Wrongful moderation: regulation of internet intermediary service provider liability and freedom of expression

Klos, M.

Part 1: A Conceptualisation of Internet Intermediary Service Provider Liability

1 A (legal) gallery of internet intermediary regulation

Introduction

One of the most persistent myths is that privately-held providers are exclusively to blame for 'censoring' users while the sovereignty of the territorial state regarding internet content regulation is eroding.[64] The opposite is true: state regulation on 'the internet' has increased since the 1990s. While not 100% successful, this regulation increase can hardly be seen as an erosion of sovereignty. States can regulate providers and are increasingly doing so. For example, the US and the EU successfully imposed regulations exempting intermediaries of (some) liability for the content user-provided information.[65] However, constitutional law and human rights standards form a limitation on state regulation of providers.[66] Regulation of providers is thus not technologically impossible or legally unrealistic.

While the content categories subjected to regulation may have changed, governmental pressure on providers to regulate user-provided information is hardly new. Two of the first challenges for the territorial state were preventing minors from encountering internet pornography and combatting annoying spam.[67] Later the focus shifted to fighting illegal content such as sexual child abuse material, (illegal) gambling, and computer-related criminality.[68] Over the years, the list of categories subjected to regulation has grown. In 2018, new legislation removed the immunity for (civil) liability claims based on sex trafficking law in the US.[69] In 2021 the EU adopted new regulations targeting online terrorist content.[70] Regulation of user-provided information is thus not merely the result of providers prohibiting specific content by imposing self-regulation. To regulate internet content, lawmakers enacted real laws backed by real fines. Many of these laws aim to regulate providers directly.[71]

---

[64] In the Netherlands, this position is represented by constitutional law scholars and by governmental advisory bodies, see for example, R. Passchier, *Artificiële intelligentie en de rechtsstaat: Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderhoud*, Den Haag, Boom juridisch, 2021, p. 81; Adviesraad Internationale Vraagstukken, 'Regulering van online content: Naar een herijking van het Nederlandse internetbeleid (AIV-advies 113)', *Adviesraad Internationale Vraagstukken,* 2020, available at adviesraadinternationalevraagstukken.nl/documenten/publicaties/2020/06/24/regulering-van-online-content (retrieved on 14 February 2022), p. 11.

[65] 47 USCA § 230 (West 2018, Westlaw Next through PL 116-91); Directive 2000/31/EC (*Directive on electronic commerce*).

[66] For example, Russia and Turkey are fairly successful in enforcing the law, see A. Kolodyazhnyy, A. Marrow & A. Osborn, 'Russia says Twitter complying with demand to remove 'banned content'', *Reuters,* 30 April 2021, available at reuters.com/technology/russia-says-twitter-is-complying-with-demand-remove-banned-content-2021-04-30 (retrieved on 15 February 2022); C. Caglayan, et al., 'YouTube says to appoint Turkey representative in line with new law', *Reuters,* 16 December 2020, available at reuters.com/article/us-turkey-socialmedia-youtube-idUSKBN28Q1T2 (retrieved on 14 February 2022). In the US, for example, the First Amendment prohibits many possible regulatory approaches, see Keller, 2021, 'Six Constitutional Hurdles for Platform Speech Regulation'.

[67] L. Lessig, *Code Version 2.0*, New York, Basic Books, 2006, p. 245.

[68] P. van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, Vol. 48, No. 5, 2011, p. 1461.

[69] Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA-SESTA), H.R. 1865, 115th Cong. (2018 through PL 115-164); Goldman, 'The Complicated Story of FOSTA and Section 230', *First Amendment Law Review*, 2019, pp. 282-284.

[70] Regulation (EU) 2021/784.

[71] Network Enforcement Act 2017 (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*); Regulation (EU) 2021/784.

Regulation may not only originate from legislation enacted by the traditional territorial state. Directives and regulations proposed by the EC and adopted by the European Parliament (hereafter: EP) and the European Council (hereafter: EUCO) lay the foundation for regulation for providers.[72] Especially noteworthy is that the EC also seeks to regulate internet intermediaries without proposing legislation by, for example, concluding legally non-binding codes with providers.[73] While these codes have no legal binding force, they may be used by a judge interpreting open norms laid down in (national) legislation in a court case.[74] Violations of a voluntary code may also lead to reputational costs for the service provider.[75] Besides the possible costs of not following regional codes, these codes offer providers and regulators advantages. Such regional regulation may lead to a higher level of compliance which is attractive for the regulator, while it also may lower compliance costs for the provider.[76]

Next to regulation targeting new content categories (such as terrorist content), new regulation adds obligations on how providers should address these different content categories. For example, new regulation imposes obligations on providers in handling erroneous removal of user-provided information.[77] Providers are made legally responsible for taking down illegal or unlawful content and protecting users' freedom of expression rights. In the EU, the ambitious proposal for the DSA published in December 2020 forms an example of such regulation.[78]

Regulation of providers takes on new forms. While providers were granted exemptions for legal liability in the 1990s, internet intermediary regulation in the 2020s seeks to codify newly found legal responsibilities for these providers.[79] During the Arab spring, the view was that social media networks were an opportunity for democratic reform.[80] In 2021 this positive view changed in critique. Election disinformation and conspiracy theories leading to the violent insurrection in the US Capitol on 6 January 2021 are just two examples of such criticism.[81] Real-world events such as

---

[72] Of which is the most notable Directive 2000/31/EC (*Directive on electronic commerce*). There is a proposal to update the Directive with the Digital Services Act, see Commission Proposal COM(2020) 825 final (*Digital Services Act*).

[73] See on the status of these codes V. Mak, *Legal Pluralism in European Contract Law*, Oxford, Oxford University Press, 2020, doi:10.1093/oso/9780198854487.001.0001, pp. 131-135.

[74] For example, Rb. Amsterdam (vzr.), 9 September 2020, ECLI:NL:RBAMS:2020:4435, Rec. 4.4-4.5 and 4.11 (*YouTube*).

[75] Bradford, 2020, *The Brussels Effect*, p. 161. See for monitoring by the EC, European Commission, 2021, 'Code of Practice on Disinformation'; European Commission, 'The EU Code of conduct on countering illegal hate speech online', *European Commission*, available at ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (retrieved on 14 February 2022).

[76] Bradford, 2020, *The Brussels Effect*, pp. 162-166.

[77] Klos, "Wrongful moderation': Aansprakelijkheid van internetplatforms voor het beperken van de vrijheid van meningsuiting van gebruikers', *Nederlands Juristenblad*, 2020/2976.

