds that the information requested is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and
c) the information directly concerns either the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.

172. In *R v Spencer*, the Supreme Court of Canada examined whether the police could request internet users' subscriber information associated with an IP address from an ISP, on a voluntary basis under the Personal Information Protection and Electronic Documents Act and without prior judicial authorisation. The Court held that 'no, users have a reasonable expectation of privacy in their ISP subscriber information, as its disclosure will often identify

[100] Dorothy Charach, 'Practical Tips for Obtaining a Norwich Order', <https://www.mccarthy.ca/en/insights/blogs/snipits/practical-tips-obtaining-norwich-order> accessed 9 October 2021.
[101] Matthew Stroh, 'Norwich Orders: Getting Behind the Mask' <https://www.wagnersidlofsky.com/norwich-orders/> accessed 9 October 2021.
[102] Marie-Andrée Vermette and Nikiforos Iatrou, 'Norwich Orders in Canada: A Tool for Twenty-First Century Litigation' <https://www.weirfoulds.com/assets/uploads/6790_Reprint-NorwichOrders-Original.pdf> accessed 10 October 2021.

users with intimate or sensitive activities carried out online with the expectation of anonymity'.[103]

## B. SECTION 2: ONLINE NEWS MEDIA

173. Canadian law does not distinguish between the methods with which news is transmitted or broadcast. As such, news transmitted online is subject to the same protections and obligations as that circulated in, for instance, physical newspapers and magazines. The foundational legal instrument that enshrines freedom of expression in Canada is the Canadian Charter on Rights and Freedoms, in particular the provisions contained in Section 2(b) – 'freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication' – and Section 1, which prescribes the government's ability to place reasonable limits in order to protect other rights and freedoms or important national values. Media regulation in Canada therefore reflects a balancing act between these two important considerations.

174. Canada's communications regulatory regime is currently in a state of flux. Recent years have seen concerted attempts to update and modernise Canada's decades-old communications legislative framework. Foundational acts such as the Telecommunications Act and Broadcasting Act have become increasingly outdated in the internet age; historically, news content was only regulated by the Canadian Radio-television and Telecommunications Commission (CRTC) if it was delivered through licensees such as radio and television stations, and specialty news services, but Canadians are increasingly accessing news content online, which now consists of a mix of audio, audiovisual and text. A series of reviews, consultations, and new legislative proposals such as bills C-10 (to amend the Broadcasting Act) and C-36 (hate speech/crimes and propaganda), have the potential to re-shape the laws that regulate Canada's online environment in the years ahead. In a relatively dynamic situation, even the names of Acts and the CRTC have been targeted for modernisation: one review recommended the title of the Broadcasting Act should be changed to the Media Communications, and the CRTC should be re-branded as the Canadian Communications Commission (CCC).

[103] *R v Spencer* [2014] SCC 43 (CanLII), [2014] 2 SCR 212.

175. Canada's current online regulatory framework is a patchwork of legislation at both the federal and provincial/territorial level. Illegal content and conduct include behaviours that violate a wide range of laws, including child exploitation and abuse, terrorist content and activity, hate crimes, incitement of violence, sale of illegal products or services, cyber violence, harassment and stalking, or non-consensual sharing of intimate images. These issues may fall under federal laws, such as the Criminal Code, and may also be covered by a wide range of provincial or territorial legislation. Illegal content and conduct are related to, but distinct from, harmful content and conduct.

176. Each type of illegal activity is addressed through distinct legal frameworks that delineate the responsibilities of law enforcement agencies, and those creating and those sharing illegal content, as well as the responsibilities and obligations of a wide range of intermediaries that make the content available. All these obligations and responsibilities are balanced against human rights, particularly the right to privacy.[104]

**a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?**

177. As with social media, research for this report uncovered no specific statutory powers with which a Canadian government entity could order the removal of online news from any website in the absence of a court-issued removal order.

178. An indicative example of an attempt by the government to remove an item of online news is *R v Canadian Broadcasting Corporation*.[105] The underlying case involved a first-degree murder charge in Alberta in relation to a victim who was under 18 years of age. Under the Criminal Code, the court was required to issue a mandatory publication ban to protect the identity of the minor victim, which it did. However, a few days before the publication ban was ordered by the court, the Canadian Broadcasting Corporation (CBC) had already posted the victim's identity and photograph on its website. Following the publication ban, the CBC indicated that it would honour the court's order and not publish any further stories identifying the victim. However, it refused to remove from its website the stories that had been posted before the publication ban had come into effect. The Crown brought an application to the

[104] Innovation, Science and Economic Development Canada, 'Canada's communications future: Time to act' <http://www.ic.gc.ca/eic/site/110.nsf/eng/00012.html#Toc26977818> accessed 10 October 2021.
[105] *R v Canadian Broadcasting Corporation* [2018] SCC 5.

court asking that the CBC be found in contempt of court for ignoring the publication ban. It also sought an interim order that, pending the contempt hearing, the CBC be required to remove the pre-existing articles from its website in order to come into compliance with the publication ban. The Supreme Court of Canada ultimately agreed with the initial court and dismissed the motion for the injunction, coming down on the side of favouring freedom of the press and expression over the importance of protecting the privacy rights of victims of crime.[106]

179. A review of Canadian case law reveals a combination of both pre-internet provisions of the Criminal Code and more modern post-internet amendments that have been applied to abusive and offensive content online. A significant component of Canada's criminal law response to problematic content on the internet has focused on protecting children from sexual exploitation and luring. However, technological change and innovation also spurred concerns around hate propagation (and terrorism), voyeurism, non-consensual distribution of intimate images and advertising sexual services that informed some of the more significant amendments to the Criminal Code between 2001 and 2015.

180. The criminal offences that may be applied to online content that could be categorised as abusive and/or offensive include (in alphabetical order by topic):

a) counselling suicide (section 241);
b) criminal harassment (section 264);
c) defamatory libel (section 298);
d) extortion (section 346);
e) fraudulent, false and harassing communications (sections 371, 372);
f) hate propagation (sections 318, 319);
g) human trafficking and advertising sexual services (sections 279.01, 279.02, 286.4);
h) identity fraud (section 403);
i) intimidation (section 423);
j) mischief in relation to data (section 430);

[106] John Polyzogopoulos, 'Removing Offending Content from the Internet Just Became Harder' <https://www.blaney.com/Removing-Offending-Content-from-the-Internet-Just-Became-Harder?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration> accessed 10 October 2021.

k) non-consensual distribution of intimate images (section 162.1);

l) obscenity (section 163);

m) uttering threats (sections 264.1 and 265); and

n) voyeurism (section 162).[107]

181. Under proposals to amend Canada's Criminal Code, Bill C-10, referenced above, would provide that all regulated Online Communication Services (OCSs) and Online Communication Service Providers must take all reasonable measures, which can include the use of automated systems, to identify harmful content that is communicated on its OCS and that is accessible to persons in Canada, and to make that harmful content inaccessible to persons in Canada, as may be prescribed through regulations by the Digital Safety Commissioner, on approval by the Governor in Council.

182. The Digital Safety Commissioner would have broad powers to order the OCSs 'to do any act or thing, or refrain from doing anything necessary to ensure compliance with any obligations imposed on the OCSP by or under the Act [amended by Bill C-10] within the time specified in the order.' The Digital Safety Commissioner may conduct inspections of OCSPs at any time, on either a routine or ad hoc basis, further to complaints, evidence of non-compliance, or at the Digital Safety Commissioner's own discretion, for the OCSP's compliance with the Act, regulations, decisions and orders related to a regulated OCS.[108]

**b) What are the tests or standards for determining whether an online news article/page needs to be removed?**

183. In *CBC*, described above, the Supreme Court of Canada confirmed that requiring a party to remove content from the internet constitutes a 'mandatory injunction', not a prohibitory one. The difference is critical, because the Court also confirmed that the test to obtain a mandatory injunction is more difficult to meet than the test to obtain a prohibitory injunction.

[107] Jane Bailey, 'Abusive and Offensive Speech Online: An Overview of Canadian Legal Responses Focusing on the Criminal Law Framework' <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/Canada-J-Bailey.pdf> accessed 10 October 2021.

[108] Michael Geist, 'Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation' <https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/> accessed 18 August 2021.

184. A prohibitory injunction is an order requiring someone to refrain from doing something in breach of another's rights. Examples are orders prohibiting a party from trespassing on the property of another or prohibiting a party from contacting another's customers. For prohibitory injunctions, the well-known test laid out in the seminal 1994 decision of the Supreme Court in *RJR-MacDonald Inc v Canada (Attorney General)* applies.[109] Under that test, a plaintiff is required to prove that:

a) there is a serious question to be tried;
b) the plaintiff will suffer irreparable harm; and
c) the balance of convenience favours the plaintiff.

185. A mandatory injunction is one that requires a party to take some positive action. As the SCC put it in *CBC*, 'a mandatory injunction directs the defendant to undertake a positive course of action, such as taking steps to restore the status quo, or to otherwise "put the situation back to what it should be", which is often costly or burdensome for the defendant and which equity has long been reluctant to compel'. Examples of mandatory orders are an order requiring a party to continue to supply another with product under a contract, to require the delivery of property to another, or to take down a fence.

186. For mandatory injunctions, the first element of the test is more stringent. The plaintiff must do more than show that it has an arguable case. The plaintiff must show that he or she has a 'strong *prima facie* case'. In *CBC*, the SCC described the meaning of 'strong *prima facie* case' as, among other things, a case with a 'strong and clear chance of success' or a case where a plaintiff is 'almost certain' of success. The SCC concluded that a plaintiff has a burden 'to show a case of such merit that it is very likely to succeed at trial'. In short, before a plaintiff can obtain an interim mandatory injunction, it must show that it is almost assured of victory at trial – a high burden.[110]

### c) Is the order of a court/tribunal a prerequisite for removal of online content?

[109] *RJR-MacDonald Inc v Canada (Attorney General),* [1994] 1 SCR 311.
[110] John Polyzogopoulos, 'Removing Offending Content from the Internet Just Became Harder' <https://www.blaney.com/Removing-Offending-Content-from-the-Internet-Just-Became-Harder?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration> accessed 10 October 2021.

187. Under the current system, only courts can order removal of online content. Under the proposed legislative and regulatory framework envisaged by lawmakers seeking to modernise Canada's communications regulations (using amendments such as Bill C-10), harmful content posted online could be addressed through a myriad of takedown requirements, content filtering, complaints mechanisms, and even website blocking, much of which can occur before the involvement of any court or tribunal.[111] As such, compliance mechanisms would consist of a combination of voluntary self-regulation by media platforms and industry, legislative provisions, and the enforcement powers of the Digital Safety Commissioner of Canada.

## C. SECTION 3: OTT PLATFORMS

188. In its definition of OTT platforms, the Canadian Radio-Television and Telecommunications Commission (CRTC) 'considers that Internet access to programming independent of a facility or network dedicated to its delivery (via, for example, cable or satellite) is the defining feature of what have been termed 'over-the-top' services'.[112]

189. Current legislative proposals seek to bring some online services under the regulatory purview of an updated Broadcasting Act, depending on the nature of the services they provide. In the same manner as described above in the section on social media intermediaries, individuals posting user-generated content to OTT platforms like YouTube are, and will remain, exempt from the CRTC's regulatory purview, but the platforms themselves would be subject to the provisions of the Act. Bill C-10 'in no way prevents online streaming services from operating in Canada or requires them to be licensed'.[113]

### a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?

[111] Michael Geist, 'Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation' <https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/> accessed 18 August 2021.
[112] CRTC, 'CRTC – Convergence Policy, Policy Development and Research: October 2011' <https://crtc.gc.ca/eng/publications/reports/rp1110.htm#ftn2> accessed 10 October 2021.
[113] Government of Canada, 'Frequently asked questions — Modernizing the Broadcasting Act for the Digital Age' <https://www.canada.ca/en/canadian-heritage/services/modernization-broadcasting-act/faq.html#a11> accessed 18 August 2021.

190. The proposed amendments to the Broadcasting Act clarify that an online service that primarily offers curated audio or audio-visual content (including OTT platforms) that intends to inform, enlighten or entertain is subject to the Act, regardless of whether the content is streamed or accessed on demand. Therefore, OTT services such as Crave, Tou.TV, Netflix, Amazon Prime, and Spotify would be subject to the Act and could be required to contribute to the Canadian broadcasting system and highlight Canadian-created media under the same obligation as traditional broadcasters. Historically, traditional broadcasters like television networks had complained that the reduced levels of regulation enjoyed by OTT platforms conveyed an unfair competitive advantage.

191. Under the proposal, the CRTC would be granted greater powers and flexibility to ensure online services contribute to the domestic funding system. The CRTC will be given 'express powers to require broadcasting undertakings, including online undertakings, to make financial contributions to support Canadian music, stories, creators and producers.' In addition, the bill would give the Commission the power to impose "conditions of service" ordering online broadcasters to support the discoverability of Canadian content; compelling foreign-based digital services to contribute to the creation of domestic content has been one of Canadian media's dominant storylines for a decade. The bill would also oblige OTT platforms to share information with the CRTC, but in a situation where the Commission might request commercially sensitive data, the bill noted the information would be protected. The bill also proposes that the Broadcasting Act be updated to better reflect Indigenous peoples, persons with disabilities and Canada's diversity in the broadcasting system.[114]

192. The Bill provides the CRTC with new enforcement powers through an administrative monetary penalty scheme (AMPs), which aligns the CRTC's enforcement powers with how it regulates telecommunications and spam. The stated objective of the AMPs scheme would be to promote compliance, not to punish.[115]

[114] Jordan Pinto, 'Canadian Heritage Minister proposes bill to regulate OTTs, grant more power to CRTC' <https://realscreen.com/2020/11/04/minister-steven-guilbeault-proposes-bill-to-regulate-otts-grant-more-power-to-crtc/> accessed 10 October 2021.

[115] Canadian Heritage, 'Supporting a Stronger, More Inclusive and More Competitive Broadcasting System' <https://www.newswire.ca/news-releases/supporting-a-stronger-more-inclusive-and-more-competitive-broadcasting-system-874490015.html> accessed 10 October 2021.

193. Services where content is uploaded by users (e.g., TikTok) would not be captured by the amended Broadcasting Act as envisaged by Bill C-10. In determining the appropriate level of regulatory oversight, the ultimate decision to include or exclude services will be made by the CRTC, taking into account the nuances of individual platforms and the services they provide.[116] Different services will be subject to different levels of regulation depending on the nature of those services:

*i)* ***Regulated.***

A service would be regulated if the CRTC determines it meets all of the following criteria:

a) Carried on in whole or in part in Canada.
b) Offers the public audio, visual or audio-visual content intended to inform, enlighten or entertain (e.g. film, TV, music).
c) The service has control of the content, and in the case of a social media service, the content is not uploaded by unaffiliated users.
d) Regulation materially contributes to implementing Canada's broadcasting policy as set out in the Broadcasting Act.

*Examples*:

a) Netflix/Crave/Ici Tou.tv – curated library of films and series with significant subscriber bases.
b) Spotify – curated library of music and podcasts, also with a significant subscriber base.

*ii)* ***Some but not all regulated***.

Services will be partially regulated if the undertaking offers a number of services:

a) Some of its services would be subject to regulation if the CRTC finds those services meet the criteria of the regulated category.
b) Other services would not be regulated if the CRTC finds they do not meet the criteria for regulation, or they meet the criteria of the 'not regulated' category.

[116] Government of Canada, 'What online services would be regulated under the new Broadcasting Act?' <https://www.canada.ca/en/canadian-heritage/services/modernization-broadcasting-act/online-service-regulation.html> accessed 18 August 2021.

*Examples:*

a) YouTube – has a social media service where users upload content (not regulated), but also offers original content and other services (e.g., YouTube music) (regulated).
b) Facebook – has a social media service where users upload content (not regulated), but also offers original series on Facebook Watch (regulated).

*iii)* ***Not regulated.***

Meets any one of these criteria:

a) Predominantly textual content or is not offered to the public.

OR

b) The service does not have control of the content, or in the case of a social media service, is uploaded by unaffiliated users.

OR

c) Regulation would not materially contribute to implementing Canada's broadcasting policy as set out in the Broadcasting Act.

OR

d) Excluded through a possible direction to the CRTC (e.g., video games).

*Examples:*

a) TikTok – operates a social media service where users upload content.
b) Le Devoir – online newspaper with textual news articles.
c) Steam – online platform offering video games.

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform be modified, or removed from any website?**

194. Research for this project uncovered no specific government authority powers to order that content hosted by OTT platforms be modified or removed from any website. However, as Bill C-10 would bring OTT platforms into the potential regulatory purview of the CRTC, they would be legally obliged to address content hosted on their platforms that violate the Broadcasting Act's five online harms: child sexual exploitation, terrorist content, incitement to violence, hate speech, and non-consensual sharing of intimate images. In this way, OTT platforms would be subject to the same regulatory regime as social media and online news

platforms: the obligation to undertake 'all reasonable measures to do whatever is within their power to monitor for the regulated categories of harmful content on their services, including through the use of automated systems based on algorithms',[117] and restrict its visibility.

195. The Digital Safety Commissioner would have access to the same administrative and monetary penalties scheme intended to ensure compliance by OTT platforms, as available for violations committed on social media and online news platforms.

[117] Government of Canada, 'Discussion page - The Government's proposed approach to address harmful content online', <https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html> accessed 9 October 2021.

# CHILE

## A. INTRODUCTION

196. Article 19 of the Chilean Constitution assures all persons with the freedom to express an opinion in any form and by any means, without prejudice to answering for crimes and abuses committed in the exercise of these freedoms according to the law. This effectively establishes freedom of expression as a fundamental right, which is further complemented by Law 19.733,[118] explaining the freedom of expression as 'not being persecuted or discriminated against because of their own opinions, seeking and receiving information, and disseminating it by any means'. However, what crimes or abuses may constitute an exception to such right is neither prescribed by the Constitution nor Law 19.733. The content filtering practice in Chile is scattered across several legislations and there is no case-law body that elucidates how the legal principles operate generally.[119]

197. Moreover, the advent of new forms of communication through technology has posed new regulatory challenges in Chile.[120] While certain existing legal provisions that govern unlawful or abusive expressions extend beyond the physical realm and cover the virtual space (e.g., sections 412 and 416 of the Criminal Code), others only limit themselves to direct physical repression (e.g. Law 20.357 and 18.314).[121] This section tries to give an overview of provisions under the Chilean legal framework that may inhibit freedom of expression in the virtual space.

---

[118] Ley 19733, Sobre Libertades de Opinion e Informacion y Ejercicio del Periodismo (On Freedom of Opinion and Information and the Exercise of Journalism).

[119] Joana Varon Ferraz, Carlos Affonso de Souza, Bruno Magrani and Walter Britto, 'Content Filtering in Latin America: Reasons and Impacts on Freedom of Expression' (2013) New Technologies and Human Rights: Challenges to Regulation 273 <www.taylorfrancis.com/chapters/edit/10.4324/9781315598147-27/14internet-content-filtering-latin-america-reasons-impacts-freedom-expression> accessed 27 September 2021.

[120] Claudio Ruiz Gallardo and J Carlos Lara Galvez, 'Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America' in Eduardo Bertoni (ed.), *Towards an Internet Free of Censorship: Proposals for Latin America* (Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE) 2011) 18 <www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/Content-Filtering-Latin-America.pdf> accessed 27 September 2021.

[121] Joana Varon Ferraz, Carlos Affonso de Souza, Bruno Magrani and Walter Britto, 'Content Filtering in Latin America: Reasons and Impacts on Freedom of Expression' (2013) New Technologies and Human Rights: Challenges to Regulation 273 <www.taylorfrancis.com/chapters/edit/10.4324/9781315598147-27/14internet-content-filtering-latin-america-reasons-impacts-freedom-expression> accessed 27 September 2021.

119

## B. SECTION 1: SOCIAL MEDIA INTERMEDIARIES

### a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?

*i) Civil liabilities*

198. This subsection illustrates the landmark decision in *Fuentes v Entel* to provide the basis for the Chilean position on online civil responsibility.[122] In *Fuentes*, the claimant filed a complaint against Internet provider Entel concerning an advertisement for sexual services, in its advertisement section. The person seemingly offering the sexual services was the claimant's underaged daughter, who received countless phone calls of an 'obscene, insulting, rude and corrupt'. While the claimant argued that her daughter's constitutional right to honour had been violated, the company declined any responsibility as the advertisement had been placed by a user through Entel's free platform, thereby the legal responsibility resulted from the content should be exclusively borne by the user who published it. Although the court dismissed the claimant's argument, it still addressed the absence of special laws on the subject and set up the legal framework for responsibilities imposed on Internet service providers (ISPs).

199. The first step in the legal analysis on internet responsibility is to determine which specific type of ISP the defendant is, including access providers, storage providers and content providers. The ruling concluded that liability lies directly with the user who provides online content when such content is illegal or harmful,[123] but liability may also extend to the ISP if it has 1) created a database with the contributions made by its clients that is available to subscribers and 2) has failed to take necessary action to identify the users who post such messages and to establish any potential liability in the case of third party damage. The Appeals Court of Concepción further clarified that the applicable laws for a civil action would be those of tort liability and access providers are not obliged to control the inclusion of content on the web and are expected to respect the free circulation of the information

[122] Entel, recurso de protección, Causa Rol No 243-99, Concepción, 6 de Diciembre de 1999.
[123] Claudio Ruiz Gallardo and J. Carlos Lara Galvez, 'Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America' in Eduardo Bertoni (ed.), *Towards an Internet Free of Censorship: Proposals for Latin America* (Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE) 2011) 18 <www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/Content-Filtering-Latin-America.pdf> accessed 27 September 2021.
120

through the web. As such, Entel had not breached any duty of care as it was not aware of the offence in question, and it removed the advertisement only a few hours after receiving the request.

200. Drawing reference from *Fuentes,* an access and connection provider which does not offer any storage capacity or content is free from liability for the content posted by end users and for their acts of communication.[124] If the ISP stores the inappropriate or infringing content, the nature of tortious liability hinges upon the ISP's knowledge of the content and whether it removes such content within a reasonable time period. In other words, a hosting service provider only becomes liable with actual knowledge as opposed to strict liability or deemed notice. It is unless the ISP is itself a content provider that it will bear a direct tortious liability.

201. Hence, the civil liability that social media intermediaries may bear with reference to the contents posted is tortious in nature. Since most social media platforms have caches that temporarily store contents,[125] they can be determined as access and storage providers. As such, legal analysis of its civil liability should follow the logic laid down in *Fuentes.*

*ii) Copyright laws*

202. In 2010, Chile updated its copyright law through the enactment of Law 20.430.[126] Under this legislation, ISPs (including both access providers and hosting providers) are exempted from civil liability if they meet certain criteria.

203. Mere access, connection and routing service providers are exempted from liability to the extent that they refrain from interfering with the content in question.[127] For suppliers of temporary and automatic storage, they are exempted if they refrain from interfering with the technological processes established by source providers and the technology that enables interaction with these providers.[128] If they prevent access to material that has also been

[124] ibid.
[125] Center for Democracy & Technology, *Chile's Notice-And-Takedown System for Copyright Protection: An Alternative Approach* (2012) <www.cdt.org/insights/chiles-notice-and-takedown-system-for-copyright-protection-an-alternative-approach/> accessed 28 September 2021.
[126] Office of the Special Rapporteur for Freedom of Expression, *Freedom of Expression and the Internet* (Inter-American Commission on Human Rights, 2013).
[127] Center for Democracy & Technology, *Chile's Notice-And-Takedown System for Copyright Protection: An Alternative Approach* (2012) <www.cdt.org/insights/chiles-notice-and-takedown-system-for-copyright-protection-an-alternative-approach/> accessed on 28 September 2021.
125
[128] ibid.

removed by the source provider after being notified, they shall not be liable.[129] Finally, providers of storage for users and search, linking and reference services are most exposed to civil liability.[130] The requirements for these providers to be exempt from liability under the Chilean copyright law are that 1) they do not have actual knowledge of the illegal nature of the content, 2) they do not get any financial gain directly attributable to the infringing activity, 3) they can and are able to control such content, 4) they have appointed a representative for notification purposes, and 5) they expeditiously remove or disable access of the infringing content.[131]

*iii) Criminal liability*

204. Although there are laws against expressions made with regards to genocide and terrorism, the respective legislations limit criminal liability to physical expressions. With that in mind, criminal liability regarding online expressions is limited to cases relating to crimes against honour and sexual contents.

205. For crimes against honour, section 422 of the Criminal Code provides that:

> Calumny and insult shall be deemed to have been committed publicly and in writing where they are disseminated by banners or posters placed in public areas; by printed materials that are not subject to the press law, lithographs, printouts or manuscripts circulated among more than five people, or through allegories, caricatures, emblems or allusions reproduced by lithography, printing, photography or any other procedure.

206. The term 'any other procedure' is opined by commentators that it is capable of extending to virtual space.[132] However, it is unclear whether such criminal liability may also extend to the ISPs, including social media intermediaries that provide the platform for the calumny or insult to be viewed by the public.

207. Similarly, although Article 161-A of the Penal Code criminalizes the act of the sharing of sexual photos or videos when there is no consent by any of the persons involved. However,

[129] ibid.
[130] ibid.
[131] ibid.
[132] ibid.

there is a legal vacuum in putting online intermediaries criminally liable.[133] During 2018-2019, a draft bill (number 11923-25) proposed adding a new paragraph to Article 161-A to punish the site administrators where these images are hosted if they do not remove them. However, until the present day, such a bill has yet to pass the legislative process, and the legal vacuum has remained.

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

208. Chile does not have any specific regulations on internet content control or filtering,[134] and no specific legislation that provides the government with the authority to directly order any removal of online contents. Conversely, as aforementioned, the Constitution of Chile made it clear that the freedom of expression in Chile is a fundamental right that can only be infringed if such expression is unlawful. When the potential criminal liability arising from expression in Chile mostly hinges on personal insult or the distribution of pornographic materials, there lacks a public aspect for the Chilean government to order the removal of online contents.

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

209. Through analysing existing legislations and cases law, the nature of online content that Chilean courts can order to be taken down from a social media intermediary can be divided into two broad categories: copyright infringement and offensive/insulting comments.

*i) Copyright infringements*

210. Starting with copyright infringements, as mentioned above, the relevant legislation governing this area is Law 20.430. As a product which is designed to implement portions of the US-Chile Free Trade Agreement, this piece of legislation largely mimics the United

[133] Centre for International Governance Innovation, *Supporting a Safer Internet Paper No.2 - Non-Consensual Intimate Image Distribution: The Legal Landscape in Kenya, Chile and South Africa* (2021) <www.cigionline.org/publications/non-consensual-intimate-image-distribution-the-legal-landscape-in-kenya-chile-and-south-africa/> accessed 28 September 2021.

[134] Eduardo Bertoni, 'Right to be … forgotten? Trends in Latin America After the *Belen Rodriguez* Case and The Impact of The New European Rules' in Giancarlo Frosio, *Oxford Handbook of Online Intermediary Liability* (OUP, 2020).

States' Digital Millennium Copyright Act.[135] Yet, one critical difference exists between the two, that the US legislation relies on a notice-and-takedown system, while the Chilean Law 20.430 requires a court order to compel blocking or removal of the infringing content.

211. For rightsholders, they must file a petition in civil court for a preliminary or permanent injunction under Article 85Q of Law 20.430. The petition must clearly identify the rights infringed, the kind of infringement, the infringing material and its location on the ISP's system or network.[136] If the petition is deemed lawful, courts are required to issue takedown orders without delay.[137] Conversely, the affected user may request the court to reconsider a takedown order by filling a petition meeting the same requirements listed above.[138]

212. To conclude, Chilean courts can takedown copyright infringement contents upon request of rightsholders. Yet, unlike the US model, mere notice from the rightsholder to social media intermediaries will not effectively trigger a takedown procedure. This procedure is summarized by the Center for Democracy as 'linking actual knowledge [of copyright infringement] to judicial process'.[139] The law also provides a balance between rightsholder and internet users, even if the content has been taken down, the aggrieved issuer of the content is allowed to request a reconsideration from the courts.

*ii) Offensive or insulting comments*

213. In *Abbott Charme, Jorge v Google.cl*,[140] the plaintiff alleged that his name is linked with insults in search engines and these accusations damaged both him and his family. The court ruled in favour of the plaintiff and showed a high willingness to take down any online comments or expressions that are injurious in nature or entails a violation of constitutional rights.[141] Similar to this judgement, in *ISB and others v VG, Google Chile and Google Inc.*,[142] the court also ordered internet sites to takedown profiles and contents containing offensive conduct against the plaintiffs, which effectively covers social media sites.

---

[135] Center for Democracy & Technology, *Chile's Notice-And-Takedown System for Copyright Protection: An Alternative Approach* (2012) <www.cdt.org/insights/chiles-notice-and-takedown-system-for-copyright-protection-an-alternative-approach/> accessed on 28 September 2021. 125
[136] ibid.
[137] ibid.
[138] ibid.
[139] ibid.
[140] Corte de Apelaciones de Valparaiso *Abbott Charme, Jorge v Google Chile* [2012] case no. 228-2012 (Chile).
[141] ibid.
[142] Corte de Apelaciones *ISB y ortos v VF, Google Chiley Google Inc.* (Chile).

214. However, with regards to the notion of the 'right to be forgotten', Bertoni observed that the Chilean jurisprudence has mostly rejected it.[143] What the notion of the 'right to be forgotten' entails is that the record of a person's previous convictions or misbehavior should be removed after a considerable period of time, so as to ensure the person being able to live a normal life after serving his time under legal sanction. Such attitude is most evidently shown in *Gomez Arata v Google Ltda and Google Inc.,*[144] where the plaintiff's name is associated with words like 'chanta'[145] and 'thief'. The court ruled against the plaintiff and held that online intermediaries are not required to monitor such contents.

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

215. The key case law discussing the conditions in which intermediaries are required to 'unmask' anonymous speakers and identify originators of content is the case *Suazo v Reclamos.cl.*[146] In this case, the plaintiff sought relief from the administrator of a website where people can leave anonymous public messages with complaints against companies and services. The plaintiff, the representative of a school, claimed that the site administrator should be held liable for a slanderous accusation posted against her. The court rejected the plaintiff's claim by recognizing the need to enforce freedom of opinion and freedom of information without prior censorship. Data protection and regulation of journalism were also mentioned by the court to prevent the identification of possible defendants. The Court of Appeal established that providers only fulfil the duty to provide the means of communications. The Supreme Court rejected the appeal, establishing that there was no abusive exercise of the right to express an opinion and inform without prior censorship.

216. Determining from the decision in *Suazo*, it is clear that the court is unwilling to allow the plaintiff's request to unmask anonymous speakers and identify originators of content. It is unless that such content is of injurious in nature that violates the constitutional right of the plaintiff that the court may interfere the anonymity online so as to impose civil or criminal

[143] Eduardo Bertoni, 'Right to be … forgotten? Trends in Latin America After the *Belen Rodriguez* Case and The Impact of The New European Rules' in Giancarlo Frosio, *Oxford Handbook of Online Intermediary Liability* (OUP, 2020). 134

[144] ibid 475.

[145] Meaning dumb, ingenious or not very sharp in Chile.

[146] *Suazo v Reclamos.cl.* (Chile).

liability to the originator of such content, which unmasking and locating them is essential for court actions.

## C. SECTION 2: ONLINE NEWS MEDIA

217. As aforementioned, Article 19(12) of the Chilean Constitution regarded freedom of expression as a fundamental right. It is important to note that such freedom extends to 'any form and any medium', which effectively covers online news media.[147] In fact, the Constitution stipulates that any person is allowed to establish, edit and maintain newspapers, magazines and periodicals under 'conditions that the law specifies', while 'in no case can the law establish a state monopoly over the media of social communication'.[148] This presents the general position of Chile's law regarding online news media that a positive legal provision is required to take down or temper with contents posted.[149] This section describes the laws that may authorise the government to remove content from online news websites, the standard for determining removal and whether the leave from the judiciary is necessary.

### a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?

218. Under the Chilean legal framework, the primary legislation governing the exercise of journalism is Law 19.733.[150] Right at the start of this law, the definition of social communication media, the primary subject of this law, is defined in Article 2 as those capable of 'transmitting, disclosing, disseminating or propagating, in a stable and periodic manner, texts, sounds or images intended for the public, whatever the medium or instrument used'. Clearly, both online news media sites, as well as their social media accounts are well covered under this law. It is important to reiterate the point made in Section 1 that acts against terrorism or genocide only apply to physical repressions and, therefore, will have no effect on online news items.[151]

---

[147] Constitute, 'Chile's Constitution of 1980 with Amendments through 2012 (*Constitución Política de la República de Chile)',* art 19(12*)* <www.constituteproject.org/constitution/Chile_2012.pdf> accessed 27 September 2021.
[148] ibid.
[149] Bureau of Democracy, United States Department of State, *Chile 2013 Human Rights Report* (2014).
[150] Patricia Pena, *Libertad de expresión y de discurso en Chile: desafíos y tensiones en el tránsito hacia una sociedad digital* (CELE, 2019).
[151] Joana Varon Ferraz, Carlos Affonso de Souza, Bruno Magrani and Walter Britto, 'Content Filtering in Latin America: Reasons and Impacts on Freedom of Expression' (2013) New Technologies and Human Rights: Challenges

219. The general position regarding these social communication media is provided under Article 3 of Law 19.733, which acknowledges the importance of pluralism in the information system and ensures the freedom to found, edit, establish, operate and maintain social communication media. Although Law 19.733 does not specify any particular crime or offence against the government which allows it to take down or remove contents from websites, Title IV and V of it does impose civil and criminal responsibilities on persons running social communication media if its contents offend or unfairly allude the reputation of another person (both natural and legal).[152] Such responsibilities include rectification and/or clarification, which in the context of online medium, may also encompass the removal of contents that are untrue or amounts to libel and slander.[153]

220. In order to effect such a right, the interested party (including the government) needs to follow the procedures laid down in Article 24, which stipulates that: a) the complaint must clearly indicate the infringement, relevant facts and applicable evidence, b) the court will then notify the social communication media, c) the social communication media must then present their discharges within the fifth business day and attach supporting evidence. If such evidence is not available, the social communication media should express that to the court, and it will set a later day for hearing in order to receive the evidence required.

221. If the court determines that there is indeed an infringement, it will order the social communication media to clarify or make rectification, which likely includes taking down the content if the news media runs in an online basis. Although Article 24 provides rights-holders with a legal pathway to safeguard their rights, it also leaves an appeal mechanism for the social communication media, such that it can request an appeal to higher courts.

222. In the case where the media does not follow the court's order of clarification or rectification, Article 28 of Law 19.733 will impose the criminal sanction of a fine to the director of the news media and at the same time suspend the operation of it. This amounts to an effective mechanism to ensure compliance with the law.

---

to Regulation 273 <www.taylorfrancis.com/chapters/edit/10.4324/9781315598147-27/14internet-content-filtering-latin-america-reasons-impacts-freedom-expression> accessed 27 September 2021.
119

[152] Edison Lanza, *Informe Especial Sobre la Libertad de Espresion en Chile 2016* (Relatoria Especial para la Liberatad de Espresion de la Comision Interamaricana de Derechos Humanos, 2016).

[153] ibid.

223. However, under Article 30 of Law 19.733, certain truths posted are immune to legal liabilities, provided that a) the imputation is produced for the purpose of defending a real public interest, or b) that the affected person exercises public functions and the imputation refers to events inherent to such exercise.

224. To further clarify what amounts to 'public interest', Article 30 listed the following:
   i) Those referring to the performance of public functions;
   ii) Those carried out in the exercise of a profession or trade and whose knowledge has a real public interest;
   iii) Those that consist of activities to which the public has had free access, free or onerous;
   iv) Actions that, with the consent of the interested party, have been captured or disseminated by any means of social communication;
   v) The events or manifestations that the interested party has left testimony in public records or archives, and
   vi) Those consisting of the commission of crimes or guilty participation in them.

225. With that in mind, the Chilean legal framework showed a high level of willingness to allow news media to carry out their responsibility to monitor the behaviour of the government, as most government actions do fall under the umbrella of 'public interest', thereby raising the standard for the government to disproof any contents that they deem inappropriate as 'public interest'-related so as to effect any acts of removal.

**b) What are the tests or standards for determining whether an online news article/page needs to be removed?**

226. Since there is no specific laws or regulations regarding online news article or page, the legal standard of whether it amounts to an infringement of another's rights should be on par with any other expressions made by social communication media.[154] Article 29 of Law 19.733 stipulates that the crime of libel and slander also applies to the expressions made by social communication media, which its effect have been discussed previously in Section 1. For the

[154] Eduardo Bertoni, 'Right to be … forgotten? Trends in Latin America After the *Belen Rodriguez* Case and The Impact of The New European Rules' in Giancarlo Frosio, *Oxford Handbook of Online Intermediary Liability* (OUP, 2020).
134

standard of whether a person is offended, or the content is unfairly alluded, the is no specific statutory guideline to it and it should depend on the particular contents involved.

**c) Is the order of a court/tribunal a prerequisite for removal of online content?**

227. As aforementioned, Law 19.377 provide a rigid procedure for any aggrieved party to go through a legal claim to effect acts of clarification or rectification to safeguard their rights. With that in mind, it is clear that it is a prerequisite for even the government to rely on the judiciary to effect their right and not abruptly remove online content.[155]

## D. SECTION 3: OTT PLATFORMS

228. Chilean law does not contain a specific regulatory regime for OTT platforms as yet. As the law currently stands, OTT platforms are regulated in a fragmented manner primarily by the general Penal Code of Chile and incidentally by the Tax Reform Law that imposes a Value Added Tax ('VAT') on OTT services. That said, a recently introduced bill in the Senate seeks to bring OTT platforms within a specific regulatory framework for digital platforms.

**a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?**

229. There is no specific regulatory framework for OTT platforms in Chile as yet. Fragmented legislative standards may arguably govern the content on OTT platforms, although they do not explicitly refer to OTT services.

*i) Penal Code of Chile*

230. Article 374 of the Penal Code of Chile states that whoever 'exhibits songs, brochures or other writings, printed or not, figures or stamps contrary to good customs' would be penalised by way of a minor imprisonment or a fine of eleven to twenty monthly tax units. It also criminalises the act of exhibiting 'pornographic material, whatever its medium, in the

[155] Claudio Ruiz Gallardo and J. Carlos Lara Galvez, 'Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America' in Eduardo Bertoni (ed.), *Towards an Internet Free of Censorship: Proposals for Latin America* (Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE) 2011) 18 <www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/Content-Filtering-Latin-America.pdf> accessed 27 September 2021.
120

preparation of which minors under eighteen have been used' with the penalty of minor imprisonment in its maximum degree.

231. Article 374 states that the act of exhibition will be deemed to have been committed in Chile when 'carried out through a telecommunications system that is accessed from the national territory'.

232. Although there is no specific ruling on the subject of OTT platforms, it is possible that the general restriction on the exhibition of child pornography and other materials contrary to good customs applies equally when such materials are exhibited on digital platforms.

*ii) 2021 Bill to Regulate OTT Platforms*

233. In September 2021, a bill was initiated to regulate the situation of digital service platforms in Chile.[156] Digital platforms are understood to be virtual infrastructures whose purpose is to facilitate a common interaction space for people to perform various tasks on the Internet. These platforms would be subject to the provisions of the Bill simply by the fact that they address their content to the country, per article 2. The Bill specifically notes that it is no longer possible to leave digital platforms to self-regulate and that it is necessary for the State to intervene.

234. Article 4 of the Bill proposes that digital platforms are to be subject to the principle of equivalence in the digital environment, the principle of regulatory compliance in accordance with the constitutional, legal and other regulatory requirements in force in Chile, and the principle of universality of access in line with network neutrality.

235. Article 6 of the Bill guarantees freedom of digital expression for consumers and users of digital platforms. According to this provision, digital platform providers shall not be liable for content if they have not originated the transmission or modified the content. They will only be liable for content that is unlawful, civilly libellous, slanderous, constituting threats or offences, if they do not act diligently to block or remove such content when they have actual knowledge of its unlawfulness.

156 "Bill, initiated by motion of the Honorable Senators Mr. Girardi, Mrs. Goic and Mr. Coloma, Mr. Chahuán and Mr. De Urresti, which regulates digital platforms", Bulletin No. 14.561-19 (2021).

236. According to Article 8 of the Bill, digital platform providers are obligated to protect the image and integrity of vulnerable persons, that is persons considered vulnerable by law due to age, condition or other similar circumstances. Such protective measures include issuing warnings for sensitive content when their addictive nature is known, or when the content is essentially aimed at adults. Protective measures, especially when it comes to adult content, include appropriate age verification mechanisms.