[78] Commission Proposal COM(2020) 825 final (*Digital Services Act*); F. Wilman, 'Het voorstel voor de Digital Services Act: Op zoek naar nieuw evenwicht in regulering van onlinediensten met betrekking tot informatie van gebruikers', *Nederlands tijdschrift voor Europees recht*, No. 1-2, 2021, doi:10.5553/NtER/138241202021027102002, p. 34; Klos, 'De Digital Services Act: implicaties voor het recht op vrijheid van meningsuiting van gebruikers van onlineplatforms', *NTM/NJCM-bull.*, 2021/13, pp. 137-138.

[79] Commission Proposal COM(2020) 825 final (*Digital Services Act*).

[80] E. Morozov, *To Save Everything, Click Here*, London, Penguin, 2014, pp. 127-128.

[81] T. Nguyen & M. Scott, "Hashtags come to life': How online extremists fueled Wednesday's Capitol Hill insurrection', *Politico,* 8 January 2021, available at politico.com/news/2021/01/07/right-wing-extremism-capitol-hill-insurrection-456184 (retrieved on 8 January 2021).

the migration crisis (for example, in the EU),[82] election interference (in various regions),[83] live streams of terrorist attacks (addressed by, for example, the EU),[84] and the COVID-19 pandemic (worldwide)[85] fuelled or strengthened the (perceived) need for new regulation.

Regulating the providers that offer internet services is not uncomplicated. Every form of internet regulation may have unintended and unpredictable side effects. These side-effects may have massive consequences for human rights.[86] While it is easy to enact legislation to require providers to be more responsible for illegal or unlawful content of user-provided information, such legislation may not always have this effect. Besides, overregulating the internet may hamper innovation and thus the economic and societal benefits that the internet could bring.[87] The territorial state, shortly put, had (and still has) to find a mode of regulation that does remedy harmful effects that may come from the usage of the internet while safeguarding the (potential) economic and social benefits (including the possibility to exercise freedom of expression rights).

The first chapter, thus, provides an answer to the question to what extent it is necessary to distinguish regulation between (different) online and offline information intermediaries to prevent overregulation and underregulation based on the content of the information. First, I set out the differences between online and offline information intermediaries to answer this question. After setting out these differences, the discussion turns to the three waves of regulation of providers to discuss the differences in regulation between online and offline providers. After this legislative overview, this chapter discusses the differences in regulation of providers based on their technological capabilities, legal obligations, and functional involvement with the content of user-provided information. In short, this chapter thus distinguishes between

1. Who is the provider of an intermediary service?
2. What is the provided intermediary service?
3. What are the specific activities, roles, and functions that the provider of an intermediary service fulfils?

1.1 Offline information intermediaries and internet intermediary service providers

Before discussing how providers relate to internet content regulation, it is first necessary to discuss what an intermediary – or more specifically, an information intermediary – is. The online dictionary

---

[82] Recitals 53 and 57 of European Parliament resolution of 13 December 2016 on the situation of fundamental rights in the European Union in 2015 (2016/2009(INI)), *OJ C 238*, *6.7.2018*, pp. 17-18; European Commission, 'Code of Conduct on Countering Illegal Hate Speech Online', *European Commission,* 30 June 2016, available at ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (retrieved on 14 February 2022), p. 1.

[83] European Commission, 2021, 'Code of Practice on Disinformation'.

[84] L. Kayali, 'Europe's struggle against viral terrorist content', *Politico,* 21 May 2019, available at politico.eu/article/how-europe-plans-to-fight-christchurch-style-viral-content-its-complicated-fake-news-social-media-facebook-twitter-eu-terrorism (retrieved on 15 February 2022); Regulation (EU) 2021/784.

[85] World Health Organization, 2020, 'Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation'; Joint Communication JOIN(2020) 8 final.

[86] For example, the risk that more content is removed than strictly necessary. Balkin refers to this as collateral censorship, see J. Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, Vol. 118, No. 7, 2018, pp. 2016-2017. Another risk is that internet intermediaries refrain from (voluntary) moderation because of the risk of liability, see A. Kuczerawy, 'The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?', *CiTiP Blog,* 14 April 2018, available at law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5 (retrieved on 15 February 2022).

[87] As noted in Recital 60 of Directive 2000/31/EC (*Directive on electronic commerce*).

Lexico defines 'intermediary' as: "A person who acts as a link between people in order to try and bring about an agreement; a mediator."[88] Intermediate has its origin in contracting *inter* and *medius*, translated as *between* and *middle*.[89] An intermediary, thus, is expected to fulfil a role as a mediator between two (or more) parties. As will be shown, the internet knows its fair share of intermediaries. While these intermediaries are vastly different in size and function, they have, as Perset states, in common that they

> bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.[90]

Providers that function as intermediaries facilitate transactions in the broadest sense of the word. Providers function primarily as intermediaries that facilitate sharing and encountering (user-provided) information on the internet. However, how these providers mediate is different from how traditional offline information intermediaries mediate. While the dictionary definition of intermediary may suggest otherwise, not all providers try to conclude agreements between users.

Intermediaries mediate between authors and readers in the traditional (offline) information intermediary industry. These information intermediaries play a decisive role in deciding what information is published and what publications are not. The characterisation of intermediaries as gatekeepers comes precisely from this role.[91] Such a gatekeeping role is not without consequences. When an intermediary has control over the content of a publication, this also creates legal responsibilities. Whether a newspaper will print a piece is the editor's decision. Printing a libellous article without sufficient fact-checking may render the newspaper liable for its content.[92]

Other intermediaries are less involved with the actual content of a publication. For example, a printer does not proofread all documents for illegal content before printing. A bookshop owner or newsstand may make hard choices regarding what is put on the scarce shelf space but not read all books or newspapers before putting them out for sale. However, this more distant role does not mean that a bookseller is entirely exempted from liability for the book's content. Knowledge of the illegal or unlawful content of the book may expose the bookseller to liability.[93] Publishers and editors may be exempted from liability for the content of books to avoid preventive (self)censorship out of fear of liability. Such exceptions, however, do not mean that

---

[88] Lexico, 'Meaning of intermediary in English', *Lexico*, available at lexico.com/definition/intermediary (retrieved on 15 February 2022).

[89] Lexico, 'Meaning of intermediate in English', *Lexico*, available at lexico.com/definition/intermediate (retrieved on 15 February 2022).

[90] K. Perset, 'The Economic and Social Role of Internet Intermediaries', *OECD Digital Economy Papers* No. 117, Paris, OECD, 2010, doi:10.1787/20716826, p. 9.