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?**

237. According to Article 6 of the new Bill, content on digital service platforms may not be removed unless it amounts to civil libel or slander, is threatening, or constitutes a crime defined by other legal bodies or incites the commission of a crime.

238. As mentioned above, the providers of such platforms will not be liable in those cases in which they did not originate the transmission or modify data or content. The actions of the providers will only be considered unlawful when they exceed the typical scope of the service, or when they do not act with due diligence, which will be understood in those cases in which they should have blocked or removed content because they had actual knowledge of its unlawfulness.

239. According to the Bill, the digital platform provider will be objectively liable for all damages (patrimonial and moral) caused to users. In case of breach of the provisions of the project, the amounts corresponding to compensation will be doubled, and may even order the temporary blocking of the platform if there is a systematic infringement.

240. The procedure to make such orders of removal or modification and to ensure compliance are however yet to be clarified.[157]

[157] Carolina del Río, Gabriela Wildner Gutierrez, and Mercedes Londoño, 'New Bill of Law to regulate Digital Platforms entries to Chilean Congress' (JDSUPRA, 10 September 2021) <https://www.jdsupra.com/legalnews/new-bill-of-law-to-regulate-digital-9902513/> accessed 12 September 2021.

# EUROPEAN UNION

## A. SECTION 1: SOCIAL MEDIA INTERMEDIARIES

241. The EU rules for the regulation of social media intermediaries are roughly twofold; a general and horizontal scheme and fragmented sector-specific rules. A general rule, E-Commerce Directive, hereinafter ECD, (and its successor Digital Services Act currently under proposal to the European Parliament from the European Commission—hereinafter DSA) stipulates the 'safe harbour' rule, by which information intermediary services are exempt from criminal, administrative and civil liabilities under certain conditions. Especially, 'hosting providers (Art. 14 ECD)', into which most of social media intermediaries are classified, are exempt from liability 'when those companies storing data for their users (e.g. webhosting) do not know that they host illegal activity or information and act expeditiously to remove or disable access to the illegal information.' This rule aims to offer horizontal and general protection from legal liabilities for them in exchange to duties of care and notice-and-take-down obligation.

242. However, neither ECD nor DSA positively establishes the general liability scheme for social media intermediaries. It is a matter of sector-specific rules or of national legislation in what circumstances liability or obligation arises to them. There are a number of sector-specific EU rules on various policy fields; for example, Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children, Directive 2019/790 on copyright and related rights in the digital single market (Digital Single Market Directive), Directive 2018/1808 on the Audiovisual Media Services Directive, Regulation 2021/784 on addressing the dissemination of terrorist content online, Regulation 2016/679 (the General Data Protection Regulation or GDPR), Directive 2019/2161 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU as regards the better enforcement and modernisation of Union consumer protection rules. The nature and the degree of overlap with ECD/DSA of these rules differ greatly in each case, but the EU commission has recently arranged the relations between general rules and sector-specific rules as *lex generalis* and *lex specialis*.[158] As the proposal for DSA states:

[158] At the time ECD was drafted, sector-specific regulations are largely the matter of national legislation (See Art 14(3)), but the emergence of EU law in various policy areas have created difficult question on the relation between ECD and specific EU rules.

> The proposed Regulation complements existing sector-specific legislation and does not affect the application of existing EU laws regulating certain aspects of the provision of information society services, which apply as *lex specialis*.[159]

243. In each section below, the questions will be discussed with regard to ECD/DSA and sector-specific rules respectively.

244. However, it is a debatable question whether social media intermediaries (including messaging apps) in a general sense such as Facebook or WhatsApp can be classified into specific legal categories, such as 'controller' in GDPR, 'hosting service provider' in some Directives, or 'online content-sharing service provider' in Digital Single Market Directive, respectively. Especially, as ECD provides 'safe harbour' only for 'information society service', a European Parliament paper argues:

> several academic studies have highlighted the uncertainties surrounding the application of the E-commerce Directive to social media companies and collaborative platforms. The CJEU has recently ruled in different ways on the question of whether the service provided by Airbnb and Google must be classified as an 'information society service'.[160]

245. Indeed, as the degree of control by intermediaries to the web contents has been greatly deepened since the enactment of ECD, some people argue that the framework of ECD presupposing 'neutrality' of intermediaries is no longer sustainable. Although DSA allegedly keeps the framework of ECD, it actually provides more detailed categories for intermediaries based on the nature of the services and the scale of the provider. Most social media intermediaries, such as Facebook or WeChat, seem to be classified to 'very large online platforms' with practically heavier obligations of monitoring and transparency than those under ECD.

**a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?**

[159] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM (2020) 825 final, 4.
[160] Tambiama Madiega, 'Reform of the EU liability regime for online intermediaries Background on the forthcoming digital services act' (Members' Research Service, EPRS PE 649.404, May 2020) 5.

246. As aforementioned, Article 14 ECD stipulates as follows:

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

247. As this provision is predecessor to Art 5 DSA, in the dimension of general rules, social media intermediaries will not be held liable as long as they comply with the reasonable standard of care (CJEU expressed the expected standard as 'a diligent economic operator' should have identified the illegality and acted expeditiously[161]). Even with that standard, Art 15 ECD (Art 7 DSA) prohibits the member states to impose a general obligation to monitor the contents or to actively find facts.

248. However, 'over the last few years the European Commission has issued a great number of documents that touch on …platforms' liability, which contribute to the formation of an emerging liability regime for unlawful content that differs profoundly from the regime of conditional liability exemption envisaged in the e-Commerce Directive.'[162] First of all, DSA, which is supposed to be a successor of ECD, essentially tightens the control over social media intermediaries. Although 'safe harbour' principle and the prohibition of requiring general monitoring remain, for 'very large platforms',[163] to which most of social media intermediary giants will be classified, the requirements for transparency and risk assessment increase their burden significantly.

---

[161] Case C-324/09 L'Oréal SA and others v eBay International AG and others [2011] [120].
[162] Maria Lillà Montagnani, 'A New Liability Regime for Illegal Content in the Digital Single Market Strategy' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020) 295.
[163] 'Very large platform', which, is a sub-category of 'online platform', which is a sub-category of 'hosting services'. 'Intermediary services' is the broadest category which includes 'hosting services'.

249. Furthermore, various sector-specific rules which emerged mainly in 2010s impose a variety of obligations and liabilities over social media intermediaries. First, rules regarding consumer protection are clearly thought to be the exception to the 'safe harbour' principle from newly added Art5 (3) DSA.[164] Directive 2019/2161 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU as regards the better enforcement and modernisation of Union consumer protection rules ('new deal for consumers' package of measures) intends to include some of social media intermediaries in its scope.[165] Essentially, under this rule social media intermediaries are subject to various liabilities arising from consumer protection law when they provide 'free digital service' in exchange to users' personal information.[166] Even when social media intermediaries merely provide individual users with online platforms to trade, they are obliged to disclose parameters of their search results.[167]

250. The rules on the protection of intellectual property may impose liabilities on social media intermediaries. In *L'Oreal v eBay*, where the scope of ECD's 'safe harbour' principle became the issue in relation to Directive 89/104 and Regulation 40/94 on trade mark protection, CJEU has ruled that if an online marketplace company optimises the presentation of the offer for sales, then it cannot invoke the exemption from legal liabilities because it cannot be regarded as neutral.[168] Similarly, in the case of copyright infringement uploaded on the online platform, Article 17 Directive 2019/790 (Digital Single Market Directive) stipulates as follows:

> 1. an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users…
> 3. When an online content-sharing service provider performs an act of communication to the public or an act of making available to the public under the conditions laid down in this Directive, the limitation of liability established in Article 14(1) of Directive

[164] See art 5 (3) DSA.
[165] See Recital (20) Preamble.
[166] See Recital (31) to (33) Preamble.
[167] See Recital (21) to (23) Preamble.
[168] Case C-324/09 L'Oréal SA and others v eBay International AG and others [2011] [116].

2000/31/EC (ECD safe-harbour provision) shall not apply to the situations covered by this Article.

251. It should be noted that social media intermediaries are not merely hosts of specific information, but potentially perform 'an act of communication' regarding infringing information here. Consequently, unless social media intermediaries take proportionate measures to disable access to or remove the infringing contents expeditiously and make best efforts to stay down such contents, they may be held liable. Additionally, when they take down specific contents, they have an obligation to give notice to/notify the uploader of the allegedly infringing contents about the reason of the removal and provide the chance of internal and judicial redresses.[169]

252. Data protection is another field where social media intermediaries may be held liable. CJEU's ruling in *Google Spain* case and subsequent codification of the right to be forgotten in Regulation 2016/679 (GDPR) have imposed on them the burden to take down, or delist the personal information from the online platform when the person requires to do so unless keeping that information is necessary for a particular reason such as 'the preponderant interest of the general public'.[170] As critics insist, this rule gives a heavy pressure for social media intermediaries to overly comply with the requirement under the potential threat of administrative liability which can lead to the huge amounts of fines, as high as four percent of annual global turnover or twenty million euros.[171]

253. Illegal or harmful contents are also the legal areas in which social media intermediaries may potentially be held liable. However, as the regulations on those contents have significant overlaps with the contents in the sections b) and c), they are not addressed here.

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

254. Neither ECD nor DSA stipulate the power of the government to require social media intermediaries to take down specific contents, as they are considered to be a matter of

[169] Directive 2019/790 (Digital Single Market Directive), art 17(9).
[170] Case C-131/12 *Google Spain SL and another v Agencia Española de Protección de Datos (AEPD) and another*, [2014] para 97, Regulation 2016/679 (GDPR), Recital (73), Preamble.
[171] GDPR art 83.

national legislation. However, two things should be noted in the context of the EU law; intermediary's duty to care and take down in ECD/DSA and sector-specific rules regarding the removal of specific contents.

255. First, though Article 14 ECD does not concern the order by the government per se, it offers exemption from legal liabilities for social media intermediaries only if they act promptly to remove illegal contents from their websites once they come to know the illegality of the specific contents. It is not obvious what 'illegal' means from the words of ECD, but the proposal by the European Commission on DSA states as follows:

> The proposed Regulation introduces a horizontal framework for all categories of content, products, services and activities on intermediary services. The illegal nature of such content, products or services is not defined in this Regulation but results from Union law or from national law in accordance with Union law.[172]

256. Putting aside national legislations, the EU-level sector-specific rules stipulate the entitlements of the competent authority of the member states to order the removal of specific contents. However, the wordings and procedures concerning those specific contents differ according to the severity of the harm and the nature of the content. For example, Art 25 Directive 2011/92 on sexual abuse states;

> 1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.
>
> 2. Member States may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.

[172] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM (2020) 825 final,4.

257. With regard to audio-visual contents concerning hate speech and violence, due to the consideration of the balance between potential harm and freedom of speech, 'without prejudice to the obligation of Member States to respect and protect human dignity, Member States shall ensure *by appropriate means* that audiovisual media services provided by media service providers under their jurisdiction do not contain' any such contents.[173] With regard to terrorist content, because of the urgency of its nature, more direct and detailed provisions are provided in the form of EU regulation, stating as follows:

> 1. The competent authority of each Member State shall have the power to issue a removal order requiring hosting service providers to remove terrorist content or to disable access to terrorist content in all Member States.[174]

258. A remaining issue is about not illegal but harmful contents, such as fake news or disinformation. As the proposal for DSA shows, the EU law is increasingly inclined to encourage self-regulation by the code of conduct of social media intermediaries.[175]

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

259. In the level of the EU law, there is no general prohibition or rules on judicial order to take down specific content. EU law takes it for granted that the courts of each member state can offer injunctive relief in the case where it is proportionally appropriate to remove specific contents based on the rightsholder's legitimate claim. In the case of intellectual property right infringement, CJEU explicitly admit in *L'Oreal* that the courts of the member states can:

> order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind.[176]

---

[173] Council Directive (EU)2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L303/69, art 1(9).
[174] Council Regulation (EC) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L172/79, art 3.
[175] For example, see Recital (68) and (69) Preamble of the proposal.
[176] Case C-324/09 L'Oréal SA and others v eBay International AG and others [2011] [128].

260. According to *Glawischnig-Piesczek v Facebook Ireland*, where Austrian politician claimed that Facebook Ireland should remove the defamatory contents against her, CJEU held that the national court's power to order host providers to remove specific contents should be extended to the contents identical, or even similar to other posts already declared unlawful. Furthermore, the court also ruled that the national court can make such order beyond territorial jurisdiction in principle.[177]

261. Directive (EU) 2017/541 on combating terrorism requires hosting service providers to remove flagged terrorist content in all member states within an hour of receiving a removal order from the competent authority. Member states are required to adopt rules on penalties, the degree of which will take into account the nature of the breach and the size of company responsible.

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

262. In the EU law, there are no general prohibition on the order by the competent authority or court to disclose the information about the origin of the specific content as well. Indeed, in *L'Oreal*, CJEU states as follows:

> Furthermore, in order to ensure that there is a right to an effective remedy against persons who have used an online service to infringe intellectual property rights, the operator of an online marketplace may be ordered to take measures to make it easier to identify its customer-sellers.[178]

263. However, especially with regard to anonymity, its 'unmasking' may have a serious issue in relation to the protection of human rights. Although CJEU is yet to address the question of whether an expectation of anonymity on the internet is an aspect of the right to the protection of personal data and the right to freedom of expression, the European Court of Human Rights relevantly admit the value of anonymity as a part of freedom of expression.[179] Since the Charter of Fundamental Rights of the EU declares that 'the meaning and scope of

[177] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, [2019] para 109.
[178] Case C-324/09 L'Oréal SA and others v eBay International AG and others [2011] [142].
[179] Delfi AS v. Estonia (2015) 62 EHRR 199, para 147.

those [corresponding] rights [with the European Convention of Human Rights] shall be the same as those laid down by the said Convention',[180] proportionality test may be required to disclose users' information. It is generally admitted that such information can be disclosed in the context of criminal or administrative law (For example, the GDPR does not apply to processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences[181]), but to what extent it should be disclosed in the context of civil law is still unclear.[182]

## B. SECTION 2: ONLINE NEWS MEDIA

264. EU regulations for online news media stem from the fundamental right to freedom of expression enshrined in Article 10(1) of the European Convention on Human Rights (ECHR). Article 10(1) grants everyone the 'freedom to hold opinions and to receive and impart information without interference by public authorities'.[183] The right to freedom of expression is a qualified right, not an absolute right. As such, this right can be restricted as per Article 10(2) of the ECHR. Keller has argued that in general, the EU retains a bias towards the freedom to publish and treats the protection of the state and the public from the harmful effects of media content as secondary concern.[184]

265. For instance, the Council of Europe treaties[185] and sector-specific EU rules on restricting publications, such as Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children, Directive 2019/790 on copyright and related rights in the digital single market (Digital Single Market Directive), and Regulation 2021/784 on addressing the dissemination of terrorist content online, makes exception for journalistic purposes. As such, journalists are bound by national codes of conduct in publishing online news. Given these exceptions, the press has an increased responsibility to provide reliable and precise

[180] Charter of Fundamental Rights of the European Union, 2012/C 326/02, art 52.
[181] See Recital (19) Preamble.
[182] For example, see *Board of Management of Salesian Secondary College (Limerick) v. Facebook Ireland Limited [2021] IEHC 287.*
[183] European Convention on Human Rights 1950, art 10(1).
[184] Perry Keller, *European and International Media Law: Liberal Democracy, Trade, and the New Media* (OUP 2011) 116.
[185] Council of Europe, Convention on Cybercrime, (ETS No. 185) including its Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, (ETS No. 185), See also Council of Europe, Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse 2007 (ETS No. 201), Convention on the Prevention of Terrorism (2005) (ETS No. 196).

information in accordance with the ethics of journalism, when publishing articles on the internet.

**a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?**

266. Public authorities can order the removal of an online news item as per Article 10(2) of the ECHR, if 'prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary'.[186]

267. The procedure that governments must follow to make online news item removal orders, and ensure compliance is not something that is regulated at the EU-level. Instead, such procedures are regulated at the national level by the Member States.

**b) What are the tests or standards for determining whether an online news article/page needs to be removed?**

268. In general, the court is involved when a claimant submits a case to the court, asking it to determine whether an online news article/page was removed in accordance with the standards laid out in Article 10(2) of the ECHR: (1) prescribed by law, (2) legitimate aim, and (3) necessary in a democratic society. First, the court will assess whether the measure was prescribed by law, meaning that the measure should have some basis in domestic law. The European Court of Human Rights has held that law needs to be formulated with sufficient precision to enable the citizen to regulate their conduct, and that they must be able to foresee the consequences of their actions.[187] Court has stated that these consequences do not need to be foreseeable with absolute certainty.[188] In assessing foreseeability, the Court also looks at the quality and accessibility of the law. The Court considers law that has been published in the national official gazette as accessible.[189]

[186] European Convention on Human Rights 1950, art 10(2).
[187] *Perinçek v. Switzerland* App no. 27510/08 (ECHR, 15 October 2015), para 131.
[188] ibid.
[189] *Semir Güzel v. Turkey* App no. 29483/09 (ECHR, 13 September 2016), para 35.

269. Second, the court will assess whether a legitimate aim was pursued by the interference. The legitimate aims of interference with the right to freedom of expression are exhaustively set in Article 10(2) of the ECHR as (1) interests of national security, territorial integrity or public safety, (2) prevention of disorder or crime, (3) the protection of health or morals, (4) the protection of the reputation or rights of others, (5) preventing the disclosure of information received in confidence, and (6) maintaining the authority and impartiality of the judiciary.

270. Third, the court will assess whether the interference was necessary in a democratic society. The general principles for assessing the necessity of an interference with freedom of expression, reiterated many times by the Court since its judgment in *Handyside v the United Kingdom*,[190] were summarised in *Stoll v Switzerland*[191] and restated in *Morice v France*[192] and *Pentikäinen v Finland.*[193] In assessing this the Court looks at whether the interference is proportionate to the legitimate aim pursued.[194] In considering whether an act is proportionate, the court will see whether there was a 'pressing social need' and assess the nature and severity of the sanctions imposed. Member States have a certain margin of appreciation in assessing whether a pressing social need exists.[195] However, where freedom of the press is at stake this margin of appreciation is in principle restricted.[196]

271. In assessing the nature and severity of the sanction, the court checks whether the sanction was intended as a form of censorship intended to discourage the press from expressing criticism.[197] The Court has found an order suspending the publication and distribution of newspapers, which it considered unjustified even for a short period[198] as 'censorship'. In determining the proportionality of a general measure, as is the case with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, the Court must primarily assess whether the legislature acted within the margin of appreciation afforded to it, in adopting the general measure and striking the balance it did. In assessing

[190] *Handyside v. the United Kingdom* App no. 5493/72 (ECHR, 7 December 1976).
[191] *Stoll v. Switzerland* App no. 69698/01 (ECHR, 10 December 2007), para 101.
[192] *Morice v. France* App no. 29369/10 (ECHR, 23 April 2015), para 124.
[193] *Pentikäinen v. Finland* App no.11882/10 (ECHR, 20 October 2015), para 87.
[194] ibid.
[195] ibid.
[196] *Dammann v. Switzerland* App no. 77551/01 (ECHR, 25 April 2006), para 51.
[197] *Bédat v. Switzerland* App no. 56925/08 (ECHR, 29 March 2016), para 79.
[198] *Ürper and Others v. Turkey* App nos.. 14526/07, 14747/07, 15022/07, 15737/07, 36137/07, 47245/07, 50371/07, 50372/07 and 54637/07 (ECHR, 20 October 2009), para 44; see also *Gözel and Özer v. Turkey* App nos. 43453/04 and 31098/05 (ECHR, 6 July 2010), para 63.

this, the court takes into account the quality of the parliamentary and judicial review of the necessity of the measure in assessing the Margin of Appreciation given to Member States.[199] A general measure has been found to be a more feasible means of achieving the legitimate aim than a provision allowing a case-by-case examination when the latter would give rise to a risk of significant uncertainty.[200] The more convincing the general justifications for the general measure are the less importance the Court will attach to its impact in the particular case.[201]

### c) Is the order of a court/tribunal a prerequisite for removal of online content?

272. At the EU level, there is no requirement for an order of the court/tribunal to remove online news content. Article 10(2) gives Member States the freedom to order content to be removed if prescribed by law and is necessary in a democratic society. National courts are involved only if someone files a court case alleging that the order to remove online content issued by the relevant authority infringed their freedom to publish under Article 10 of the ECHR. Once such a case has been submitted, the court then determines whether the freedom to publish under Article 10(1) of the ECHR has been restricted in accordance with Article 10(2) of the ECHR.

## C. SECTION 3: OTT PLATFORMS

273. The general framework for regulation of over-the-top (OTT platforms) within the EU is the Audiovisual Media Service Directive 2010/13/EU (AVMSD), as amended by Directive (EU) 2018/1808.[202] For the purposes of this report, this Directive (as amended) will henceforth be referred to as the AVMSD.

### a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?

[199] *Animal Defenders International v. the United Kingdom* App no. 48876/08 (ECHR, 22 April 2013), paras 108-109.
[200] *Evans v. the United Kingdom* App no. 6339/05 (ECHR. 10 April 2007), para 89.
[201] *Animal Defenders International v. the United Kingdom* App no. 48876/08 (ECHR, 22 April 2013).
[202] Council Directive (EU) 2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L303/69, art 1(9).

274. As discussed earlier, there are a tapestry of measures dealing with electronic communication services and various policy concerns, such as terrorist content, the protection of children and consumer protection. However, these Directives operate as *lex specialis* and do not affect the existing framework in the AVMSD, which operates as *lex generalis*.

275. Video-sharing platform services' are also defined in Article 1(1)(aa) of the AVMSD. The Article adopts a tripartite definition, classifying 'video-sharing platform services' on the basis of three criteria. The commonality in all three criteria are that services provide 'programmes' or 'user-generated videos' to the 'general public', whether or not this is a 'principal purpose', an 'essentially functionality' or merely a 'dissociable section' of services of a 'wider nature'. Such platforms thus fall within the scope of the AVMSD as commercial services addressed to the public.

276. The chief purpose of the AVMSD is to govern EU co-ordination of national legislation on all audio-visual media. The relevant authorities are thus the legislative bodies of the EU (i.e. the European Parliament), as well as national media regulators, whose 'independence' is guaranteed by the 'Goals of EU co-ordination' highlighted by the European Commission.[203] There is nonetheless a role for regulators, since 'codes of conduct and voluntary practices' play a greater role in the online environment than in traditional sectoral environments.[204] Thus, whilst the AVMSD and the Directives mentioned earlier on protection of minors and commission of terrorist offences are the primary legislative instruments, regulatory requirements are also shaped by 'soft' legal instruments.

277. A 2015 report by the Directorate-General for Internal Policies[205] considers that EU-level harmonisation 'remains the only effective way of abolishing differences between the legal systems of individual Member States' by replacing them with 'a uniform set of rules, binding on all Member States and all commercial operators'.[206]

[203] European Union <www.europa.eu/european-union/index_en> accessed 28 September 2021.
[204] 'Over the Top Players: Market Dynamics and Policy Challenges' (European Parliament- Directorate General for Internal Policies) 73 <www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf> accessed 28 September 2021.
[205] ibid.
[206] ibid.

278. Nonetheless, as mentioned earlier, much regulation takes place in the form of voluntary measures adopted by OTT platform providers. For example, in 2016 the Commission agreed with Facebook, Microsoft, Twitter and YouTube on a 'Code of Conduct on countering illegal hate speech online'.[207] The Code provides that providers are to have in place 'clear and effective processes to review notifications regarding illegal hate speech' so they can remove or disable access to such content.[208] Similar codes include the Commission's 2015 Better Regulation Agenda, as well as the Communities of Practice (CoP).[209] Other initiatives supported by the Commission, such as the Better Internet for Kids and the European Cloud Computing Strategy, respond to specific social or industry concerns.

279. As such, the conclusion is that the regulatory space is largely defined by the self-regulation of OTT platforms.

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?**

280. Although the codes of conduct aforementioned provide for removal of potentially harmful content by *companies and providers*, they do not assist governmental authorities in removing or modifying OTT content. Governments are thus reliant on the framework of primary legislation provided by the EU.

*i) Article 28b(1)*

281. Under Chapter IXa AVMSD, Member States are the subjects of a new obligation, pursuant to Article 28b, to ensure that appropriate measures are taken by video-sharing platforms under their jurisdiction to protect i) minors from content which may impair their physical, mental or moral development (Art.28b(1)(a); ii) the general public from content containing incitement to violence or hate speech (Art.28b(1)(b); iii) the latter from content the

[207] Council (EC) of 31 May 2015 Code of Conduct countering hate speech online <www.ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/assessment_of_the_code_of_conduct_on_hate_speech_on_line_-_state_of_play__0.pdf> accessed 28 September 2021.
[208] ibid 2.
[209] 'Over the Top Players: Market Dynamics and Policy Challenges' (European Parliament- Directorate General for Internal Policies) 73 <www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf> accessed 28 September 2021.

dissemination of which constitutes a criminal offence (i.e. public provocation to commit a terrorist offence, child pornography, and racism and xenophobia) (Art.28b(1)(c)).

282. While Art. 28b(1) may be a means by which national authorities may affect the content hosted by OTT platforms, governments seeking to do so face the preliminary hurdle of establishing that the platform provider was established on its territory for the purposes of Art. 28a(1) or 28a(2).

283. A platform is within the jurisdiction of a Member State if it was established on the territory of that Member State within the meaning of Article 3(1) of Directive 2000/31/EC.

284. Assuming this is the case, under Article 28b(6), Member States may impose such measures which are "practicable and proportionate", and which must be determined "in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake."[210] Such measures include, for the protection of minors, the operation of age verification systems,[211] mechanisms for users to report or flag content[212] and parental controls.[213]

285. With regard to the protection of 'legitimate interests', it may be thought that the protection of freedom of speech represents a potential hurdle to governments seeking to remove content from OTT platforms. The 'free speech right' is enshrined in Art. 11 of the EU Charter of Fundamental Rights, which includes reference to the "freedom and pluralism of the media" (Art.11(2)) and which corresponds to Art. 10 of the European Convention on Human Rights. However, in *Delfi AS v Estonia*, the ECtHR held that the restriction of the internet portal Delfi's freedom of expression served the legitimate aim of protecting the reputation and rights of others.[214] Thus, although free speech is a statutory right, it is not immutable and may be displaced by 'legitimate aims'. Moreover, the decision to impose liability based on Delfi's failure to stop the defamatory comments despite the knowledge that the article in question had the potential to trigger defamatory comments caused

[210] Council Directive (EU)2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L303/69, art.28(3).
[211] ibid, art 28b(4)(e).
[212] ibid, art 28b(4)(d).
[213] ibid, art 28b(4)(h).
[214] ECHR, Grand Chamber, Case of *Delli AS v. Estonia* (Application no. 64569/09), Jun. 16, 2015, paras 130, 145.

significant controversy.[215] It nonetheless remains to be seen what the scope of 'legitimate aims' is, and whether *Delfi* can be confined to its facts (defamatory comments).

286. The measures may not, however, include ex-ante or upload filtering (Art. 28b(3)). In theory, this precludes national governments from monitoring OTT platforms.

287. However, the text of the AVMSD itself does not clarify whether such measures may include removal. It gives examples of appropriate measures, such as those mentioned above, including age verification and flagging – i.e., measures relying on notification of harmful content by users themselves. Nonetheless, Art.28b(6) may assist governmental authorities as far as removal is concerned. It authorises Member States to impose measures that are 'more detailed or stricter' than those referred to in paragraph (3) of the Article. Paragraph (3) is thus not exhaustive and is merely illustrative. Governments' ability to remove content from OTT platforms thus hinges on the scope and content of 'appropriate measures'[216]

288. Another limitation of Art.28b is that it operates 'without prejudice to Articles 12 to 15 of Directive 2000/31/EC'[217] (the 'Electronic Commerce Directive', otherwise known as the ECD). For the purposes of this report, Articles 12 and 15 are the most relevant. *Prima facie,* Art.28b appears not to infringe on cyber-liberalism by preserving some forms of intermediary immunity for OTT platform providers.

289. Article 12 ECD (the 'mere conduit' provision) provides that Member States shall ensure that the service provider shall not be held liable for information transmitted, provided the provider i) does not initiate the transmission;[218] ii) does not select the receiver of the transmission[219] and iii) does not select or modify the information in the transmission.[220] Article 15(1) ECD states that Member States shall not impose a general obligation on providers to monitor the information which they transmit or store, nor a general obligation to seek facts or circumstances indicating illegal activity. However, Member States may

[215] <www.globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/> accessed 22 October 2021.
[216] ML Montagnani and A Trapova, 'New Obligations for Internet Intermediaries in the Digital Single Market-Safe Harbors in Turmoil ?' (2019) 22(7) Journal of Internet Law 3.
[217] Council Directive (EU)2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L303/69, art 28b(1).
[218] Council Directive 2000/31EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) L 178/1, art 12(1)(a).
[219] ibid, art.12(1)(b).
[220] ibid, art 12(1)(c).

'establish obligations for information society service providers to inform the public authorities of alleged illegal activities undertaken or information provided by recipients of their service…'(Art. 15(2)).

*ii) Procedure*

290. Although the culminative effect of the AVMSD and Art. 16 ECD (which refers to 'the voluntary transmission of codes of conduct'[221]) is that much of the primary responsibility for content regulation lies with individual service providers, the ECD provides for a range of compliance mechanisms Member States may take against providers. Article 18(1) provides that Member states shall ensure that court actions available under national law concerning information services' activity allow for the rapid adoption of measures 'designed to terminate any alleged infringement and to prevent further impairment of the interests involved.' Article 19(1) also provides that Member States:

> shall have adequate means of supervision and investigation necessary to implement this Directive effectively and shall ensure the service providers supply them with the requisite information.

291. Member States must therefore legislate towards these ends in national law or face the prospect of an infringement procedure under Article 258 TFEU.

292. However, as previously mentioned, the primary regulatory responsibility appears to lie with the platform providers, with Member States playing a residual legislative role.

[221] ibid, art.16(1)(b).

# GERMANY

## A. SECTION 1: SOCIAL MEDIA INTERMEDIARIES

293. The position relating to social media intermediaries is governed by the German Network Enforcement Act ('*Netzwerkdurchsetzungsgesetz*' (NetzDG)), the Administrative Offences Act ('*Ordnungswidrigkeitengesetz*' (OWiG)), the German Civil Code ('*Bürgerliches Gesetzbuch*' (BGB)), the German Criminal Code ('*Strafgesetzbuch*' (StGB)), the German Constitution (*Grundgesetz* (GG)), the Inter-State Treaty on Media (*Medienstaatsvertrag* (MStV)) and the Telemedia Act (*Telemediengesetz* (TMG)).

### a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?

294. The Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)[222] governs the regulation of content on social media. Its stated objective is to combat online hate speech and fake news. The Act, however, does not impose a general obligation to monitor content on its platform, but merely to maintain an effective complaints procedure for processing user complaints and imposes reporting obligations in the form of publication of specified details in the Federal Gazette and on the platform's websi. The provider of a social network shall be exempt from the reporting and complaint procedure obligations stipulated in Act if the social network has fewer than two million registered users in the Federal Republic of Germany.

295. Section 3 of the Act mandates that on the receipt of a complaint the social media intermediary must take immediate note of it and check if the 'content reported in the complaint is unlawful and subject to removal or whether access to the content must be blocked'. It also imposes an obligation to remove manifestly unlawful content within 24 hours unless an agreement allowing for a longer time period has been reached with the law enforcement authority. For other content that is subject to challenge, there is a time limit of 7 days with provisos allowing for a longer time limit where a factual determination of the veracity of the allegation is required, or where the social media intermediary has agreed to

[222] Bundesgesetzblatt 2017, Part 1, Nr 61, p 3352 (German) <www.perma.cc/7UCW-AA3A> accessed 30 September 2021.

refer decisions regarding unlawfulness to a recognised self-regulation institution. What constitutes a recognised self-regulation institution is further defined in the section.

296. The Act elaborates on monitoring and reporting mechanisms and liability takes the form of regulatory fines for violations of these provisions. The Act on Regulatory Offences governs the imposition of regulatory fines and the competent administrative authority for such imposition is the Federal Office of Justice. According to section 4 of the Network Enforcement Act, 'the Federal Ministry of Justice and Consumer Protection, in agreement with the Federal Ministry of the Interior and the Federal Ministry for Economic Affairs and Energy, shall issue general administrative principles on the exercise of discretion by the regulatory fine authority in initiating regulatory fine proceedings and in calculating the fine.' The Act also provides for judicial appeal against the decision of the Federal Office of Justice.

297. Section 4(5) of the Act states that, 'if the administrative authority wishes to issue a decision relying on the fact that content which has not been removed or blocked is unlawful within the meaning of section 1(3), it shall first obtain a judicial decision establishing such unlawfulness. The court with jurisdiction over the matter shall be the court that rules on the objection to the regulatory fine order. The application for a preliminary ruling shall be submitted to the court together with the social network's statement. The application can be ruled upon without an oral hearing. The decision shall not be contestable and shall be binding on the administrative authority.'

298. The 2021 amendment to the Network Enforcement Act, 'authorizes the Federal Office of Justice to approve arbitration bodies organized under private law for out-of-court settlements of disputes between complainants/users and social media providers. Participation in arbitration is voluntary.'[223]

299. The Act to Amend the Network Enforcement Act in 2021 expanded the powers of the Federal Office of Justice. 'The amendment gives the Federal Office of Justice powers to supervise compliance with the act. Once it has determined that an infringement has occurred, the office can require the social media provider to remedy the infringement. It can also request information about implementation measures, the number of registered users in

[223] Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech' <www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/> accessed 29 September 2021.

Germany, and the number of complaints received in the past calendar year. Witnesses are obligated to testify in the administrative procedure.'[224]

300. In the case of removal, the content must be retained as evidence and stored for this purpose within the scope of Directives 2000/31/EC and 2010/13/EU for a period of ten weeks according to sec. 3 (2).

301. An intermediary can also be liable under civil law for third-party content it has stored for a user - as a so-called 'Störer' (interferer). This arises from sec. 1004 of the German Civil Code[225] by analogy in the case of infringements of personal rights and from copyright law.

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

302. While there is no separate provision for the government to order removal, the Network Enforcement Act allows for removal of content as detailed above.

303. Sec. 1 (3) of the Network Enforcement Act defines unlawful content as content that fulfils the requirements of regulations of the German Criminal Code[226] which affect the protection of the state, public order, personal honour and sexual self-determination. More specifically, the nature of the content would have to be

- Dissemination of propaganda material of unconstitutional organisations (sec. 86 German Criminal Code)
- Use of symbols of unconstitutional organisations (sec. 86a German Criminal Code)
- Preparation of serious violent offence endangering state (sec. 89a German Criminal Code)
- Instruction for committing serious violent offence endangering state (sec. 91 German Criminal Code)
- Treasonous forgery (sec. 100a German Criminal Code)

[224] 'Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech', <www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/> accessed 29 September 2021.
[225] See for an English version of an older version (2013) of the German Civil Code: <https://www.gesetze-im-internet.de/englisch_bgb/> accessed 23 September 2021.
[226] See for an English version of an older version (2019) of the German Criminal Code: <https://www.gesetze-im-internet.de/englisch_stgb/> accessed 23 September 2021.

- Public incitement to commit offences (sec. 111 German Criminal Code)
- Disturbing public peace by threatening to commit offences (sec. 126 German Criminal Code)
- Forming criminal organisations (sec. 129 German Criminal Code); Forming terrorist organisations (sec. 129a German Criminal Code); Foreign criminal and terrorist organisations; confiscation (sec. 129b German Criminal Code)
- Incitement of masses (sec. 130 German Criminal Code)
- Depictions of violence (sec. 131 German Criminal Code)
- Rewarding and approval of offences (sec. 140 German Criminal Code)
- Revilement of religious faiths and religious and ideological communities (sec. 166 German Criminal Code)
- Dissemination, procurement, and possession of child pornography (sec. 184b German Criminal Code)
- Insult (sec. 185 German Criminal Code); Malicious gossip (sec. 186 German Criminal Code); Defamation (sec. 187 German Criminal Code)
- Violation of intimate privacy by taking photographs or other images (sec. 201a German Criminal Code)
- Threatening commission of serious criminal offence (sec. 241 German Criminal Code)
- Forgery of data of probative value (sec. 269 German Criminal Code)

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

304. In addition to intellectual property violations, the types of content that can be removed are mainly covered by the Network Enforcement Act as discussed in the section above.

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

305. Amendments to the Network Enforcement Act which are in various stages of implementation greatly expand the access of the Federal Criminal Police (BKA) in cases of

online hate crimes to personal user data.[227] 'Personal data includes usernames, internet protocol (IP) addresses, port numbers and with a judicial order passwords.'[228]

## B. SECTION 2: ONLINE NEWS MEDIA

306. Online news media are subject to a rather complicated and piecemeal regulatory framework. This is due in part to a lack of specific regulation on online news media and in part to the federal structure of Germany because legislative powers concerning (online news) media are split between the federal level and the State level. While regulating the content of media is within the powers of the States,[229] the regulation of the technical side of (online) media[230] as well as criminal law,[231] criminal procedure,[232] civil law,[233] and the law of civil procedure[234] are not.[235] As a result, the regulatory landscape is quite complex. Yet there are only few, if any, differences between the regulation of the sixteen German States because the States have agreed on Inter-State treaties between them ('*Staatsvertrag*') harmonizing the rules applicable to media. These treaties are the Inter-State Treaty on Media ('*Medienstaatsvertrag*' (MStV)) and the Inter-State Treaty on Media and the Protection of Minors ('*Jugendmedienstaatsvertrag*' (JMStV)). The MStV is of quite recent vintage as it entered into force on November 7 2020 replacing the former Inter-State Treaty on Broadcasting ('*Rundfunkstaatsvertrag*' (RStV)). Thus, there is only few if any case law on its provisions

307. Also, constitutional law issues of online news media contribute to the complexity of the regulatory framework because online news media are subject to (scholarly) debate on the basic right applicable to such activities. Given the historical roots of the press in written

[227] Freedom House, 'Germany' <www.freedomhouse.org/country/germany/freedom-net/2021> accessed 30 September 2021.
[228] ibid.
[229] See arnd Uhle, 'Art 73' in Theodor Maunz and Günter Dürig, *Grundgesetz-Kommentar* (94th edn, C.H. Beck 2021) paras 166 and 172.
[230] The federal level possesses exclusive legislative powers for matters of telecommunication pursuant to Art 73(1) No. 7 Basic Law.
[231] See for an English version of an older version (2019) of the German Criminal Code: <www.gesetze-im-internet.de/englisch_stgb/> accessed 27 August 2021.
[232] See for an English version of an older version (2019) of the German Code on Criminal Procedure: <www.gesetze-im-internet.de/englisch_stpo/> (last visited 27 August 2021).
[233] See for an English version of an older version (2013) of the German Civil Code: <www.gesetze-im-internet.de/englisch_bgb/> accessed 27 August 2021.
[234] See for an English translation of an older version (2013) of the Code of Civil Procedure: <www.gesetze-im-internet.de/englisch_zpo/englisch_zpo.html> accessed 27 August 2021.
[235] Here, the federal level exercised its legislative powers under Art 74(1) No. 1 Basic Law.

publications, online news had been traditionally excluded from the scope of application of the freedom of the press[236] and were, instead, protected by freedom of broadcast[237].[238] Even though the Federal Constitutional Court held in a recent judgment that the content of online news media is protected by the freedom of the press, this case concerned archives providing access to older articles which had been published in print before.[239] It seems, hence, that only for the online distribution of a print medium, one can safely argue that it is protected by the freedom of the press,[240] while a growing number of scholars argue that the freedom of the press also protects online-only news media.[241] Whereas online media would be protected by the Constitution either way, the debate has consequences on the regulatory sphere because the constitution allows broadcasting to be a largely regulated activity (and its exercise depends on a licence) while it does not do so for the press.[242] Thus, the differences of opinion on the constitutional right protecting online media has a bearing on governmental powers that may be exercised against such activities. As will be seen later, this might account for the potentially far-reaching governmental powers vis-à-vis digital media.

308. In any case, State legislation on media does not treat online news pages as press, but as 'Telemedien'.[243] Accordingly, pure online media are not subject to the States' legislation on the press,[244] but the MStV.