[91] J. Oster, *Media Freedom as a Fundamental Right*, Cambridge, Cambridge University Press 2015, doi:10.1017/CBO9781316162736, p. 62.

[92] See, for example, *Lindon, Otchakovsky-Laurens and July v. France* [GC], no. 21279/02, 36448/02, § 65-67, ECHR 2007-IV, 22 October 2007, ECLI:CE:ECHR:2007:1022JUD002127902; *Khawar v. Globe Intern., Inc.*, 965 P.2d 696, 704-708 (Cal. S.C. 1998); *Globe Intern., Inc. v. Khawar*, 119 S.Ct. 1760 (1999).

[93] See, for example, *Smith v. People of the State of California*, 80 S.Ct. 215, 216-220 (1959); HR, 14 February 2017, ECLI:NL:HR:2017:220 (concl. P.C. Vegter), Rec. 2.1 and 3.4, *Nederlandse Jurisprudentie* 2017/259, m.nt. E.J. Dommering; R. Blommestijn & M. Klos, 'Een giftige paddenstoel voor de vrijheid van meningsuiting: Bol.com en het verbieden van 'foute' boeken', *Nederlands Juristenblad*, 2020/1209.

they have no legal responsibilities at all.[94] The general principle is simple: increasing control over and involvement in the content of a publication comes with (legal) responsibilities.

Information intermediaries are unmissable for producers and consumers of such information. Precisely this position makes information intermediaries a potent regulator over what information finds its way to consumers and what information does not. The internet is not different with respect to the reliance on information intermediaries. Users browsing the internet may feel that there are no gatekeepers – that there are no gates. A user posting on a social media platform perhaps may not realize how many intermediaries are involved. The user first has an internet connection facilitated by an internet service provider. Without this connection posting to an internet platform would be impossible. The website facilitating user-provided information is the second intermediary. The website and the provider all use intermediary services of their own. As shown, not all these intermediaries offer control points over user content. Not all intermediaries fulfil a gatekeeping role or have the (technological and legal) possibilities or responsibilities to intervene in what content can find its way on the internet.

Providers of internet information intermediary services are different from traditional information intermediaries. Posting on the internet does not require a printer to print a tweet before its content is available. There is no bookstore with limited (shelving) space for a limited selection of social media posts. Providers that offer social media functionalities do not exercise ex-ante editorial control over user-provided information often.[95] Social media platforms perhaps exist by the grace of allowing user-provided information.[96] That users can post everything they like does not mean that the providers of these platforms do not perform a governing or gatekeeping role.[97] Providers can and do intervene in the content of user-provided information. Sometimes such interventions are even referred to as a form of (private) 'censorship'.[98] As Lessig notes, censorship is a hefty term to use in the context of legitimate speech regulation. Lessig refers to legitimate 'censorship' as "speech regulation".[99] Due to the negative connotation of censorship, in this dissertation, censorship is merely used in the context of clearly illegitimate governmental interventions on freedom of expression rights.

---

[94] In the Netherlands, for example, the publisher and printer cannot be prosecuted for "crimes committed by the printing press" as long as they state the name and place of residence of the person who ordered the printing on the print or reveal the person when the examining magistrate request to do this, see Article 53 and 54 of Wetboek van Strafrecht (Dutch Criminal Code).

[95] In the Netherlands, some online news papers that offer such functionalities pre-screended user comments at one time in their history, such as nu.nl.

[96] According to the OECD which relies on the terminology user-created or generated content this concerns public accessible, non-professional content which has some creative effort, see OECD, 'Participative Web and User-Created Content', *OECD,* 2007, available at oecd-ilibrary.org/science-and-technology/participative-web-and-user-created-content_9789264037472-en, doi:10.1787/9789264037472-en, pp. 17-18.

[97] F.T. Wu, 'Collateral Censorship and the Limits of Intermediary Immunity', *Notre Dame Law Review*, Vol. 87, No. 1, 2011, pp. 298-300; E.B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*, Cambridge, Cambridge University Press, 2015, doi:10.1017/CBO9781107278721, pp. 52-56; Par. 6.21 of Wilman, 2020, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*, p. 177. Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech', *Harvard Law Review*, 2018.

[98] M.K. Land, 'Against Privatized Censorship: Proposals for Responsible Delegation', *Virginia Journal of International Law*, Vol. 60, No. 2, 2020, p. 46.

[99] Lessig, 2006, *Code Version 2.0*, p. 254.

A second relationship in which providers mediate is between the service user (probably including you) and governments that seek to regulate the user.[100] States seek to regulate the content of user-provided information not by imposing fines or punishments on the creator of the information with illegal content but by regulating the providers that offer the service. Balkin contrasts this "new-school speech regulation" with "old-school speech regulation", in which governments directly regulate the responsible party as the creator of the information with illegal content.[101] According to Balkin, "new-school speech regulation" is characterised by states "attempting to coerce or co-opt private owners of digital infrastructure to regulate the speech of private actors."[102] Because the state depends on the providers to carry out state regulations, the provider plays a mediating role between the state and the user.

How providers shape their roles and what users expect from them is different from traditional intermediaries. Nobody frowns when a newspaper edits a reader-submitted piece for an opinion page (as long as the line of thought is maintained). Newspapers even select between different contributions offered to them. Similar interventions on, for example, Facebook are unthinkable. Newspapers edit; providers of social media platforms do not. This difference, however, does not mean that internet intermediaries do not intervene in user content at all. Providers do fulfil roles that come close to classic editorial functions: moderation and curation. While moderation usually sees to remedying extremes of the content of user-provided information or other user behaviour,[103] curation encompasses selecting and organising user-provided information based on its content.[104] The distinction between moderation and curation is not always easy to make and is certainly not recognised by every scholar.[105] As Paragraph 2.2 shows, curation may sometimes even take the form of moderation. For this paragraph, it is necessary to consider that moderation involves remedies imposed after establishing a rule violation. In contrast, curation encompasses recommendations made to (groups of) users based on the information's content and the users' characteristics.

All providers that offer a platform for user-provided information have some moderation in place. According to Gillespie, moderation "is essential, constitutional, definitional" for platform services.[106] Providers offering platform services typically allow users to submit information and offer social tools to encounter and interact with such user-provided information.[107] Because providers offer a service to upload user-provided information, they can intervene in the content of this information. This intervention may see to editing the content of the information but also

---

[100] R. MacKinnon, *Consent of the Networked: The Worldwide Struggle For Internet Freedom*, New York, Basic Books, 2013 [2012], p. 9.

[101] Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, pp. 2015-2016.