**a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website? What is the procedure that the government follows to make such an order and to ensure compliance?**

[236] Art 5(1) sentence 2 alternative 1 Basic Law.
[237] Art 5(1) sentence 2 alternative 2 Basic Law.
[238] See Franz Schemmer, 'Art 5' in Volker Epping and Christian Hillgruber (eds), *Beck'scher Online-Kommentar Grundgesetz* (47th edn, C.H. Beck 2021), para 43; Helmuth Schulze-Fielitz, 'Art. 5 Abs. 1-2' in Horst Dreier (ed.), *Grundgesetz-Kommentar* (3rd edn, Mohr Siebeck 2013), para 91.
[239] 1 BvR 16/13, 2020 (Federal Constitutional Court, 6 November 2019) para 94.
[240] See Christian Starck and Andreas Paulus, 'Art 5' in Hermann von Mangoldt, Friedrich Klein and Christian Starck, *Grundgesetz* (7th edn, C.H. Beck 2018) para 132.
[241] Christoph Grabenwarter, 'Art 5 Abs. 1, Abs. 2' in Theodor Maunz and Günter Dürig, *Grundgesetzkommenar* (94th edn, C.H. Beck January 2021), para 251; Hans D. Jarass, 'Art 5' in Hans D. Jarass and Bodo Pieroth, *Grundgesetz für die Bundesrepublik Deutschland* (16th edn, C.H. Beck 2020), para 111a; Rudolf Wendt, 'Art 5' in Ingo von Münch and philip Kunig, *Grundgesetz-Kommentar* (7th edn, C.H. Beck 2021) para 59.
[242] See on the difference and its roots in the Federal Constitutional Court's jurisprudence: Christoph Möllers, 'Freedom of the press on the Internet ('Pressefreiheit im Internet)' (2008) 39 *Archiv für Presserecht* 241.
[243] See Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021), para 3 who critizes this technique.
[244] There are, however, two notable exceptions: the Saarland and Rhineland-Palatinate have enacted Media Laws which also apply to online media, see Sect. 1(1) Landesmediengesetz Rheinland-Pfalz and Sect. 1(1) Mediengesetz Saarland.

309. As there is no comprehensive act specifically on online news media, government powers to remove online news items are scattered in the three main branches of German law, that is public law, private law, and criminal law.

*i) Public law powers to remove online news items*

310. State authorities may remove online news items on the basis of Sect. 109 MStV and Sect. 20(1) and (4) JMStV.[245] Under Sect. 109 MStV (in conjunction with Sect. 20(4) JMStV) content may be removed if it violates rules under the MStV such as obligations on advertisements or gambling[246] or contains content contrary to JMStV such as fighting the liberal democratic order ('freiheitlich-demokratische Grundordnung'),[247] glorifying Nazi crimes or war, inciting hatred against minority groups, or child pornography.[248] Notably, some obligations under the MStV are exempted from being enforced by the State Media Authorities ('*Landesmedienanstalten*'), including *inter alia* requirements on legal notices,[249] while the duty to adhere to recognized standards of journalism ('*anerkannten journalistischen Grundsätzen*') are only partially excluded from these government powers. Courts and literature also acknowledge that the State Media Authorities may also enforce civil law and criminal law rules on the protection of honour or other legislation,[250] even if the person concerned does not initiate proceedings him- or herself.[251] Thereby, the provision allows for a potentially far-reaching control of online news media.

---

[245] Online news media are generally regarded as tele-media ('Telemdedien'), more precisely as tele-media with journalistic and editorial content ('*journalistisch-redaktionell*') see Bernd Holznagel and Sarah Hartmann, 'Teil 3 Rundfunk und Telemedien' in Thomas Hoeren, Ulrich Sieber and Bernd Holznagel (eds), *Handbuch Multimedia-Recht* (56th edn, C.H. Beck 2021), para 115. Because Sect. 20(4) JMStV effectively only extends the enforcement powers granted under Sect. 109 MStV to enforce violations of the JMStV, it suffices for present purposes to treat both as one and indicate differences where applicable.

[246] Sect. 22 MStV.

[247] See for a definition 1 BvB 1/51 (Federal Constitutional Court, 23 October 1952) 12 ; see for a translation of the pertinent part of the judgment: Christian Bumke and Andreas Voßkuhle, *German Constitutional Law* (OUP 2020), para 1509.

[248] See for the full list Art. 4 JMStV. The provision largely reflect criminal law offences, without requiring any mens rea, see Murad Erdemir, '§ 4 JMStV' in Gerald Schuster and Fabian Spindler (eds), *Recht der elektronischen Medien* (4th edn, C.H. Beck 2019) para 1.

[249] Sect. 109(1) sentence 1 MStV, see further Christoph Fiedler, '§ 109 MStV' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021) para 8.

[250] Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021, para 18.

[251] Different from its predecessors, s 109 MStV does not establish a subsidiary role of the government authorities if third party rights are in question, see s 59(5) RStV.

311. For violations of recognized standards of journalism,[252] the MStV introduces a differentiated model of oversight involving industry self-regulation. Basically, the provision distinguishes three types of news outlets. *First*, all those news outlets being members of the German Press Council are subject to the Press Council's compliance procedures only.[253] *Secondly*, online news media may also join other organisations of industry self-regulation.[254] However, the State Media Authorities may review decisions taken by those organization and demand their reversal,[255] which the State Media Authorities may not do vis-à-vis decisions taken by the German Press Council. *Thirdly*, those media not being a party to any such form of industry self-regulation are subject to the complete authority of the State Media Authorities under Sect 109 MStV.[256]

312. As far as enforcement is concerned, an order to remove online content ('*Verwaltungsakt*') may be enforced without an additional court order according to the respective State's laws on enforcing acts of the administration ('*Landesverwaltungsvollstreckungsgesetze*'). Before enforcing the order, the State Media Authority, would have to threaten enforcement and decide for a method of enforcement prior to actually enforcing. Importantly, the authority would be obliged to adhere to the principle of proportionality when doing so.[257]

313. Given the difficulties involved in targeting authors or news outlets based abroad,[258] the State Media authorities may also oblige third-parties (such as host, cache or access providers) to remove content if the provider of the news media itself may not be addressed successfully.[259] Thus, the liability of third-parties such as host, cache or access providers is of a subsidiary nature only. Importantly, Sect. 109(3) MStV ties any such responsibility of third parties to

---

[252] S 19 MStV. Essentially, this provision obliges mediat o adhere to basic principles of journalism ('journalistische Grundsätze'). Most importantly, journalists are obliged to check facts as far as possible and to reproduce them accurately, see Wolfgang Lent, '§ 19 MStV' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021) para 5.

[253] Under its rules of procedure, the remedies for any violation of the German Press Code are an advice notice, a disapproval, or a reprimand (Sect 10(5) German Press Code). The Press Council may not order the removal of any content. See for an English version of the German Press Code: <www.presserat.de/files/presserat/dokumente/download/Press%20Code.pdf> accessed 27 August 2021.

[254] See s 19(3) and (4) MStV.

[255] See s 19(8) MStV.

[256] Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021, para 16; Wolfgang Lent, 'Paradigmenwechsel bei den publizistischen Sorgfaltspflichten im Online-Journalismus – Zur Neuregelung des § 19 Medienstaatsvertrag' (2020) 64 *Zeitschrift für Urheber- und Medienrecht* 593, 596.

[257] See 6 K 7151/02 (Administrative Court of Cologne, 3 March 2005), 2005 MultiMedia und Recht 399, 401.

[258] Probably the most common obstacle of ensuring removal of a news item is raised by unknown or foreign news outlets or authors.

[259] S 109(3) MStV.

the requirements under the Federal Act on Telemedia ('*Telemediengesetz*', TMG).[260] Generally speaking, addressing third parties for domestic online publications will be disproportionate because the company or person running the online news site can be addressed first.[261]

314. To evaluate the government powers under Sect. 109 MStV, it is instructive to contrast them to the powers to confiscate the printed press. The latter is subject to confiscation under criminal law only.[262] Thus, online media is subject to more far reaching government interference than the printed press, which has been criticised in the literature arguing that the protection accorded to the printed press should be extended to online media.[263] While this argument finds support in the increasing inclination to include online media in the freedom of the press, courts so far have not supported this view.[264] If, thus, the enforcement powers against online press media are perhaps surprisingly far-reaching, there is no indication of a widespread use of any such powers. In any case, the basic rights would severely limit any such activities. The powers of Sect. 109 MStV appear to be rarely invoked (apart perhaps from issues of pornography and illicit gambling) in relation to the content of online media, perhaps with the most widely discussed exception of a line of cases against websites containing Nazi propaganda in the early 2000s.[265]

*ii) Civil law remedies against content*

315. Whereas the powers under Sect 109 MStV (or for that purpose its predecessors) have been of little practical relevance due to their stringent requirements,[266] civil law liability has played a much bigger role. Notably, online news media are liable for their own content (or third-party content which they adopted as their own)[267] according to the general rules of civil

[260] S 7-10 TMG, 2007.
[261] Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021, para 54.
[262] Hartmut Brenneisen, 'Polizeirechtsfestigkeit der Presse- und Versammlungsfreiheit' (2021) 136 *Deutsches Verwaltungsblatt* 931-935. This is the case because the States' Acts on the Press are a *lex specialis* vis-à-vis all other government powers and these acts either do not provide for powers of confiscation.
[263] Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021), para 43; Wolfgang Schulz, '§ 59 RStV' in Reinhart Binder and Thomas Vesting (eds) *Beck'scher Kommentar zum Rundfunkrecht* (4th edn, 2018), para 15; see on earlier legislation: Christoph Engel, 'Die Internet-Service Provider als Geiseln deutscher Ordnungsbehörden' (2003) 6 MultiMedia und Recht (Beilage 4/2003) 1-35.
[264] See for such a view 8 B 2567/02 (Higher Administrative Court Münster, 19 March 2003), 2003 Neue Juristische Wochenschrift 2183, 2185. See for a critical assessment: Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021) [43].
[265] See 8 B 2567/02 (Higher Administrative Court Münster, 19 march 2003, 2003 Neue Juristische Wochenschrift 2183, 2185; see also Schulz (n 263) paras 52 et seq.
[266] See Frederik Ferreau, 'Desinformation als Herausforderung für die Medienregulierung' (2021) 52 Archiv für Presserecht 204-210, 206.
[267] VI ZR 144/11 (Federal Supreme Court, 27 March 2012), 2012 Neue Juristische Wochenschrift 2345.

law.[268] Crucially, government agencies may also invoke these provisions to remove content.[269]

316. Under civil law, a person may file a claim for injunctive relief ('*Unterlassungsanspruch*')[270] based on an analogous application of Sect. 1004 Civil Code[271] if the content is either factually incorrect (in case of a statement of fact) or otherwise libellous (in case of an opinion).[272] Essentially, this claim is based on the protection of the personal honour, standing, and integrity of a person. The claim also encompasses the removal of online articles.[273] Importantly, German civil law also knows a more far-reaching remedy obliging media to publish a retraction ('*Widerruf*'). This remedy is, however, only available against statements of fact due to the overriding importance of the freedom of opinion.[274] Apart from injunctive relief according to Sect. 1004 Civil Code, a similar obligation to remove content may also arise as a consequence of a tort.[275] In contrast to injunctive relief, which works on a no-fault basis, such a liability requires at least negligent conduct on the side of the news media.

317. The obligation to remove content under Sect. 1004 Civil Code also applies to other persons than those who wrote or published the content. While the TMG provides for some privileges *inter alia* for host and access providers,[276] it is generally understood that these privileges do not apply to claims for injunctive relief.[277] Thus, host provider, access, or cache provider are equally liable under this provision. For other causes of action, the privileges do, however, apply. Most importantly, providers are not obliged to monitor the legality of third-party content they deal with.[278]

---

[268] S 7(1) TMG.
[269] See for the federal State: VI ZR 83/07 (Federal Supreme Court 22 April 2008), 2008 Neue Juristische Wochenschrift 2262, 2265.
[270] See Heinz Georg Bamberger and Christian Förster, '§ 12' in Wolfgang Hau and Roman Poseck (eds), *Beck'scher Online-Kommentar BGB* (59th edn, C.H. Beck 2021) [365].
[271] N.B. courts do also invoke other provisions as a basis without however having an influence on the substance of the claim, see Frank Spohnheimer, '§ 1004' in Beate Gsell, Wolfgang Krüger, Stephan Lorenz and Christoph Reymann (eds), *Beck'scher Online-Großkommentar BGB* (C.H. Beck 2021) [332].
[272] N.B. German law traditionally distinguishes opinions (which are protected by Art 5(1) Basic Law) and statements of facts (which are not). As a consequence of this distinction, the remedies for these scenarios differ.
[273] See VI ZR 340/14, (Federal Supreme Court, 28 July 2015), 2016 Neue Juristische Wochenschrift 56, 57.
[274] Heinz Georg Bamberger and Christian Förster, '§ 12' in Wolfgang Hau and Roman Poseck (eds), *Beck'scher Online-Kommentar BGB* (59th edn, C.H. Beck 2021) [354].
[275] In particular, it may arise as a consequence arising from S 823(1) Civil Code, S 823(2) Civil Code in conjunction with e.g., a criminal offence (S 187 Criminal Code for instance) or S 824 Civil Code.
[276] See s 8-10 TMG.
[277] See I ZR 304/01, 158 BGHZ 236, 246 (Federal Supreme Court, 11 March 2004), ; Christian Volkmann, '§ 1004 BGB' in Gerald Spindler and Fabian Schuster (eds), *Recht der elektronischen Medien* (4th edn, C.H. Beck 2019) para 65.
[278] S 7(2) TMG.

318. As a result of such a civil lawsuit, if successful, the government holds a title requiring the online news provider to remove the article which is enforceable under the rules civil procedure. In the case of an injunction against an online news item, compliance is enforced by imposing a penalty payment (of up to EUR 25,000) or coercive detention.[279] Notably, such enforcement proceedings require yet another Court proceeding in which, however, the merits are no longer subject of the dispute.

*iii) Criminal law procedures to remove online media content*

319. Removing online news items under criminal law first requires a criminal offence. For present purposes, insult[280] and defamation[281] are among the most important. Under German criminal law, it may also be punished if defamatory allegations of fact may not be proved by the defendant.[282] Theses offences do not only protect personal honour and dignity, but they also extend their protection to groups of persons[283] and punish the allegation of untrue or not provable facts vis-à-vis other persons than the victim which are of a defamatory character as well as libellous opinions or facts regardless of whether they are alleged only in the presence of the victim or a third person. In addition, there are various other delicts which may be committed by online news media such as disparagement of the State and the denigration of symbols incriminating inter alia public 'uses [of] abusive language against or maliciously disparages the Federal Republic of Germany or one of its Länder or its constitutional order'.[284]

320. If such an offence has been committed, the Criminal Code and the Code of Criminal Procedures provide powers of confiscation *before* a criminal conviction[285] as well as a further consequence *of* a conviction.[286] The former power is provisional in nature and is aimed at securing the later (final) confiscation. Yet, these powers do not cover data per se, but only the data storage medium (i.e. a server).[287] They depend on the finding of an illegal content and are, thus, consequences of criminal proceedings.

---

[279] S 888 Code of Civil Procedure. See on the application to injunctions VI ZR 236/61, BGHZ 37, 187, 190 (Federal Supreme Court, 5 June 1962),; see also Ralf Bendtsen, '§ 888 ZPO' in Johann Kindl and Caroline Meller-Hannich (eds), *Gesamtes Recht der Zwangsvollstreckung* (4th edn, Nomos 2021) para 5.
[280] S 185 Criminal Code.
[281] S 187 Criminal Code.
[282] S 186 Criminal Code.
[283] The exact contours of such protection are subject to intricate doctrinal constructions, see Brian Valerius, '§ 185' in Bernd v. Heintschel-Heinegg (ed.), *Beck'scher Online-Kommentar StGB* (50th edn, C.H. Beck 2021) paras 8-13.
[284] S 90a Criminal Code. A similar offence can be committed against organs of the State, see s 90b Criminal Code.
[285] S 111b, 111q Code of Criminal Procedure.
[286] S 74, 74d Criminal Code.
[287] Qs 34/13 (Local Court Hamburg, 2 September 2013) 629, 2013 Neue Juristische Wochenschrift 3458, 3459.

**b) What are the tests or standards for determining whether an online news article/page needs to be removed?**

321. Although there are different provisions allowing for the removal of online news content, any such removal has to involve a balancing test. Importantly, any of these tests will be heavily influenced by the applicable basic rights, which, consequently, means that the tests will be relatively stringent in any case.

*i) Requirements to remove online content under public law*

322. Using the powers under the MStV and JMStV is subject to a test of proportionality. Ordering the removal of a news item is only legal if there is no other – equally effective – way to achieve the desired aim[288] and any such measure must be restricted to parts of the content if this suffices to achieve the desired aim.[289] Most importantly, ordering the removal is illegal if this is disproportionate compared to the importance of the content for the provider or the general public.[290] Essentially, these provisions do no more than reiterating the constitutional test of proportionality that would apply anyways.[291]

323. If the online media includes content which is also printed, any such removal is subject to additional requirements aiming at re-aligning confiscation under the MStV with the powers under the Code of Criminal Procedure.[292] Hence confiscation must not be out of proportion to the relevance of the aim pursued, taking into account the importance of the basic rights and it must be ordered by a court.[293] Yet, this rule is textually limited to instances where the digital content has also been printed. This raises intricate questions on the scope of government powers for online-only media (or media with content which is only partially identical with the print version). On face value, it would seem that those publications do not profit from the privilege accorded under this rule. Given the increasing willingness to protect online media under the freedom of the press, it seems logical to extend the provision to the online-only 'press' as well. In any case, an order to remove online news media would have

[288] S 109(2) sentence 2 MStV.
[289] S 109(2) sentence 3 MStV.
[290] S 109(2) sentence 1 MStV.
[291] Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021, para 31.
[292] Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021, para 35.
[293] S 109(2) sentence 4 MStV.

to scrutinized in light of the applicable basic rights, most importantly the freedoms of press (or broadcasting), as well as opinion (if applicable).

*ii) Requirements to remove online content under civil law*

324. As the State does not have a personal honour of itself, the Federal Supreme Court limited claims under Sect. 1004 Civil Code to remove (online) statements to instances, which could have a grave influence on the functioning of the agency in question.[294] Crucially, the Court remarked that the State may not use civil law to silence critique on its actions. Thus, the role of the basic rights had to be taken into account when assessing the merits of the claim.[295]

325. According to the *jurisprudence constante* of the Federal Supreme Court, a Court analysing a claim for injunctive relief in such matters must engage in a balancing exercise weighing the competing rights and interests at stake.[296] If the State brings such a claim, a court will have to give special consideration of the freedoms of press, opinion, or broadcasting in question.[297]

*iii) Requirements to remove online content under criminal law*

326. Before discussing the tests applied by Courts to determine whether online content must be removed, it is important to note that this is only a consequence of a criminal conviction. Thus, the online content concerned must violate a criminal law. At this point, the justification afforded to statements safeguarding legitimate interests[298] is of vital importance. While the press does not enjoy any special rights in this regard,[299] the provision requires a careful balancing of competing interests and, importantly the statement must be appropriate, necessary and proportionate to safeguard the legitimate interest.[300] For the press, it is a legitimate interest to research and disseminate news of public interest, take positions, criticise, or otherwise participate in public discourse.[301] For the balancing analysis, Courts

[294] VI ZR 83/07, (Federal Supreme Court, 22 April 2008) 2262, 2265.
[295] ibid.
[296] See VI ZR 175/58 (Federal Supreme Court, 22 December 1959), 31 BGHZ 308, 312; Frank Spohnheimer, '§ 1004' in Beate Gsell, Wolfgang Krüger, Stephan Lorenz and Christoph Reymann (eds), *Beck'scher Online-Großkommentar BGB* (C.H. Beck 2021), para 334.4.
[297] Stefan Söder, '§ 823 BGB' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021) para 294.
[298] S 193 Criminal Code.
[299] Brian Valerius, '§ 193' in Bernd v. Heintschel-Heinegg (ed.) *Beck'scher Online-Kommentar StGB* (50 edn, C.H. Beck 2021) para 36.
[300] Philipp Regge and Christian Pegel, '§ 193' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zuum Strafgesetzbuch* (4th edn, C.H. Beck 2021) paras 30-35.
[301] Kristian Kühl, '§ 193' in Karl Lackner and Kristian Kühl (eds), *Strafgesetzbuch* (29th edn, C.H. Beck 2019) para 8.

also take into account whether the standards of journalism have been adhered to.[302] These standards, among others entail obligations to verify information, indicate doubts, and not arbitrarily deviate from sources.[303]

327. Even if a news item causes criminal liability, a Court may order its (or rather the data storage's) confiscation only if the content itself is punishable and it if it either has been disseminated at least once illegally or is intended for such use.[304] Generally speaking, the former is the case if the content is seditious, offensive, inciting hate against minorities, glorifying violence, pornographic, or otherwise libellous.[305] Despite the mandatory language employed in Sect 74d Criminal Code, a Court has to assess the proportionality of such measure and, *inter alia*, take into account the basic rights at stake.[306]

328. Importantly, only if the object subject to confiscation is within the possession of those involved in the dissemination, a confiscation may be ordered. At this point, it is crucial that online content itself is not subject to such measures (because its intangible data only), but its physical storage.[307] As, in turn, the hosting servers are not in the possession of its clients (who disseminate illegal content), these may not be subjected to confiscation under criminal law.[308] However, as the web host is obliged to remove illegal content in line with its liability under civil law in conjunction with Sect 10 TMG, those providers will usually have a contractual right to delete such content (on short notice) based on their contract with the media concerned.[309]

329. Even before the conviction, such measures may be ordered by a Court under Sect. 111b Code of Criminal Procedure if there is reason to believe that the items will be subject to confiscation under Sect. 74d Criminal Code. According to the Federal Supreme Court's case law, this is the case if there is a certain probability that the items will be confiscated as a

---

[302] See ibid para 11; see already Federal Constitutional Court, order of 25 january 1961, 1 BvR 9/57, 12 BVerfGE 113, 130.
[303] See in more detail Jörg Eisele and Ulrike Schittenhelm, '§ 193' in Adolf Schönke and Horst Schröder *Strafgesetzbuch* (30th edn, C.H. Beck 2019) para 18.
[304] S 74d(1) sentence 1 Criminal Code.
[305] Wolfgang Joecks and Markus Meißner, '§ 74d' in Wolfgang Joecks and Klaus Miebach (eds) *Münchener Kommentar zum Strafgesetzbuch* (4th edn, C.H. Beck 2020) para 8.
[306] Frank Saliger, '§ 74d' in Urs Kindhäuser, Ulfried Neumann and Hans-Ullrich Paeffgen (eds) *Strafgesetzbuch* (5th edn, Nomos 2017), para 15.
[307] Local Court (LG) Hamburg, court oder of 2 September 2013, 629 Qs 34/13, 2013 Neue Juristische Wochenschrift 3458, 3459 et seq.
[308] Astrid Auer-Reinsdorff, '§ 21 Providerverträge' in Astrid Auer-Reinsdorff and Isabell Conrad (eds) *Handbuch IT- und Datenschutzrecht* (3rd edn, C.H. Beck 2019) para 47.
[309] See for such a clause ibid para 45.

result of criminal proceedings.[310] Irrespective of whether the content forms part of the press, such measures may not be ordered 'if its prejudicial consequences, in particular jeopardising the public interest in prompt dissemination, are manifestly disproportionate to the importance of the matter.'[311]

### c) Is the order of a court/tribunal a prerequisite for removal of online content?

330. As far as criminal law and civil law[312] are concerned, any removal of online content is subject to a prior court decision. Notably, even in cases of imminent danger, the Code of Criminal Procedure requires a prior court order if a content is published periodically.[313] Online media may very well fulfil this requirement.[314] Only contents not published periodically may be confiscated by an order of the public prosecutor, which, however, needs to be approved by a Court within three days of issuing of the public prosecutor's order.[315]

331. For public law, this is a matter of uncertainty and largely depends on the interpretation accorded to the MStV.[316] If it is construed literally, online-only media could be subject to confiscatory measures without any court decision. From a constitutional law perspective, it seems plausible to subject any removal of online news content to a prior Court order and thus treat online media on an equal footing with the traditional press.[317] Yet, this issue has not been adjudicated so far with regard to online press.

## C. SECTION 3: OTT PLATFORMS

### a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?

[310] Federal Supreme Court (BGH), order of 12 july 2007, StB 5/07, 2008 NStZ 419.
[311] S 111q(1) Code of Criminal Procedure.
[312] While an obligation to remove content under civil law does exist theoretically even without a court decision, any enforcement would require a title which would, almost exclusively, be a court decision, see S 704 Code of Civil Procedure.
[313] S 111q(4) sentence 2 Code of Criminal Procedure.
[314] See Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021, para 37.
[315] S 111q(4) sentence 2 and 3 Code of Criminal Procedure.
[316] More precisely, the privilege accorded to online media (partially) identical with the printed press under Sect. 109(2) sentence 4 MStV.
[317] See for such a view Christoph Fiedler, '§ 2 HPresseG' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021, para 42.

332. The MStV – which also provides the most important regulatory framework for online news media – is also the single most relevant piece of legislation on this issue. Basically, the MStV introduces three types of media which can be relevant for OTT platforms. These are media platforms ('*Medienplattform*'), media intermediaries ('*Medienintermediär*'), and user interfaces ('*Benutzeroberflächen*'). The main difference between media platforms and media intermediaries is the role the content provider plays in selecting and curating the content while both offer a variety of tele media or broadcasting-services. The difference is best seen when comparing platforms like YouTube and Netflix. Whereas the latter curates their content consisting of own and third-party tele media, the former basically allows any kind of tele media to be uploaded without deciding on the content. Therefore, Netflix is a media platform under the MStV, while YouTube is a media intermediary.[318] Such a distinction is, however, impossible with regard to user interfaces because both of them will (almost inevitably) have such an inter-face and, thus, the provisions applicable to user interfaces will apply alongside the specific provisions on media platforms or intermediaries respectively.[319] For present purposes, the report will only address media platforms because curating the content by the provider is the more realistic scenario for on-demand video streaming platforms.

333. While the MStV is the most relevant piece of regulation, it is worth pointing out the rules on civil liability as well as criminal liability previously discussed remain applicable. Also the JMStV applies to media platforms and, accordingly, the State Media Authorities may order the removal of content pursuant to Sect. 20(1) and (4) JmStV in conjunction with Sect. 109 MStV if the content violates the prohibitions under the JMStV.

334. Under the MStV, media platforms are obliged to guarantee a diverse programme. In particular, when selecting/admitting third-party content, they may not discriminate against comparable content and they may not unreasonably restrict access to the platform for those providers.[320] The ultimate aim of this provision is to guarantee that the technical side of the platform as well as access to it are not designed in a way that would undermine the diversity of the program.[321]

---

[318] Stephan Ory, 'Medienintermediäre, Medienplattformen, Benutzeroberflächen?', (2021) 65 *Zeitschrift für Urheber- und Medienrecht* 472, 479.
[319] ibid.
[320] S 82 MStV.
[321] Andreas Gummer, '§ 82' in Hubertus Gersdorf and Boris Paal (eds) *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021) para 46.

335. Regarding the user interface, the MStV establishes prohibitions of discrimination and unreasonable restrictions to the findability of content in the platform as well as specific requirements for content from public or private broadcasting.[322] Interestingly, the MStV also requires the platform to ensure that the user may easily customize the arrangement of contents on the interface in a permanent way.[323] Media platforms are also obliged to lay open the principles guiding the selection and arrangement of content on their platform. This information must be permanently, directly, and easily accessible to its users.[324] Besides, the MStV also posits that media platforms are bound by the constitutional order and are obliged to obey all general laws[325] and the laws protecting personal honour.[326]

336. Despite the far-reaching regulation of OTT platforms, it is worth noting that they do not require any prior licensing.[327] Rather, a potential provider of a media platform or a potential intermediary only has to inform the competent State Media Authority of this intention one month prior to starting its business.[328] Besides, the obligations outlined above do not apply to media platforms which generally have less than 20,000 daily users on the monthly average.[329]

337. As OTT platforms fall within the purview of the MStV, the State Media Authorities have jurisdiction to control them. As a measure of last resort, they may take legal measures under Sect. 109 MStV, which also allows for the removal of content (if necessary). As has been pointed out above, the State Media Authorities are independent from government authorities. To specify the content of the obligations under the MStV, the State Media Authority are authorized to enact rules ('*Satzungen*'). This power is, however, restricted by the limits of the authorization.[330]

---

[322] S 84(2)-(5) MStV.
[323] S 84(6) MStV. This requirement is, however, subject to the technical feasibility. The provider may provide proof that such a change is either technically impossible or would require a disproportionate effort, Sect. 84(7) MStV.
[324] S 85 MStV.
[325] This term refers to Art 5(2) Basic Law which provides that any limitation on the freedoms of expression, press, and broadcasting may only be imposed by general law. This term has been subject to quite some controversy, and it would seem to prohibit laws that prohibit an opinion as such without pursuing a legal interest worthy of protection irrespective of the opinion, see Bumke and Voßkuhle (n 247) paras 656-665.
[326] S 79(3) MStV.
[327] Andreas Gummer, '§ 79' in Hubertus Gersdorf and Boris Paal (eds), *Beck'scher Online-Kommentar Informations- und Medienrecht* (32nd edn, C.H. Beck 2021) para 7.
[328] S 79(2) MStV.
[329] S 78 sentence 1 No. 2 MStV.
[330] S 88 MStV.

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?**

338. The requirements and procedures established under Sect. 109 MStV apply *mutatis mutandis* to the removal or modification of content on OTT platforms. Thus, violations of the duties incumbent upon media platforms can be sanctioned by State Media Authority. Any such measure is, however, contingent upon a proportionality test.[331] Importantly, the MStV also imposes a duty upon OTT platforms to fulfil orders against third-party content that is disseminated via the platform.[332]

[331] S 109(2) sentence 1-3 MStV.
[332] S 79(4) sentence 2 MStV.

# UNITED STATES OF AMERICA

## A. SECTION 1: SOCIAL MEDIA INTERMEDIARIES

339. In the United States, there are two significant hurdles which present themselves to both government and the private citizen in relation to social media intermediaries' decisions surrounding content. First, courts have routinely held that the First Amendment[333] only provides protection against state actors and is not implicated by the action of private companies. Second, the provisions of Section 230 of the Communications Decency Act 1996 (CDA) impose some restrictions. In the backdrop of these legal instruments, this section will address how the USA regulates social media intermediaries.

### a) What are the circumstances in which a social media intermediary and its officers may be held liable for content posted on its website/mobile app?

*i) Section 230 of the Communications Decency Act 1996*

340. Section 230(c)(1) of the CDA states that: 'no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.'[334]

341. Section 230(c)(2)(a) further provides that 'no provider or user of an interactive computer service shall be held liable on account of – any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.'[335]

342. The two provisions of the CDA highlighted create immunity from liability in a coordinated manner. First, Section 230(c)(1) provides intermediaries with a 'safe harbour' provision, whereby interactive service providers are not treated as the publisher or speakers of third-party generated content. Second, Section 230(c)(2), also known as the 'Good Samaritan

[333] The First Amendment states: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. Constitution of the United States, Amendment I.

[334] 47 USC s 230(c)(1).

[335] 47 USC s 230(c)(2)(a).

Clause', provides that interactive service providers and users may not be held liable for voluntarily acting in good faith to restrict access to objectionable material. Although Section 230 of the Communication Decency Act is often interpreted as a requirement that interactive service providers act neutrally, the combined effect of the two clauses has the consequence of creating an effect wholly opposite to that sentiment.[336]

343. Section 230(f)(2) defines an interactive computer service as 'any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server.'[337] As subsequent court decisions have clarified, online platforms such as Facebook, Twitter and other social media intermediaries are considered "interactive computer service" providers.[338]

344. Section 230(e)(3) of the Communication Decency Act pre-empts any contrary state law, providing that 'no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section'.[339] Section 230(e) outlines a few exemptions where immunity will not apply: federal criminal statutes,[340] intellectual property law,[341] and sex trafficking laws.[342] For instance, Section 230 of the CDA will shield Internet Service Providers, including social media intermediaries, from legal suits alleging defamation online.

345. Although the categories of 'interactive computer service' provider and 'information content provider' appear to be diametrically opposed to one another, it is possible for a single platform to display both types of behaviour. Therefore, the key test for immunity from liability under Section 230(c)(1) to apply is whether the service provider developed the underlying content.[343] As a result, subject to the few exceptions highlighted above, immunity from liability will often turn on the factual nature of the intermediary and whether they are

[336] Francis Fukuyama and Andrew Grotto, 'Comparative Media Regulation in the United States and Europe' in Nathaniel Persily and Jonathan Tucker (eds), *Social Media and Democracy: The State of the Field and Prospects for Reform* (CUP 2020) 209.
[337] 47 USC s 230(f)(2).
[338] Valerie Brannon, 'Free Speech and the Regulation of Social Media' (Congressional Research Service 2019) 10 <https://crsreports.congress.gov/product/details?prodcode=R45650> accessed 27 August 2021.
[339] 47 USC s 230 (e)(3).
[340] 47 USC s 230 (e)(1).
[341] 47 USC s 230 (e)(2).
[342] 47 USC s 230 (e)(5).
[343] Valerie Brannon (n 338) 11.

acting as a service provider or a content creator in relation to the piece of content concerned.[344]

*ii) Exceptions to Section 230 of the Communications Decency Act 1996 Protection*

346. Although many courts have followed the precedent set by the Fourth Circuit Court of Appeals under *Zeran v America Online*, where the court interpreted Section 230 as a broad liability shield for Internet service providers, there are still instances where Section 230 does not apply.[345] These cases generally fall into one of three categories: (i) if the provider or user of an interactive computer service induced or contributed to the development of the illegal content in question; (ii) if the plaintiff's claim does not arise from the defendant's publishing or content moderation decisions (Section 230 only provides protection against liability arising from the defendant's role as a publisher); and (iii) if the provider or user of an interactive computer service fails to meet Section 230(c)(2)'s 'Good Samaritan' or 'good faith' requirement.[346]

347. The 2008 case of *Fair Housing Council of San Fernando Valley v Roommates.com* was the first case to identify limits to Section 230.[347] Roommates.com matches potential roommates with one another, and to do so, required users to disclose their sex, sexual orientation, and familial status, then list their roommate preferences, including those same characteristics. Roomates.com would then automatically match users with other potential roommates based on these traits. The Fair Housing Councils of San Fernando Valley and San Diego sued Roommates.com for violating the Fair Housing Act ('FHA'), a federal law, as well as the California Fair Employment and Housing Act ('FEHA'). The FHA prohibits housing discrimination based on sex and familial status, among other traits.[348] And the FEHA prohibits housing discrimination based on sex, sexual orientation, and familial status, among other traits.[349] The Ninth Circuit Court of Appeals ruled that Section 230 did not apply because Roommates.com required users to provide information protected under anti-discrimination laws as a condition of using the website. By requiring this information,

---

[344] ibid 12.
[345] *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 328 (4th Cir. 1997).
[346] Ashley Johnson and Daniel Castro, 'The Exceptions to Section 230: How Have the Courts Interpreted Section 230?' (Information Technology and Innovation Foundation 2021) <https://itif.org/publications/2021/02/22/exceptions-section-230-how-have-courts-interpreted-section-230> accessed 30 August 2021.
[347] *Fair Hous. Council of San Fernando Valley v. Roommates.com*, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc); ibid.
[348] 42 U.S.C. s 3604(c) (1968).
[349] Cal. Gov. Code ss 12955.

Roommates.com induced the illegal content and was found liable for breaking federal and state housing law. Four years later, in *Fair Housing Council of San Fernando Valley v Roommate.com*, the Ninth Circuit ruled differently, concluding that the FHA and FEHA did not apply to roommate selection.[350] While the court later reversed its decision on the holding of the case, the initial judicial reasoning became a key example of limits on Section 230 protection.

348. The rationale of being liable when participating in the creation of illegal content was applied in the case of *FTC v Accusearch.*[351] Here, a separate court reaffirmed the reasoning in *Roommate.com* when they ruled that Accusearch could not shield itself from liability under Section 230 since it was 'responsible for the development of offensive content' when it played an active role in running a website that facilitated the sale of individuals' personal information. Even though the personal information came from third parties, Accusearch was found responsible since 'it in some way specifically encourages development of what is offensive about the content'.

349. The Fight Online Sex Trafficking Act ('FOSTA'; also known as the 'Stop Enabling Sex Traffickers Act (SESTA)', after an earlier version of the bill, or FOSTA-SESTA) addresses sex trafficking under Section 230(e)(1).[352] FOSTA aims to fight sex trafficking by reducing legal protections for online platforms, therefore removing Section 230 coverage under these circumstances.[353] FOSTA specifically states that 'Section 230 of such Act does not prohibit the enforcement against providers and users of interactive computer services of Federal and State criminal and civil law relating to sexual exploitation of children or sex trafficking, and for other purposes;' this includes conduct that 'promotes or facilitates prostitution.'[354] The rule applies retroactively to sites that violate it.

350. Section 230 does not provide protection against breach of contract. If a defendant promises to remove content and the plaintiff relies on that promise, but the defendant fails to do so ('even when the defendant has no independent legal obligation to perform the promised

[350] *Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC*, 666 F.3d 1216 (9th Cir. 2012).
[351] *FTC v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009).
[352] Text - H.R.1865 - 115th Congress (2017-2018): Allow States and Victims to Fight Online Sex Trafficking Act of 2017 2018.
[353] ibid.
[354] ibid.

act'), the plaintiff may be able to file a promissory estoppel claim.[355] In *Barnes v Yahoo!, Inc.* the plaintiff's ex-boyfriend had created fake profiles of her on a Yahoo! site, which contained nude photographs of her and solicitations for sexual intercourse.[356] The plaintiff reported the fake profiles and sent requests to Yahoo! to remove them. She received an assurance from Yahoo!'s director of Communications that the director would 'personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it.' However, the fake profiles remained. The plaintiff filed a negligence claim and a promissory estoppel claim. The Ninth Circuit found Yahoo! not liable under the negligence claim as Section 230(c)(1) precludes an Internet service provider from liability 'as the publisher or speaker of any information provided by another information content provider.' However, Yahoo! was found liable for breach of contract under the promissory estoppel claim, which treated Yahoo! as a party in a verbal contract. The court made a distinction, however, that a general monitoring policy would not be sufficient to create liability under a theory of promissory estoppel.

351. In *Doe v Internet Brands,* the plaintiff, an aspiring model, posted her information on a networking website for the modeling industry called Model Mayhem.[357] Two men posing as talent scouts - Lavont Flanders and Emerson Callum – contacted her in order to lure her to a fake audition and sexually assault her. Flanders and Callum had been running similar schemes using Model Mayhem since 2006. When Internet Brands purchased Model Mayhem in 2008, they learned of Flanders and Callum's activity shortly thereafter, but failed to warn its users of the two men's activities. The court found that 'actual knowledge by Internet Brands from an outside source of information about criminal activity' shifts the claim beyond just Internet Brands' publishing decisions. In this case, the claim did not arise from Internet Brands 'mishandling the removal of third party content' or '[failing] to adequately regulate access to user content,' but its failure to warn users of illegal activity it knew about taking place on its platform. Here, the court ruled that Section 230 protection did not apply.

352. In *Diamond Ranch Academy v Filer*, the defendant was sued for defamation for posts she uploaded onto a website about Diamond Ranch Academy.[358] The defendant argued that

[355] Johnson and Castro (n 346); Berkman Klein Center for Internet & Society, 'Online Activities Not Covered by Section 230' (*Digital Media Law Project*) <https://www.dmlp.org/legal-guide/online-activities-not-covered-section-230> accessed 30 August 2021.
[356] *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1107 (9th Cir. 2009).
[357] *Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016); Johnson and Castro (n 346).
[358] *Diamond Ranch Acad., Inc. v. Filer*, No. 2:14-CV-751-TC, 2016 U.S. Dist. LEXIS 19210 (D. Utah 17 February 2016).

under Section 230, and precedent from the *Batzel v Smith* case, she had immunity and could not be held liable for simply reposting third-party statements. In *Batzel v Smith*, the court ruled that 'the exclusion of "publisher" liability [by Section 230] necessarily precludes liability for exercising the usual prerogative of publishers to choose among proffered material and to edit the material published while retaining its basic form and message.'[359] The district court in the case of *Filer* did not accept this argument. It distinguished the defendant's posts from those found in *Batzel*, holding that Filer's posts 'do not lead a person to believe that she is quoting a third party,' and that Filer 'did more than simply post whatever information the third parties provided.' In combining her own statements with others and selectively choosing statements that reflected negatively on Diamond Ranch Academy, the defendant was found to have materially altered the content of the posts and failed to 'retain [the material's] basic form and message.'[360] This material alteration of the posts' meanings removed Section 230 protection.

353. Under Section 230(c)(2)(a) 'no provider or user of an interactive computer service shall be held liable on account of – any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.' This is notedly different from Section 230(c)(1) for two reasons: (i) Section 230(c)(1) grants protections for actions *not* taken;[361] and (ii) unlike Section 230(c)(1)'s broader protection, Section 230(c)(2) limits protection only to actions 'taken in good faith.'