[102] Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2016.

[103] Lexico, 'Meaning of moderation in English', *Lexico*, available at lexico.com/definition/moderation (retrieved on 15 February 2022).

[104] Lexico, 'Meaning of curate in English', *Lexico*, available at lexico.com/definition/curate (retrieved on 15 February 2022).

[105] The distinction between 'hard' moderation and 'soft' curation is not easy to make. For example, Daphne Keller views removal and ranking as a subset of curation activities, see Keller, 2019, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech'.

[106] Gillespie, 2018, *Custodians of the Internet*, p. 21.

[107] See for Gillespie's definition of platform, Gillespie, 2018, *Custodians of the Internet*, p. 18 and 21. The definition provided here and by Gillespie overlaps with the definition of 'online platform' as proposed in the Digital Services Act, see Article 2(h) of Commission Proposal COM(2020) 825 final (*Digital Services Act*), p. 45.

lead to complete removal or limiting its accessibility. Moderation sees to activities relating to "detection, review, and enforcement"[108] of the platform's guidelines which is hard or impossible when there is no direct access to and control over user-provided information. Providers that offer a service consisting of platform functionalities without moderation are a rarity. According to Gillespie, moderation is "the commodity" offered by these services. Moderation makes a platform usable. Without moderation, illegal or undesirable content would swamp the platform.[109] Therefore, even platforms that promise almost unrestricted freedom of expression have some moderation.[110] While a broad range of remedies is available, moderation efforts typically lead to keeping information up (no violation) or removing information (after a violation) based on its content.[111] The rationality behind removal and the possible alternative remedies is part of the discussion in Chapter 2 of this dissertation.

Moderation is the first, most defining activity of these internet intermediary service providers. The second activity undertaken by these providers is curation. Curation comes close to classic editorial functions. All platform services include some moderation. In contrast, not all services offer curation.[112] As set out, curation encompasses selecting and organising user-provided information. Curation is different from moderation since curation usually is not used to remedy the platform's policy violations. Curation encompasses decisions about what, how and when information with specific content is shown to users. Many providers use so-called 'recommender systems'[113] – automatic systems to recommend user-provided information to other users.[114] While filtering and recommending relevant content is a classic intermediary function, the difference is that providers are hardly active or conscious. Instead, predictions form the basis for recommendations of what user-provided information may be relevant for those who receive these recommendations.[115] Providers, however, often lack in-depth knowledge of why automatic systems make a specific recommendation because the process is complex. For example, Twitter noted in some countries that its algorithm amplified posts by right-wing politicians more than user-provided information posted by left-wing politicians. The reason for this difference in amplification? Twitter could not tell for sure.[116] Recommender systems (automatic systems that recommend user-provided information to other users), for example, take into account previous interactions with other information and what other users clicked on that have similar profiles to the user that receives the recommendations. There are signs that these recommender systems, for example, recommend user-provided information with extremist content after viewing content that

---

[108] Gillespie, 2018, *Custodians of the Internet*, p. 21.

[109] Gillespie, 2018, *Custodians of the Internet*, p. 207.

[110] Parler, 'Community Guidelines', *Parler,* 2 November 2021, available at parler.com/documents/guidelines.pdf (retrieved on 15 February 2022).

[111] Goldman, 'Content Moderation Remedies', *Michigan Technology Law Review*, 2021, pp. 4-6.

[112] Of course, this position could be contested as well. The argument can be made that platforms that do not select or organise user content but simply provide a chronological timeline which is also a form of curation.

[113] Article 2(o) of Commission Proposal COM(2020) 825 final (*Digital Services Act*), p. 45.

[114] Gillespie, 2018, *Custodians of the Internet*, p. 196.

[115] Legally, how internet intermediaries are involved in user content, may matter for their liability, see Judgement of the Court (Grand Chamber) of 12 July 2011 in *C-324/09, L'Oréal SA and Others v. eBay International AG and Others*, ECLI:EU:C:2011:474, in particular Rec. 116.

[116] R. Chowdhury & L. Belli, 'Examining algorithmic amplification of political content on Twitter', *Twitter Blog,* 21 October 2021, available at blog.twitter.com/en_us/topics/company/2021/rml-politicalcontent (retrieved on 14 February 2022); Chowdhury & Belli, 2021, 'Examining algorithmic amplification of political content on Twitter'.

only relates lightly to such extremist content.[117] Automatic content curation is thus not a stamp of approval of the provider vowing for the authenticity, originality, or factuality of the content of information in question. The providers may have other goals in recommending user-provided information to other users.[118] However, amplifying information with specific content is not (always) grounded in a conscious decision.

In its gatekeeping role, a provider could exercise broad discretion. Providers are merely required to moderate illegal or unlawful content. Providers, however, could moderate additional categories of content on top of illegal content.[119] Providers that curate even have a broader discretion in promoting and demoting user-provided information. In doing so, some providers assert that they are concerned with upholding their users' freedom of expression rights.[120] However, there is little transparency about how providers regulate user-provided information.[121] Next to a lack of transparency, only a few (in the EU) to almost none (in the US) legal remedies exist for users to oppose moderation efforts the user deems unfair.[122]

A distinction between ex-ante and ex-post regulation is helpful in this respect. Ex-ante regulation encompasses interventions before admittance; ex-post regulation to inventions on user-provided information already admitted to the service. While ex-ante regulation of user-provided information comparable to traditional media is still technologically possible, many providers refrain from such ex-ante control because it is hard to scale. Instead, they choose ex-post moderation of user-provided information. Providers choose such moderation since the liability regime for user-provided information differs from traditional media. Newspapers exercising editorial control also bear legal responsibility for what they publish. For providers, this is not necessarily the case.[123] Traditional media usually are liable for publishing illegal content. In contrast, some additional conditions must be satisfied for internet providers (at least) before the provider can be held liable. There may be good reasons for such exceptionalism.[124] For example, state regulation imposing liability on providers for the content of user-provided information may lead

---

[117] Research suggests that this is the case with YouTube, see J. Whittaker, et al., 'Recommender systems and the amplification of extremist content', *Internet Policy Review*, Vol. 10, No. 2, 2021, doi:10.14763/2021.2.1565 pp. 12-13 and 15-16.

[118] Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, pp. 2047-2048.

[119] See, for example, Article 14 of Directive 2000/31/EC (*Directive on electronic commerce*). A similar argument is made by Keller, 2019, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech', p. 26.

[120] See, for example, Meta, 'Mark Zuckerberg Stands for Voice and Free Expression', *Meta Newsroom,* 17 October 2019, available at about.fb.com/news/2019/10/mark-zuckerberg-stands-for-voice-and-free-expression (retrieved on 14 February 2022).

[121] W. Benedek & M.C. Kettemann, *Freedom of Expression and the Internet*, Strasbourg, Council of Europe Publishing, 2020, pp. 87-89; Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech', *Harvard Law Review*, 2018, pp. 1665-1666.

[122] D.K. Citron, 'Fix Section 230 and hold tech companies to account', *Wired,* 6 May 2021, available at wired.co.uk/article/section-230-social-media (retrieved on 14 February 2022); Keller, 2019, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech', p. 2; Council of Europe, 2021, 'Content moderation: best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation', pp. 31-33.

[123] Most noteworthy, 47 USCA § 230(c) (West 2018, Westlaw Next through PL 116-91); Article 14 of Directive 2000/31/EC (*Directive on electronic commerce*).

[124] The term 'exceptionalism' is derived from Goldman, 2010, 'The Third Wave of Internet Exceptionalism'.

to a 'chilling effect'[125] on users' freedom of expression rights.[126] Because providers have a legal incentive to engage in excessive moderation of illegal content, this may lead to a chilling effect encompassing the removal of grey-area content that is not illegal or unlawful.

Regulation that imposes liability on providers is not the only reason providers regulate user-provided information. For example, political pressure to act against online terrorist content may be a vestibule to legislation backed by fines, causing providers to self-regulate in advance.[127] However, also non-state pressure may influence the policies of providers. Users voting with their feet or calling for a boycott may have such effects.[128] Besides, providers may copy the policies that apply to other services, leading to the formation of what douek calls "content cartels".[129] A distinction between regulation from other types of influence is necessary. Regulation means using rules that aim to alter the provider's conduct. Mere influence does not encompass such rules. However, for this dissertation, government actors signalling that they will enact regulation will also be counted towards regulation because it aims to control the conduct of providers by enacting rules.[130]

While pressure on providers is not always successful,[131] it is undeniable that providers operate in a highly regulated landscape. Such regulation directly or indirectly targets user-provided information and thus affects the user who provided the information to the service. Because the provider is the primary target of and responsible for carrying out regulation, how such regulation views the user's role is secondary. Therefore, it is necessary to discuss the landscape in which these providers function. Why did providers become the primary target for regulation? Why do governments not invest in better regulating users instead? How does such regulation relate to the technological features of these providers? What are the legal categories used to understand these

---

[125] *Lexico* defines 'chilling effect' as

> A discouraging or deterring effect on the behaviour of an individual or group, especially the inhibition of the exercise of a constitutional right, such as freedom of speech, through fear of legal action.

See, Lexico, 'Meaning of chilling effect in English', *Lexico*, available at lexico.com/definition/chilling_effect (retrieved on 15 February 2022).

[126] Wu, 'Collateral Censorship and the Limits of Intermediary Immunity', *Notre Dame Law Review*, 2011, pp. 304-308.

[127] Citron, 'Extremist Speech, Compelled Conformity, and Censorship Creep', *Notre Dame Law Review*, 2018, pp. 1037-1038.

[128] However, the cost of leaving or changing platforms may be too high, see Gillespie, 2018, *Custodians of the Internet*, p. 177. This is caused by network effects: the value of a network (or platform) is tied to its amount of users, see M. Yemini, 'The New Irony of Free Speech', *Columbia Science and Technology Law Review*, Vol. 201, No. 1, 2018, pp. 181-182. Of course, this brings intermediaries in a position of enormous power, see F. Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power', *Theoretical Inquiries in Law*, Vol. 17, No. 2, 2016, doi:10.1515/til-2016-0018, p. 496.

[129] e. douek, 'The Rise of Content Cartels', *Knight Columbia,* 11 February 2020, available at knightcolumbia.org/content/the-rise-of-content-cartels (retrieved on 14 February 2022), pp. 18-19.

[130] C. Angelopoulos, et al., 'Study of fundamental rights limitations for online enforcement through self-regulation Institute', *Institute for Information Law (IViR),* 2015, available at hdl.handle.net/11245.1/7317bf21-e50c-4fea-b882-3d819e0da93a, pp. 56-57.

[131] D. Rushe & Associated Press, 'Mark Zuckerberg: advertisers' boycott of Facebook will end 'soon enough'', *The Guardian,* 2 July 2020, available at theguardian.com/technology/2020/jul/02/mark-zuckerberg-advertisers-boycott-facebook-back-soon-enough (retrieved on 15 February 2022).

providers? How does this relate to the roles and functions these providers fulfil? These questions are central to this first chapter.

1.2 Drafting the laws of the internet

In the 1990s, legislators had to deal with a thorny question: to what extent should providers be liable for the content of user-provided information? Enacted legislation offers an 'exceptionalist'[132] position to these providers, which treats providers differently than their offline counterparts. This exceptionalism arose because the providers of internet intermediary services are viewed differently from their offline counterparts, which justifies a different legal treatment. New proposals for legislation are (necessary) built upon these pre-existing statutes: there is always some path dependency. Earlier choices with respect to the legal regimes influence new regulations.[133] EU proposal for the new DSA builds upon the e-Commerce Directive enacted in 2000.[134] In the US, new proposals for legislation must somehow relate to the 1996 enacted Section 230 of the CDA.[135] The discussion of this legislation takes place in Part 2. For now, it is necessary to remark that lawmakers seek to increase the regulatory burden for providers, making them responsible for distinct content categories of user-provided information and (perceived) harms that come from the existence of these services.

While lawmakers increasingly add new obligations for providers in legislation, this does not mean that a critical stance from the state was absent before. According to Goldman, internet regulation came in three waves of "exceptionalism", which means that the internet is in all these waves treated differently from other, mainly traditional – offline – media.[136] In the first wave, regulation favoured providers over offline media; in the second wave, regulation became stricter for providers of internet intermediary services. The third wave came with a more nuanced view of internet intermediary regulation by differentiating regulation between providers based on their characteristics.[137]

1.2.1 The first wave: exceptionalist statutes that form the foundation

On 24 May 1995, the New York Supreme Court ruled in a defamation case against such a provider in *Stratton Oakmont v. Prodigy*. Prodigy exploited an online bulletin board – an early predecessor of social media platforms. Such a bulletin board allowed users to publish comments. In the 'Money Talk'-section, comments were posted on the subject of the brokerage house Stratton Oakmont. Some of these comments were defamatory.[138] Stratton Oakmont sued Prodigy for damages and asked for a court order to remove the defamatory comments.[139] Whether Prodigy qualified as a distributor or publisher of the defamatory comments was pivotal for the liability of Prodigy. As Kosseff notes, the distributor/publisher distinction was decisive at the time. As a distributor,

---

[132] Goldman, 2010, 'The Third Wave of Internet Exceptionalism'.