354. In *E-Ventures Worldwide v Google*, E-Ventures (an online publishing and research firm that performed search engine optimization (SEO)) brought claims of unfair competition, amongst other claims, against Google when Google classified the firm's websites as 'pure spam' and removed the websites from Google's search results.[362] Google claimed their actions were shielded by Section 230. As their actions were that of actively filtering content, the applicable liability exemption would have been under Section 230(c)(2). The court ruled that Google did not qualify for protections under Section 230, stating that Section 230 exemption did not apply because Google may have acted anticompetitively, and if this was

[359] *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003).
[360] *Diamond Ranch Acad., Inc. v. Filer* (n 358) internally quoting *Batzel v. Smith* ibid.
[361] *John Doe v. GTE Corporation*, 347 F.3d 655 (2003).
[362] *e-ventures Worldwide, LLC v. Google, Inc.,* 188 F. Supp. 3d 1265 (M.D. Fla. 2016).

the case, aforementioned actions of delisting E-Ventures' websites were not taken in good faith. Google did ultimately win the case, however, when the court ruled that the 'First Amendment protects Google's actions and precludes all of e-ventures' claims.'[363]

355. *E-Ventures*' rationale was applied to *Enigma Software Group v Malwarebytes*. Enigma, a company that offers malware removal tools, sued competitor Malwarebytes, alleging anticompetitively behaviour when Malwarebytes configured its anti-malware products to block users from downloading and using Enigma's products.[364] Malwarebytes raised Section 230(c)(2) as a defense, arguing that it shielded it from liability for blocking access to certain content. the Ninth Circuit Court of Appeals disagreed and ruled that Section 230(c)(2) did not apply. Section 230(c)(2) 'does not immunize blocking and filtering decisions that are driven by anticompetitive animus.'

*iii) Copyright and the Digital Millennium Copyright Act*

356. The Digital Millennium Copyright Act (DMCA) notice and takedown process was enacted by Congress as a tool for copyright holders to have user-uploaded content which infringes their copyright to be removed from websites. Generally, the process entails the copyright owner sending a takedown notice to a service provider requesting the material infringing copyright to be removed. If all the elements that ought to be included in the takedown notice are provided, the service provider may continue to refuse to takedown material, however, they would potentially open themselves to secondary liability for assisting with copyright infringement.

357. Section 512 of the Digital Millennium Copyright Act (DMCA) provides exemptions for four categories of ISPs from monetary remedies if their acts follow the requirements listed under the Act.[365] The four categories of ISPs which receive safe harbour include: 'conduit', 'caching', 'hosting', 'online directories and hyperlinks'.[366] ISPs are provided with a wide immunity from liability if they comply with the notice-and-takedown procedures. For example, if hosting ISPs faithfully perform the removal and replacement pursuant to the

[363] *e-ventures Worldwide, LLC v. Google, Inc.,* No. 214CV646FTMPAMCM, 2017 WL 2210029 (M.D. Fla. 8 February 2017)
[364] *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.,* 946 F.3d 1040 (9th Cir. 2019), cert. denied, 141 S. Ct. 13, 208 L. Ed. 2d 197 (2020).
[365] 17 USC s 512.
[366] 17 USC s 512(b)(1).

procedures established, they are not responsible for any mistaken removal and replacement.[367]

**b) Can the government order that content be removed, and if so in what circumstances, and what types of content?**

358. The federal government of the USA faces the twin hurdles of the First Amendment and Section 230 in their attempts to have content removed from online platforms. Any attempts to introduce federal law that regulates internet content decisions would likely qualify as state action sufficient to implicate the First Amendment.[368] In addition, due to the dual provisions of section 230(c)(1) and (2), to the extent that private litigants or state governments would wish to hold social media intermediaries liable under existing laws regarding presenting third-party content or restricting access to content, those suits have largely been barred.

359. A fundamental principle of First Amendment jurisprudence is the "content discrimination" principle. As Justice Marshall expressed in *Police Department of the City of Chicago v Mosley*, 'the First Amendment above all else means that the government may not restrict expression because of its message, ideas, subject matter or content.'[369] A content-based restriction, as opposed to a content-neutral restriction, is a key differentiation under First Amendment jurisprudence because content-based restrictions are subject to 'strict scrutiny' analysis.[370] Strict scrutiny requires government to show that it has a compelling governmental interest for its regulation and that the regulation is the least speech-restrictive way to further its interests.

360. For example, in *Reno v ACLU*, two statutory provisions which were enacted to protect minors from 'indecent' and 'patently offensive' communications on the Internet did not survive strict scrutiny under the First Amendment.[371] As the Court explained, the 'general, undefined terms 'indecent' and 'patently offensive' cover large amounts of nonpornographic material with serious educational or other values.'[372] Therefore, in practice, because of

[367] Jie Wang, *Regulating Hosting ISP's Responsibilities for Copyright Infringement: The Freedom to Operate in the US, EU and China* (Springer 2018) 146.
[368] Brannon (n 338).
[369] *Police Department of the City of Chicago v Mosley* 408 US 92 (1972) 95.
[370] David Hudson, *Legal Almanac: The First Amendment: Freedom of Speech,* (Aspatore Books 2012) s 2:2.
[371] *Reno v American Civil Liberties Union* 521 US 844 (1997).
[372] ibid 877.

Section 230 and the First Amendment, there are few, if any, federal or state laws that expressly govern social media intermediaries' decisions about whether and how content can be presented or removed.[373]

361. Consequently, users' ability to post speech on social media platforms and governments' ability to order for content to be removed is primarily secured through self-regulation by virtue of moderation policies, terms and conditions created and enforced by the intermediaries. Inevitably, relying on self-regulation from social media intermediaries creates the consequence of not only the removal of illegal speech, but also the possibility of the removing otherwise legal speech.

362. In the intellectual property and copyright context, the US government is involved in substantial enforcement efforts directed at online intermediaries.[374] For example, in January 2012, the FBI seized and closed Megaupload, an online intermediary that was alleged to be facilitating massive copyright infringement. The owners of Megaupload were subsequently criminally indicted. In addition, if suspected of copyright infringement, the US Government is also capable of conducting domain name seizures.[375]

**c) What is the nature of the content that a court can order to be taken down from a social media intermediary?**

363. Another fundamental principle of First Amendment jurisprudence which is applicable to social media intermediaries and Online News Media is the separation between protected and unprotected speech. Under the unprotected speech approach, once the Court determines that a category of speech has little to no value, it can be banned entirely.[376] It is important to note, however, that the most recent decisions of the Supreme Court have reflected a reluctance to add any new categories of excepted speech and to interpret narrowly the current exemptions in place for unprotected speech.[377] As the categories of unprotected speech are equally applicable to the regulation of Online News Media, the full categories and applicable tests/standards will be fully detailed in that section. Nevertheless, once a category

[373] Brannon (n 338).
[374] Jack Lerner, 'Secondary Copyright Infringement Liability and User-Generated Content in the United States' in Frosio (ed) (n 28) 362.
[375] ibid 363.
[376] David Hudson, *Legal Almanac: The First Amendment: Freedom of Speech* (Aspatore Books 2012) s 3.1.
[377] For example, see *US v. Stevens*, 559 US 460 (2010).

of speech is considered by the Court as unprotected under the First Amendment, it may be prohibited entirely.[378]

*i) Intellectual Property*

364. As detailed above, one of the exceptions to Section 230 of the CDA is intellectual property law. In copyright law, the Digital Millennium Copyright Act provides the notice and takedown procedure for alleged copyright infringement to be removed from service providers. Similarly, trademark infringements are also an area of intellectual property law that is governed by the courts.[379] Although the DMCA does not apply to trademark infringement, similar principles based on contributory and vicarious liability are applied in the United States.[380]

365. In *Tiffany v eBay*, Tiffany brought an action against eBay after counterfeit pieces of Tiffany jewellery had been sold on eBay. The Southern District of New York, affirmed by the Second Circuit, held that eBay was neither directly nor indirectly liable for third parties' sales on its website. eBay was not directly liable for trademark infringement because the use of Tiffany's trademark 'describe[d] accurately the genuine Tiffany goods offered for sale on its website. And none of eBay's uses of the mark suggested that Tiffany affiliated itself with eBay or endorsed the sale of its products.'[381] was a protected, nominative fair use of the trademark. In regard to contributory liability, the Second Circuit stated that eBay was not contributorily liable for trademark infringement because Tiffany failed to demonstrate that eBay was 'supplying its services to individuals who it knew or had reason to know were selling counterfeit Tiffany goods.'[382]

366. It is important to note that legal recourse and litigation is not the only method for the removal of content, many social media intermediaries have their own policies and procedures governing intellectual property infringement.

---

[378] Kathleen Ruane, 'Freedom of Speech and the Press: Exceptions to the First Amendment' (Congressional Research Service 2014) 1 <https://sgp.fas.org/crs/misc/95-815.pdf> accessed 25 August 2021.
[379] The governing trademark law statute under federal law is provided in the Lanham Trademark Act of 1946.
[380] Beatrice Martinet and Reinhard Oertli, 'Liability of E-Commerce Platforms for Copyright and Trademark infringement: A World Tour' (American Bar Association 2015) <https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2014-15/may-june/liability-e-commerce-platforms-copyright-trademark-infringement-world-tour/> accessed 31 August 2021.
[381] *Tiffany (NJ) Inc v eBay Inc* 600 F 3d 93, 103 (Court of Appeals, 2nd Circuit 2010).
[382] ibid 109.

**d) What are the conditions in which intermediaries may be compelled to 'unmask' anonymous speakers and identify originators of content?**

367. The US Supreme Court has long protected anonymous speech and expression on the basis that it furthers the First Amendment's goal.[383] Lower courts have also applied First Amendment rights to protect anonymous online speech. For example, the Supreme Court of Pennsylvania held that 'court-ordered disclosure of Appellants' identities represents a significant possibility of trespass upon their First Amendment rights.'[384] A federal district court in California held, in 1999, that citizens had 'a legitimate and valuable right to participate in online forums anonymously or pseudonymously.'[385] However, as the right to free speech is not absolute, there are certain situations in which intermediaries may be required to 'unmask' anonymous speakers and content-creators.

368. Due to Section 230 of the CDA, the ISP is not liable for the third-party content online. As a result, claimants can only challenge content on a website directly against the person who posted the objectionable content on the website.

*i) Copyright*

369. Section 512 (h) of the DMCA provides that 'copyright owners or a person authorised to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer.'[386]

a) The request must include: (a) a copy of the relevant notification; (b) a proposed subpoena; and (c) a sworn declaration.
b) The subpoena authorises and orders the service provider receiving the notification to 'expeditiously disclose to the copyright owner or person authorised by the copyright owner information sufficient to identify the alleged infringer of the material described.'[387]

[383] Sophia Qasir, 'Anonymity in Cyberspace: Judicial and Legislative Regulations' (2013) 81 Fordham Law Review 3651, 3664.
[384] *Melvin v. Doe*, 836 A.2d 42, 49, 50 (Pa. 2003).
[385] *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999).
[386] 17 USC s 512(h)(1).
[387] 17 USC s 512(h)(3).

370. In the US, the subpoena under DMCA 512 (h) can only be issued to ISPs who run caching, hosting, or information location tools. Access providers are immune from such subpoenas.[388]

*ii) John Doe subpoena*

371. John Doe subpoenas provide a general procedural tool for the identity of "anonymous" posters to be identified. John Doe subpoenas allow plaintiffs to discover the identity of anonymous online speakers from their ISP or websites they have visited. John Doe subpoenas are a general tool that is applicable in any situation where an anonymous speaker needs to be unmasked, for example, defamation, harassment, or copyright. Generally, the subpoena operates by filing two separate applications. First, the plaintiff must subpoena the website for the IP address of the user who made the online comments. Second, the plaintiff must subpoena the Internet Service Provider that provides its customers their IP address.

372. Despite the procedural and legal importance of the John Doe subpoena, there is no single standard in the USA that governs its application.[389] In *Columbia Insurance Co. v Seescandy*, the California District Court adopted a motion-to-dismiss standard.[390] *In re AOL*, a suit filed in Virginia state court, the plaintiff only needed a "good faith basis" for his claim, significantly lower than the motion-to-dismiss standard.[391] Nevertheless, case law has begun to coalesce among the importance of two key factors: (a) ensuring the defendant has notice and opportunity to respond to the subpoena before his identity is exposed and (b) the strength of the plaintiff's underlying claim.[392]

373. In the context of copyright, Joe Doe subpoenas operate as an alternative path to the subpoena provided within section 512 of the DMCA. Nevertheless, in determining whether to grant a John Doe subpoena, a court will consider the following factors: (1) the claim of copyright infringement, (2) the possibility the identity information may be destroyed, (3) the disclosure request must be narrowly tailored, (4) the subpoena must substantially contribute

[388] Jie Wang, *Regulating Hosting ISP's Responsibilities for Copyright Infringement: The Freedom to Operate in the US, EU and China* (Springer 2018) 146, 181.
[389] Nathaniel Gleicher, 'John Doe Subpoenas: Toward a Consistent Legal Standard' (2008) 118 Yale Law Journal 320, 325.
[390] *Columbia Insurance Co. v Seescandy.com* 185 FRD 573 (N.D. Cal 1999), 579.
[391] *In re Subpoena Duces Tecum to America Online Inc.* 52 Va. Cir. 26 (Cir. Ct. 2000).
[392] Nathaniel Gleicher, 'John Doe Subpoenas: Toward a Consistent Legal Standard' (2008) 118 Yale Law Journal 320, 343.

to the case; (5) whether the defendant could be identified without the subpoena.[393] Internet users are contacted before the disclosure of their identity, so they can file a motion to squash or modify the subpoenas.[394]

## B. SECTION 2: ONLINE NEWS MEDIA

374. Currently, online news media is not a discrete and separate category for regulation in the USA. As stated above, the Supreme Court has held that traditional First Amendments rights continue to apply online. *In re Anonymous Online Speakers,* the Ninth Circuit held that online speech "stands on the same footing as other speech – there is no basis for qualifying the level of First Amendment scrutiny that should be applied to online speech.'[395] As such, the First Amendment to the United States Constitution forms the backbone of regulatory oversight concerning freedom of the press and its application to the internet, and by extension, online news media. In addition, in some instances, online news media are also able to take advantage of the safe harbour provisions established under section 230 of the CDA.

### a) In what circumstances, if any, may a government authority order that an online news item must be removed from any website?

*i) First Amendment and Content Removal*

375. As a result of landmark decisions from the US Supreme Court, the circumstances for government intervention in free speech and the freedom of the press is severely limited, albeit not absolute. As acknowledged above, content-based regulation is presumed unconstitutional and is subject to strict scrutiny analysis. Moreover, only a few limited categories of speech are deemed "unprotected" by the First Amendment and can be banned entirely.

376. The first landmark decision invoking the press clause of the First Amendment was *Near v Minnesota. Near* established a fundamental constitutional principle that once the press has obtained information that it deems newsworthy, the government can 'seldom, if ever,

[393] Jie Wang, *Regulating Hosting ISP's Responsibilities for Copyright Infringement: The Freedom to Operate in the US, EU and China* (Springer 2018) 146, 181.
[394] ibid.
[395] *In re Anonymous Online Speakers* 661 F.3d 1168, 1173 - Court of Appeals, 9th Circuit (2010).

prevent that information from being published.'[396] *Near* was the first case to recognize that the First Amendment generally prohibits prior restraints by government to prevent speech or publication from occurring. A prior restraint being a government order – from a court, government official, or a legislative body – which prohibits expression before it occurs.[397] In *New York Times Co. v United States*, or the 'Pentagon Papers case', the Court reiterated that 'any system of prior restraints of expression…[bears] a heavy presumption against its constitutional validity.'[398]

377. The foundation of First Amendment case law was further expanded in *New York Times Co. v Sullivan*. In *Sullivan*, Justice Brennan stated that the 'erroneous statement is inevitable in free debate, and…it must be protected if the freedoms of expression are to have the 'breathing space' that they need to survive.'[399] The United States is founded on the 'profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials.'[400]

378. There are, however, several caveats to address that may apply in the context of online news media. As illustrated above, the free press clause of the First Amendment would have traditionally protected the media institutions that would encompass 'online news media'. However, the First Amendment and US jurisprudence makes no clear demarcation on what constitutes the 'press'. In 1789, the 'press' referred to the printing press.[401] As technology evolved, the Press Clause would protect all products of the printing press, including books and newspapers. The Press Clause has always protected the technology, rather than a group of favoured speakers in the form of organised media.[402] The rise of the Internet has effectively severed the distinction between 'speech' and 'the press' as it provides for the technology that was previously only available to a select few.

[396] *Near v State of Minnesota* 51 S Ct 625 (1935).
[397] Stephen J Wermiel, 'Freedom of the Press: Challenges to this Pillar of Democracy' (*American Bar Association,* 26 March 2019*)* <https://www.americanbar.org/groups/public_education/publications/insights-on-law-and-society/volume-19/insights-vol-19-issue-2/freedom-of-the-press/> accessed 29 September 2021.
[398] *New York Times Co. v United States* 403 US 713, 723 (1971).
[399] *New York Times Co. v Sullivan* 376 US 254, 271-272 (1964).
[400] ibid 270.
[401] Ashutosh Bhagwat, *Our Democratic First Amendment* (CUP 2020) 25.
[402] ibid.

379. As a result, First Amendment jurisprudence does not place heavy emphasis on whether an institution ought to be recognised as 'online news media'. For instance, news that are authored by bloggers also receive protection from the First Amendment. In *Obsidian Finance Group v Crystal Cox*, the Ninth Circuit stated that 'the protections of the First Amendment do not turn on whether the defendant was a trained journalist, formally affiliated with traditional news entities…a First Amendment distinction between the institutional press and other speakers is unworkable.'[403]

380. Second, courts have also taken into considerations of the nature of the medium and asked whether there are special characteristics that may justify greater regulation. For example, radio and television broadcasters are held to a stricter standard of regulation. This was justified on the basis of a public right to "suitable access" to ideas and a scarce radio and television spectrum for broadcasters.[404] However, in *Reno v ACLU*, the Supreme Court noted that factors which previously justified greater regulation of the media did not apply to the Internet.[405] The Court rejected the government's argument that regulation was permissible because the internet was analogous to broadcast media, a forum in which the Court has permitted greater regulation of speech. Unlike the broadcast industry, the Internet is not considered as 'invasive' as radio or television.[406]

*ii) Section 230 and Online News Media*

381. The application of Section 230 of the CDA is also capable of immunising certain activities of online news media from liability. In *Miles v Raycom Media*, the claimant alleged that the news website did not filter alleged defamatory third-party comments published on its website.[407] The Court, however, rejected this argument stating that 'an interactive computer service is entitled to immunity as long as it did not create or author the particular information at issue.'[408] As a result, the defendant news media was immune from the allegedly defamatory third-party comments that accompanied the article. In *Collins v Purdue University*, an article published by the Federated Publications, both on and offline, inferred that Mr. Collins was involved in another students' disappearance, attracting 'vitriolic and hateful' comments.[409]

---

[403] *Obsidian Finance Group LLC v Cox* 740 F3d 1284, 1291 - Court of Appeals, 9th Circuit (2014).
[404] *Red Lion Broadcasting Co. v. Federal Communications Commission* 395 US 367, 390 (1969).
[405] *Reno v American Civil Liberties Union* 521 US 844 (1997) 854.
[406] ibid 869.
[407] *Miles v RAYCOM Media Inc.* District Court, SD Mississippi (2010).
[408] ibid.
[409] *Collins v Purdue University* 703 F Supp 2d 862, 868 – District Court, ND Indiana (2010).

The court rejected Collins' claim, Federated publications could only be held liable for defamation 'in its own material published on the website.'[410] Moreover, as Federated did not create, develop, encourage, or apply any editorial function to the comments, it was immune from liability for the third-party content posted on its website by the CDA.[411] Once again, the key question lies in the factual determination of whether the intermediary created the actionable content.

382. Even with the rise of the Internet, *Sullivan's* core principles remain a central part of the US media regulation landscape.[412] Moreover, Section 230 of the CDA continues to treaty the internet as a different regulatory medium by '[privileging] online publishers over offline publishers by giving online publishers more favourable legal protection.'[413] As a result, the regulatory landscape in the United States surrounding freedom of the press and freedom of speech is notably against government intrusion, with limited general justifications that permit restrictions on speech.