[133] For a brief description of this phenomenon, see L.B. Solum, 'Legal Theory Lexicon: Path Dependency', *Legal Theory Blog,* 2 September 2018, available at lsolum.typepad.com/legaltheory/2018/09/legal-theory-lexicon-path-dependency.html (retrieved on 15 February 2022).

[134] Commission Proposal COM(2020) 825 final (*Digital Services Act*), pp. 1-3.

[135] FOSTA-SESTA, H.R. 1865, 115th Cong. (2018 through PL 115-164).

[136] Goldman, 2010, 'The Third Wave of Internet Exceptionalism', p. 165.

[137] Goldman, 2010, 'The Third Wave of Internet Exceptionalism', pp. 165-167.

[138] *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L Rep 1794 (N.Y. Sup. Ct. 1995). Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, pp. 45-48.

[139] Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, p. 48.

Prodigy would only be liable when scienter could be proven. As a publisher, Prodigy would be liable no matter what.[140]

How was Prodigy involved in the user-provided information? Prodigy, the court established, 1) set the rules on the bulletin board, 2) reserved the right to delete posts in violation of these rules, and 3) manually reviewed the bulletin board for violating the rules but abandoned this practice due to the large volumes of comments. Instead, Prodigy replaced manual review with automatic scanning software. This software only scanned for words that were on a so-called blocklist. However, this automatic filtering software could not evaluate whether the comment's meaning was defamatory. For such comments, Prodigy relied on a notice and takedown procedure. Prodigy would remove defamatory comments after it received a notification.[141] Based on how Prodigy handled user-provided information, the Court concluded that Prodigy exercised editorial control over the comments and that Prodigy thus could be considered a publisher of these comments.[142]

The *Prodigy* ruling led to a discussion in the US House of Representatives. Two members of the House, Christopher Cox and Ron Wyden, expressed their concern that the *Stratton Oakmont* ruling would lead providers to refrain from moderation out of fear of liability. Another risk was that it would cause providers to shut down their services. Therefore, Cox and Wyden proposed an amendment to the Communications Decency Act, which was adopted and codified into law as Section 230.[143] Section 230 aimed to exempt providers from liability as a "publisher or speaker" for the content of user-provided information[144] and wished to encourage voluntary moderation by shielding providers from liability for voluntary "good faith" moderation.[145] These protections will be discussed more extensively in Chapter 3. As Kosseff notes, Section 230 offers much broader protection to providers than traditional media.[146] For example, under Section 230, whether a provider has knowledge (scienter) of defamatory content of user-provided information is irrelevant.[147] The reasons, the text of the statute, and its effects on the internet make Section 230 truly an exceptionalist statute.[148] Paragraph 3.1 discusses the different exceptions and nuances of Section 230 protections. For now, it is only necessary to keep in mind that Section 230 offered an

---

[140] This is the standard laid down in *Cubby, Inc. v. CompuServe, Inc.*, 776 F.Supp. 135, 139-142 (S.D. New York 1991); Kosseff, 2019, *The Twenty-Six Words That Created the Internet*. Under Section 230, the publisher/distributor distinction, however, has lost its meaning since distributing could be seen as a subclass of publishing for the purpose of Section 230, see *Zeran v. America Online, Inc.*, 129 F.3d 327, 331-334 (3rd Cir. 1997).

[141] Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, pp. 49-51.

[142] Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, p. 52. *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L Rep 1794 (N.Y. Sup. Ct. 1995).

[143] Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, pp. 60-66; D. Citron & B. Wittes, 'The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity', *Fordham Law Review*, Vol. 86, No. 2, 2017, pp. 405-406; 47 USCA § 230 (West 2018, Westlaw Next through PL 116-91).

[144] 47 USCA § 230(c)(1) (West 2018, Westlaw Next through PL 116-91).

[145] 47 USCA § 230(c)(2) (West 2018, Westlaw Next through PL 116-91).

[146] Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, p. 65.

[147] E. Goldman, 'Why Section 230 Is Better Than the First Amendment', *Notre Dame Law Review*, Vol. 95, No. 1, 2019 (available at scholarship.law.nd.edu/ndlr_online/vol95/iss1/3), p. 38.

[148] E. Goldman, 'An Overview of the United States' Section 230 Internet Immunity', *in* G. Frosio (Ed.) *The Oxford Handbook of Online Intermediary Liability*, Oxford, Oxford University Press, 2020, doi:10.1093/oxfordhb/9780198837138.013.8, pp. 162-165.

exemption for liability from user-provided information to providers that do not equally apply to traditional intermediaries.

The history of how the e-Commerce Directive of 2000 made it into the EU lawbooks is different and less exciting. The Directive, as its name suggests, deals with electronic commerce. Only a portion of the Directive discusses the legal exception of liability for providers.[149] Section 230 would (mainly) get its EU equivalent in Article 14, which limits the liability for hosting service providers,[150] and Article 15, which prohibits member states from imposing a general obligation on internet intermediaries to monitor for user-provided information with illegal or unlawful content.[151] As discussed in Paragraph 4.1, the protections offered by the e-Commerce Directive are not absolute and certainly not unconditional. While there could be a freedom of expression incentive behind these provisions, the original proposal dating from 1998 suggests that economic motives were of primary concern to the drafters of the Directive. Elimination of internal market barriers is a requirement to fully profit from the innovation provided by providers of internet services. One of these barriers was that internet intermediaries had to adhere to the different liability regimes enacted by the member states of the EU.[152] The meaning of the Directive for the internal market still has a prominent place in the Directive.[153] However, unlike the 1998 proposal, the 2000 Directive also refers to users' freedom of expression rights in the recitals.[154] Recitals, setting out the purpose and goals of the Directive, may gain legal meaning in court proceedings in interpreting the provisions laid down in the Directive.[155] For example, as Recital 46 notes, interventions on user-provided information required under the Directive "has to be undertaken in the observance of the principle of freedom of expression".[156] The e-Commerce Directive offered some exemptions from liability for the content user-provided information. Exemptions that are, again, not offered to traditional information intermediaries – even when they blindly copy-paste the content of the information.

Goldman describes the first wave of exceptionalist regulation as 'Internet Utopianism'. Goldman's primary focus as a US legal scholar is on US Section 230. By granting such an exemption from liability, providers of internet intermediary services were (largely) left unregulated. Meaning that providers were not actively required to combat user-provided information containing illegal or unlawful content.[157] These statutes may be different from those that apply to traditional

---

149 'Liability of intermediary service providers' is the title of the fourth section of Directive 2000/31/EC.

150 Hosting services are not liable for user content as long they 1) have not knowledge or are not aware of the illegal content 2) act expeditiously when they gain such knowledge or awareness and remove or disable access to this content, see Article 14 of Directive 2000/31/EC (*Directive on electronic commerce*). But, see also Article 12 and 13 of Directive 2000/31/EC (*Directive on electronic commerce*).

151 Article 15 of Directive 2000/31/EC (*Directive on electronic commerce*).

152 Recital 2, 4-5 and more specific 16 of Proposal COM(1998) 586 final of 23 December 1998 for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, *OJ C 30, 5.2.1999*.

153 Recital 2-3 and 5-7 of Directive 2000/31/EC (*Directive on electronic commerce*).

154 Recital 9 and 46 of Directive 2000/31/EC (*Directive on electronic commerce*).

155 Van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, 2011, pp. 1467-1468.

156 Recital 46 of Directive 2000/31/EC (*Directive on electronic commerce*).

157 Goldman, 2010, 'The Third Wave of Internet Exceptionalism', p. 165.

intermediaries, to which often more strict liability regimes apply.[158] US Section 230 and the safe harbours in the Directive are the products of a time of internet optimism. This optimism can be characterised as utopian regarding what the internet would bring, combined with the (incorrect) claim that the internet was unregulatable.[159] One of the voices of this utopian thinking was Barlow. In 'A Declaration of the Independence of Cyberspace' Barlow argued that 'Cyberspace' is and should be independent of the territorial state and its government:

> We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.[160]

Barlow's view is a form of norm duality: what is prohibited offline is not necessarily prohibited on the internet. However, this utopian thinking never found its way to the US or EU lawbooks. As Lawrence Lessig notices in *Code Version 2.0* published in 2006, the internet and state regulations differed from when the first edition came out in 1999. Lessig:

> the dominant idea among those who raved about cyberspace then was that cyberspace was beyond the reach of real-space regulation. Governments couldn't touch life online. And hence, life online would be different, and separate, from the dynamic of life offline.[161]

How governments understood the internet in 1999 changed radically in 2006. In 2006 it was clear that the territorial state was interested in regulating the internet and could do so. Internet exceptionalism and the cyberlibertarian ideal are thus not one-on-one related.[162] Neither the US nor the EU in the 1990s accepted the unregulatability of the internet. Instead, the US and the EU seemed warry that a lack of exceptionalism would hamper innovation and harm freedom of expression. Not because the internet was beyond the reach of the law, but because of the fear that existing legislation could hinder innovation.[163]

While governments increasingly exert sovereignty over the internet,[164] the exceptionalist legislation enacted in the 1990s is still in place. [165] The exceptionalist laws became a monumental part of the internet intermediary regulation landscape. Scholars, providers, and legislators became fond of this legislation. The following paragraphs show that it is difficult to change such fundamental legislation.

---

[158] For example, in the Netherlands a provider is better protected than a book seller for criminal prosecution for group defamation, see Blommestijn & Klos, 'Een giftige paddenstoel voor de vrijheid van meningsuiting: Bol.com en het verbieden van 'foute' boeken', *Nederlands Juristenblad*, 2020/1209.

[159] Lessig, 2006, *Code Version 2.0*, p. 3.

[160] J. Barlow, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation,* 8 February 1996, available at eff.org/nl/cyberspace-independence (retrieved on 14 February 2022).

[161] Lessig, 2006, *Code Version 2.0*, p. ix.

[162] H.B. Holland, 'In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism', *University of Kansas Law Review*, Vol. 56, No. 2, 2008, doi:10.17161/1808.19996, p. 376.

[163] Recital 2-3 and 5-7 of Directive 2000/31/EC (*Directive on electronic commerce*); 47 USCA § 230(b) (West 2018, Westlaw Next through PL 116-91).

[164] For example, the EC keeps emphasising that conduct that is illegal offline is also illegal online which is an expression that EU norms also apply to the internet, see European Commission, 'Europe fit for the Digital Age: Commission proposes new rules for digital platforms', *European Commission,* 15 December 2020, available at ec.europa.eu/commission/presscorner/detail/en/ip_20_2347 (retrieved on 14 February 2022).

[165] For example, 47 USCA § 230 (West 2018, Westlaw Next through PL 116-91); Article 12-15 of Directive 2000/31/EC (*Directive on electronic commerce*).

1.2.2 The second wave: internet paranoia

While received in the early 1990s with optimism and utopian thinking, a more critical perspective emerged in the late 1990s. The second wave – which Goldman dubbed "Internet Paranoia" – meant that online activities were more strictly regulated than similar offline activities.[166] While the assumption was that internet regulation of the state was easy to circumvent, governments could regulate the internet by regulating the providers offering services on the internet.[167] The second wave of exceptionalism showed that undesirable conduct on the internet was only possible to regulate by regulating the providers.[168] Providers (often against their will) may enable users to engage in illegal or unlawful conduct by offering their services. This conduct is challenging for the state to address without the provider's help.[169] In other words, the state requires a point of control to regulate internet content successfully. The territorial state relies on providers such as Google, Microsoft, Facebook, and Amazon. These providers offer the means to carry out regulation and thus form targets for regulation themselves.[170]

Internet paranoia is never wholly abandoned. While it has a negative connotation, internet paranoia does not mean (necessarily) that there is an overreaction from governmental actors. Internet paranoia merely means that the treatment of internet providers diverges from the treatment of offline media. For example, during the COVID-19 pandemic, governments treated providers differently from traditional offline media with an unprecedented sense of urgency. While COVID-19 mis- and disinformation could also be spread by offline media, the governmental focus was mainly on providers of internet intermediary services. COVID-19 mis- and disinformation thus mark a new 'peak' of internet paranoia. The World Health Assembly declared that an "infodemic" was taking place, "particularly in the digital sphere, as well as the proliferation of malicious cyber-activities that undermine the public health response".[171] The EC repeated this in words and policy.[172] Despite this language, it is necessary to remark that misinformation and disinformation are not necessarily illegal. User-provided information that qualifies as disinformation or misinformation under providers' policies may even fall under the protection of freedom of expression rights.[173] Chapters 3 and 4 discuss that freedom of expression rights

---

166 Goldman, 2010, 'The Third Wave of Internet Exceptionalism', pp. 165-166.

167 J. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation', *U.C. Davis Law Review*, Vol. 51, No. 3, 2018, p. 1187.