*iii) Protected and Unprotected Speech*

383. The Court has accomplished this by separating and creating categories of unprotected speech. Some types of speech are categorically unprotected, the protection status of others vary by receiving less than full protection according to the medium and whether they are targeted or consumed by children. Examples of content that fall under the category of unprotected speech include words or actions meant to incite violence or that influence others to commit acts of violence, defamation, child pornography and content harmful to minors, the creation or distribution of obscene materials, speech integral to criminal conduct, fighting words, and true threats.[414]

384. Therefore, in general, content-based removals of speech are presumptively unconstitutional and will be subject to strict scrutiny. Moreover, the US Supreme Court has explicitly rejected a 'free-floating test for First Amendment coverage…that [involve] ad hoc balancing of

[410] ibid 879.
[411] ibid.
[412] The Editorial Board, 'The Uninhibited Press, 50 Years Later' (*New York Times,* 8 March 2014) <https://web.archive.org/web/20210110031037/https://www.nytimes.com/2014/03/09/opinion/sunday/the-uninhibited-press-50-years-later.html> accessed 25 August 2021.
[413] Eric Goldman 'An Overview of the United States' Section 230 Internet Immunity' in Frosio (ed) (n 28) 162.
[414] *United States v Alvarez* 132 S Ct 2537, 2544 (2012).

relative social costs and benefits.'[415] As a result, the categories of unprotected speech that the government may regulate and have banned because of their content is limited.

**b) What are the tests or standards for determining whether an online news article/page needs to be removed?**

385. There are very few categories of unprotected speech that the government may regulate, based on which it may ask for content to be taken down from an online news media platform.

*i) Defamation*

386. In order to sustain a defamation claim, the US courts have adopted different standards depending on whether the claimant is a private or public figure.[416] As provided by the Supreme Court in *Sullivan,* for public officials and public figures to recover damages for false statements, 'actual malice' must be proved. The 'actual malice' test places the burden on the public figure to prove that the news media acted either in recklessness or deliberate falsehood.[417] A private figure may not recover damages for defamation without showing some type of fault, although not necessarily of actual malice.[418] However, if a defamatory statement involves a matter of public concern, even a public figure is required to show actual malice in order to recover damages.[419]

*ii) Obscenity*

387. In order for material to be obscene and unprotected under the First Amendment, it must fulfil the three part test established in *Miller v California*: '(a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.'[420]

[415] *United States v. Stevens* 130 SCt 1577, 1585 (2010).
[416] Ruane (n 378) 21.
[417] ibid.
[418] ibid.
[419] ibid.
[420] *Miller v California* 413 US 15, 24 (1973).

*iii) Incitement*

388. In *Brandenburg v Ohio*, the Supreme Court held that the First Amendment protects advocating the use of force or lawbreaking 'except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.'[421]

*iv) Fighting words*

389. In *Chaplinsky v New Hampshire,* the Supreme Court held that the First Amendment does not protect 'fighting words' which is defined as those 'likely to provoke the average person to retaliation, and thereby cause a breach of the peace.'[422]

*v) True threats*

390. In *Virginia v Black*, 'true threats' was defined as encompassing those statements 'where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals. The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats protect[s] individuals from the fear of violence and from the disruption that fear engenders, in addition to protecting people from the possibility that the threatened violence will occur.'[423]

*vi) Speech integral to criminal conduct*

391. The First Amendment affords no protection to speech 'used as an integral part of conduct in violation of a valid criminal statute.'[424]

*vii) Child pornography and speech harmful to minors*

392. As noted by the Supreme Court in *New York v Ferber*, child pornography is unprotected by the First Amendment if the materials 'visually depict sexual conduct by children below a specified age,' and the 'category of 'sexual conduct' proscribed must also be suitably limited and described.'[425] Child pornography is an unprotected category of speech for all persons. However, another category of materials which is unprotected as to minors is known as the 'harmful to minors' exception.[426] Generally, statutes with harmful-to-minor laws will based

[421] *Brandenburg v Ohio* 395 US 444, 447-448 (1969).
[422] *Chaplinsky v New Hampshire* 315 US 568, 574 (1942).
[423] *Virginia v Black et al* 538 US 343, 359-360 (2003).
[424] *Giboney v Empire Storage & Ice Co.,* 336 US 490, 498 (1949).
[425] *New York v. Ferber* 458 US 747, 764 (1982).
[426] Hudson (n 376) s 4:4.

themselves upon the obscenity test set out in *Miller*, but add on each prong the phrases 'as to minors.'[427]

*viii) Intellectual Property*

393. Although system of prior restraint is presumed unconstitutional, it is generally permitted, even in the form of a preliminary injunction, in intellectual property cases, such as copyright or trademark.[428]

**c) Is the order of a court/tribunal a prerequisite for removal of online content?**

394. As there is currently no direct government regulation in the United States of online news media, there is no specific order from a court or tribunal that is a prerequisite for the removal of online content. The nature of exemptions created under the First Amendment are, however, overseen and developed by the judiciary. Under the general categorization method, it is up to the courts to determine whether expression falls into one of a select number of unprotected categories.[429]

395. In step with the regulatory regime prevalent in the USA, unpublishing requests and removal of online news content is an area of self-regulation decided by the news agency or individual that published the article. However, in the USA, the culture amongst journalists on unpublishing requests are that they are 'rarely considered acceptable in newsrooms.'[430]

## C. SECTION 3: OTT PLATFORMS

396. Currently, over-the-top on-demand video streaming platforms ('OTT' platforms) are not directly regulated by United States federal laws or government authorities; however, should they be, they would most likely fall under the authority of the Federal Communications Commission ('FCC') and the U.S. Communications Act of 1934, as amended (the 'Act').[431]

---

[427] ibid.
[428] Ruane (n 378) 7.
[429] Hudson (n 376) s 3.1.
[430] Hye Soo Nah and Stephanie Craft, 'Unpublishing the News: An analysis of US and South Korean Journalists' Discourse About an Emerging Practice' (2019) 13 International Journal of Communication 2575, 2580.
[431] Notice of Proposed Rulemaking: Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services 2015 (FCC 14-210); Michael O'Rielly, 'FCC Regulatory Free Arena' (*Federal Communications Commission*, 1 June 2018) <https://www.fcc.gov/news-events/blog/2018/06/01/fcc-regulatory-free-arena> accessed 25 August 2021; Hughes Hubbard & Reed, 'U.S. Television on the Internet and the New "MVPDs"

While there is no specific regulatory law governing OTT platforms, they are still subject to U.S. copyright laws and specific applicable rules by the FCC.[432]

397. As OTT platforms are unregulated in the United States, aside from U.S. copyright laws, there is no U.S. governmental entity that issues takedowns or modification of content. OTT platforms regulate themselves, and some have taken steps to increase transparency.

**a) How is the content hosted by over-the-top on-demand video streaming platforms (OTT platforms) regulated?**

*i) OTT Platforms exist in an FCC Regulatory Free Area*

398. Currently, OTT platforms are not directly regulated by United States federal laws or government authorities; however, should they be, they would most likely fall under the authority of the Federal Communications Commission ('FCC') and the U.S. Communications Act of 1934, as amended (the 'Act').[433] This lack of regulation is due, in part, to debate on how to define – and therefore regulate – OTT platform content in relation to the current regulatory framework. Traditionally, the FCC has created rules for content based on the method of their physical transmission (e.g. broadcast television, cable, and direct-to-home satellite), with each method of transmission subject to a different set of rules.[434] The FCC further classifies cable, satellite and similar providers as 'multichannel video programming distributors' ('MVPDs') and subjects them to additional rules.[435] OTT platforms, on the other hand, transmit video programming over the internet over which there is no physical (i.e. tangible) transmission method.

399. Generally, the FCC makes rules through a 'notice and comment' procedure by which the FCC 'gives the public notice that it is considering adopting or modifying rules on a particular

(UPDATED)' (*Hughes Hubbard & Reed*, 23 August 2021) <https://www.hugheshubbard.com/news/u-s-television-on-the-internet-and-the-new-mvpds-updated> accessed 24 August 2021.

[432] Hughes et al, ibid; Federal Communications Commission, 'Closed Captioning of Internet Video Programming' (*Federal Communications Commission*, 5 June 2012) <https://www.fcc.gov/consumers/guides/captioning-internet-video-programming> accessed 25 August 2021; Harris Wiltshire Grannis LLP-Kent D Bressie et al, 'In Brief: Media Law and Regulation in USA' (*Lexology*, 5 August 2020) <https://www.lexology.com/library/detail.aspx?g=9b11e378-0934-4444-99ad-5a864191f899> accessed 24 August 2021.

[433] Notice of Proposed Rulemaking: Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services 2015 (FCC 14-210); Michael O'Rielly, 'FCC Regulatory Free Arena' (*Federal Communications Commission*, 1 June 2018) <https://www.fcc.gov/news-events/blog/2018/06/01/fcc-regulatory-free-arena> accessed 25 August 2021.

[434] Harris Wiltshire Grannis LLP-Kent D Bressie et al (n 432).

[435] ibid.

subject and seeks the public's comment.'[436] The FCC then considers the comments when developing final rules. On December 19, 2014, the FCC utilized this procedure when it issued a Notice of Proposed Rulemaking entitled 'Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services.'[437] This new rule proposed that the definition of the term MVPD under the Act be updated to include OTT platforms. In doing so, the OTT platforms would, amongst other things, have the rights and responsibilities of MVPDs and fall under current U.S. regulations.

400. However, there are four main prongs under the current MVPD framework that precludes the inclusion of OTT platforms. Firstly, the current definition of MVPD is incompatible with OTT platforms. Under the Act, MVPDs are entities that 'make available for purchase, by subscribers or customers, multiple channels of video programming.'[438] What was to be considered 'video programming' was previously settled when the FCC held that 'video distributed over the Internet qualifies as "video programming" given its quality is comparable to programming provided by TV broadcast stations.'[439] What remained was determining how to interpret the phrase 'multiple channels of video programming.' The use of the word 'channels' in this phrase precludes OTT platforms because the term used within the definition of an MVPD includes the use of a 'physical "transmission path,"' stated differently, 'the term MVPD includes entities that control at least some portion of the physical means by which the programming is delivered – for example, via a physical cable that the provider owns or via spectrum that the provider is licensed to use,' elements of which current OTT platforms like Netflix or YouTube do not have.[440]

401. Secondly, within the Notice the FCC proposed MVPD to 'mean distributors of multiple linear video programming streams.'[441] However, while this proposed definition would encompass entities who provide such content, regardless of if they control the transmission path of said content, the distributors of this 'linear' or prescheduled streams of video programming do not include distributors of non-linear programming like video-on-

[436] Federal Communications Commission, 'What We Do' (*Federal Communications Commission*, 22 November 2010) <https://www.fcc.gov/about-fcc/what-we-do> accessed 24 August 2021.
[437] Federal Communications Commission, 'Notice of Proposed Rulemaking: Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services' (15 January 2015).
[438] 47 U.S.C. § 522 - Definitions s 522(13).
[439] Hughes et al (n 431).
[440] ibid; Notice of Proposed Rulemaking: Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services n 81.; *In the Matter of Sky Angel U.S.*, LLC, 25 F.C.C. Rcd. 3879, 3883 (2010).
[441] Federal Communications Commission, 'Notice of Proposed Rulemaking: Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services' (15 January 2015) para 6.

demand.[442] Failure to include non-linear programming excludes on-demand services like Amazon Prime Instant Video, Hulu Plus, and Netflix, in their current forms.[443]

402. Thirdly, should purely on-demand OTT platforms choose 'to incorporate 24-hour-a-day, continuous pre-programmed linear streams of video'[444] to comply with this proposed regulation, they would still need to (i) fulfil the requirement of providing third party content, and (ii) provide 'a service similar to or competitive with traditional MVPDs.' [445] Questions also remain on what fulfils the minimum requirement of 'multiple channels.' Would twenty channels suffice? Or would the minimum amount of 'multiple' be determined by a certain number of programming hours? And what of hybrid OTT providers that distribute both multiple channels of linear and on-demand programming? While the FCC has not taken a position on these questions, some have posited that since current MVPDs provide both linear and non-linear programming, should OTT distributors qualify as MVPDs, then offering on-demand content along with linear programming 'may not materially prejudice its MVPD status.'[446]

403. Fourthly, the term MVPD requires that the entity makes multiple channels of video programming 'available for purchase.'[447] The FCC asks for comments on what it means to make such content for purchase, but 'tentatively conclude that the term means making an offer to consumers to exchange video service for money.'[448] The Notice goes on to seek comments on the question of 'if a cable or satellite company offers its subscribers access to supplemental online linear video services without a separate charge, but as part of their paid television packages, does this offering constitute making the online services "available for purchase"?' [449]

---

[442] United States Code, 2006 Edition, Supplement 5, Title 47 - TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS s 522(12).
[443] Hughes et al (n 431).
[444] ibid.
[445] ibid; Federal Communications Commission, 'Notice of Proposed Rulemaking: Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services' (15 January 2015) para 25.
[446] Hughes et al (n 431).
[447] United States Code, 2006 Edition, Supplement 5, Title 47 - TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS s 522(12, s 522(13).
[448] Federal Communications Commission, 'Notice of Proposed Rulemaking: Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services' (15 January 2015) para 27.
[449] ibid 15.

404. Since the Notice was issued in 2014, the FCC has not voted on the matter, and there currently exists no regulation of OTT content by the FCC.[450] Nevertheless, the ever increasing presence of OTT platforms has prompted the FCC to issue some standalone rules like requiring 'captioned programs shown on TV to be captioned when re-shown on the Internet.'[451] Moreover, while OTT platforms in the United States may be regulatory free, U.S. copyright laws still apply.

*ii) OTT Platforms Interplay with Copyright and Advertising Law*

405. OTT platforms are subject to U.S. copyright laws. One major example being the U.S. Supreme Court case *American Broadcasting Companies, Inc. v Aereo, Inc.*, 134 S.Ct. 2498 (2014). For a monthly fee, Aereo offered subscribers free, over-the-air broadcast television programming over the Internet. Additionally, much of this programming included copyrighted works that Aereo did not own nor have a license to transmit. The Court determined that Aereo (and therefore other similar entities) could not transmit such programming without receiving copyright authorization. Subsequent decisions 'clarified that such entities cannot employ the statutory copyright license reserved for cable systems.'[452]

406. This is not to say that if OTT platforms that provided multiple streams of linear programming were classified as MVPDs they would automatically obtain retransmission rights to television broadcast linear programming. Rather, these OTT platforms would still need to qualify for the compulsory copyright licensing scheme under the Copyright Act, specifically, under Section 111 of the Copyright Act which 'provides "cable systems" (as defined by the Copyright Act) a statutory license to retransmit copyrighted broadcast performances if the "cable system" pays a statutory fee for those performances.'[453]

407. There is a myriad of restrictions placed on broadcast television, cable, and satellite providers when airing advertisements. The Federal Trade Commission (amongst other entities)

---

[450] Michael Balderston, 'TV Affiliates Want FCC to Reexamine OTT Regulation' (*TVTechnology*, 22 June 2020) <https://www.tvtechnology.com/news/tv-networks-want-fcc-to-reexamine-ott-regulation> accessed 25 August 2021; Michael O'Rielly, 'FCC Regulatory Free Arena' (*Federal Communications Commission*, 1 June 2018) <https://www.fcc.gov/news-events/blog/2018/06/01/fcc-regulatory-free-arena> accessed 25 August 2021

[451] Federal Communications Commission, 'Closed Captioning of Internet Video Programming' (*Federal Communications Commission*, 5 June 2012) <https://www.fcc.gov/consumers/guides/captioning-internet-video-programming> accessed 25 August 2021.

[452] Harris Wiltshire Grannis LLP-Kent D Bressie et al (n 432).

[453] 17 U.S. Code § 111 - Limitations on Exclusive Rights: Secondary Transmissions of Broadcast Programming by Cable' (*LII / Legal Information Institute*) pt (f)(3) <https://www.law.cornell.edu/uscode/text/17/111> accessed 26 August 2021.

prohibits all providers from engaging in false and misleading advertising, regardless of the form of transmission used.[454] Advertisements dealing with regulated topics may also be subject to additional requirements regardless of whether the ads appear on television, online, or elsewhere. Examples include (i) under the Federal Election Commission (and some state law), advertisements by political candidates must include certain mandatory disclosures; (ii) advertisements for pharmaceuticals must fulfill Food and Drug Administration requirements related to drug advertising; (iii) broadcast television, cable, and satellite providers must adhere to FCC restrictions on advertising in children's programming and advertising of tobacco products; and (iv) under the CALM Act adopted by the FCC, commercial advertisements are prohibited from being louder than the programming that surrounds them.[455] These restriction do not currently apply to streaming online video/OTT platforms.[456]

*iii) Benefits and Obligations of MVPD status for OTTs*

408. Should the FCC ever align the concept of OTT platforms under the MVPD framework, OTT platforms would gain the regulatory privileges of MVPD status as well as their legal obligations under the Act and FCC rules.[457] Benefits of MVPD status include the right to seek relief under the program access rules (47 U.S.C. § 548) and the retransmission consent rules.[458] Section 47 U.S.C. § 548 of the Act aims to minimize anticompetitive behavior between cable operators and satellite programming distributors against MVPDs. Amongst other provisions, MVPDs are provided protections such as (i) safeguards against cable operators stifling cooperation between satellite broadcast and cable programming distributors and MVPDs, (ii) prohibitions on discrimination by satellite programming vendors against MVPDs via prices, terms, and conditions of sale or delivery, and (iii) prohibitions on exclusive contracts between cable operators and satellite programming that keeps MVPDs from obtaining programs from said satellite distributors in which the cable operators hold an attributable interest for distribution.

409. Under retransmission consent rules found under Section 47 U.S.C. § 325(b)(3)(C)(ii) of the Act and Section 47 C.F.R. § 76.65 of the Code of Federal Regulations, broadcasters are required to negotiate in good faith with MVPDs for retransmission consent, with the rules

[454] Harris Wiltshire Grannis LLP-Kent D Bressie et al (n 481).
[455] ibid.
[456] ibid.
[457] Notice of Proposed Rulemaking (n 104) para 36.
[458] ibid.

prohibiting broadcasters from negotiating exclusive retransmission consent agreements with any MVPD. If an MVPD believes that a broadcaster has violated these provisions, they can file a complaint with the FCC in accordance with 47 C.F.R. § 76.65(c).

410. Regulatory and statutory obligations of MVPDs include those relating to (i) program carriage; (ii) the competitive availability of navigation devices (including the integration ban); (iii) good faith negotiation with broadcasters for retransmission consent; (iv) Equal Employment Opportunity ('EEO'); (v) closed captioning; (vi) video description; (vii) access to emergency information; (vi) signal leakage; (vii) inside wiring; and (viii) the loudness of commercials.[459] Furthermore, 'to the extent that an Internet-based distributor of video programming falls within the definition of an MVPD, it will be able to take advantage of the privileges of MVPD status but will also be subject to MVPD obligations, unless the [FCC] waives some or all of them if authorized to do so.'[460]

**b) In what circumstances, if any, may a government authority order that content hosted by an OTT platform must be modified, or removed from any website?**

411. As there is currently no government regulation in the United States of OTT platforms, there is no specific government entity that orders content modifications or takedowns by OTT platforms. Infringements of U.S. copyright laws aside, OTT platforms are largely self-regulated in the United States, and determine for themselves which content to maintain, modify, or remove from their platforms.

412. To increase transparency, and acknowledgement of their global audience, some OTT platforms like Netflix have published transparency disclosures like those published by other internet companies.[461] Within their 2019 Environmental and Social Governance report, Netflix listed all the content it removed because of written government takedown demands since they began streaming in 2007. As of February 2020, nine titles have been removed after written takedown demands from various government entities, none of which were

[459] ibid.
[460] ibid, para 37.
[461] Netflix, 'Environmental Social Governance: 2019 Sustainability Accounting Standards Board (SASB) Report' (2019) <https://s22.q4cdn.com/959853165/files/doc_downloads/2020/02/0220_Netflix_EnvironmentalSocialGovernanceReport_FINAL.pdf> accessed 27 August 2021.

from the United States.[462] Demands to remove these nine titles came from five countries: New Zealand, Vietnam, Germany, Singapore, and Saudi Arabia.[463] The report notes Netflix's compliance with these foreign governmental demands, their response being to remove the applicable titles from viewing only from the respective country whose governmental entity submitted the written takedown demand. For example, in 2015, Netflix removed content after a written demand from the New Zealand Film and Video Labeling Body. They removed that content from its service only in New Zealand.[464]

[462] ibid 7.
[463] ibid.
[464] ibid.