168 Goldman does not connect 'Internet Paranoia' directly to internet intermediary regulation but only to a different treatment of similar conduct on the internet to offline conduct (for example, online hunting was criminalised while offline hunting was not). However, the different examples offered by Goldman see to regulating this conduct trough regulating internet intermediaries, see Goldman, 2010, 'The Third Wave of Internet Exceptionalism', pp. 165-166.

169 For example, Yahoo! was held responsible for allowing users from the US to sell Nazi paraphilia to users in France. After Yahoo! changed its policy, the case was dismissed as no longer relevant in the United States, see *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisémitisme (LICRA)*, 433 F.3d 1199 (9th Cir. 2006).

170 Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation', *U.C. Davis Law Review*, 2018, p. 1175.

171 The Seventy-third World Health Assembly, 'Resolution WHA73.1: COVID-19 response', *World Health Organization,* 19 May 2020, available at apps.who.int/gb/ebwha/pdf_files/WHA73/A73_R1-en.pdf (retrieved on 15 February 2022); World Health Organization, 2020, 'Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation'.

172 Joint Communication JOIN(2020) 8 final, pp. 1 and 8-10.

173 J. van Hoboken, et al., 'Het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties', Amsterdam, IVIR, 2019, available at ivir.nl/publicaties/download/Rapport_desinformatie_december2019.pdf, pp. 18-19.

primarily work between the state and its citizens, meaning that state interference in their citizens' freedom of expression rights is restricted. That said, this does not mean that disinformation is not harmful. The state might have a legitimate interest in regulating COVID-19 mis- and disinformation.

The obligation for the state to respect citizens' freedom of expression rights seems to lose importance when regulating user-provided information through providers. US President Biden said in an interview that online platforms did not do enough against COVID-19 misinformation, which led to the qualification that they are "killing people".[174] While Biden retracted this statement a few days later,[175] the signal was clear: providers must step up their game in combating COVID-19 misinformation. Such non-legislative pressure to regulate speech is known as 'jawboning' – a practice that, according to Genevieve Lakier, may raise First Amendment issues in the US.[176] Not only is informal pressure put on providers to regulate COVID-19 misinformation, but there is also a legislative proposal that seeks to exempt service providers from Section 230 immunity for COVID-19 misinformation.[177]

To be clear: internet paranoia does not mean that (potential) legislative responses form an exaggeration. COVID-19 disinformation is harmful and may pose a real threat – how significant a threat will become apparent in the future. "Paranoia", instead, refers to the difference in treatment compared to traditional media. When it comes to harmful (not necessarily illegal) disinformation, providers face a stricter approach than traditional media.[178] There are no proposals to make television networks liable for the spread of COVID-19 misinformation. There are no legislative proposals to introduce new governmental oversight over television networks spreading mis- or disinformation. In this respect, providers of internet intermediary services are treated differently from traditional media. However, this new internet paranoia does not lead to abolishing exemptions for liability of the content of user-provided information. Instead, these exceptionalist laws – at their core – seem to survive new proposals – they even might be reinforced.[179] However,

---

[174] D. Judd, M. Vazquez & D. O'Sullivan, 'Biden says platforms like Facebook are 'killing people' with Covid misinformation', *CNN,* 17 July 2021, available at edition.cnn.com/2021/07/16/politics/biden-facebook-covid-19/index.html (retrieved on 15 February 2022).

[175] B. Klein, M. Vazquez & K. Collins, 'Biden backs away from his claim that Facebook is 'killing people' by allowing Covid misinformation', *CNN,* 20 July 2021, available at edition.cnn.com/2021/07/19/politics/joe-biden-facebook/index.html (retrieved on 15 February 2022).

[176] G. Lakier, 'The Trump Lawsuits, the Biden Administration's Misinformation Advisory and the Thorny First Amendment Problem of Jawboning', *Lawfare,* 26 July 2021, available at lawfareblog.com/trump-lawsuits-biden-administrations-misinformation-advisory-and-thorny-first-amendment-problem (retrieved on 15 February 2022).

[177] A bill to amend the Communications Act of 1934 to provide that, under certain circumstances, an interactive computer service provider that allows for the proliferation of health misinformation through that service shall be treated as the publisher or speaker of that misinformation, and for other purposes (Health Misinformation Act of 2021), S. 2448, 117th Cong. (2021).

[178] For example, in the Netherlands the Rathenau Institute devoted an entire report to online moral excesses that, according to the report, should be responded to with exceptionalist measures aimed only at internet intermediaries. Evidently, moral transgressions on the Internet are so serious that they deserve their own approach, without going as far as criminalisation that also extends to offline media, see M. van Huijstee, et al., 'Online ontspoord: Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland', *Rathenau Instituut,* 7 July 2021, available at rathenau.nl/nl/digitaal-samenleven/online-ontspoord (retrieved on 15 February 2022).

[179] For example, the Digital Services Act-proposal contains an explicit exemption from liability arising from voluntary actions in 'detecting, identifying and removing, or disabling of access to, illegal content', see Article 6 of Commission Proposal COM(2020) 825 final (*Digital Services Act*), p. 47.

informal governmental pressure and formal legislation that makes internet intermediaries liable for user content may affect these laws contrary to their initial meaning.[180] While providers are not legally obligated to screen user-provided information for unlawful, illegal and (certainly not) harmful content, they may feel pressured to do so. However, these effects, at least until now, do not pose a real threat to the exceptionalist statutes.

1.2.3 Exceptional exceptionalism: a gallery of statutes

Both 'Internet Utopianism' and 'Internet Paranoia' express an exceptional state regulation stance towards the internet. The internet is treated differently from traditional, offline media. In the case of utopianism, the regulation of providers is more favourable in comparison to offline intermediaries. With internet paranoia, this is the other way around. Providers, in this case, are regulated stricter than offline intermediaries that deal with similar types of content or conduct. As shown, regulation of providers still knows its fair share of utopianism and paranoia. Utopianism and paranoia, however, are complemented with a more nuanced view of regulation. According to Goldman, this 'Exceptionalism Proliferation', which forms the third wave, can be characterised as the differentiation of regulation between types of providers.[181] Goldman points out, as an example, that social media networks are regulated differently from other websites.[182]

While Goldman noticed the 'Exceptionalism Proliferation' in 2010,[183] this may still be the default in regulating providers in 2021. At least, this is the case in the EU. While the EC emphasises that "[w]hat is illegal offline is also illegal online",[184] an exceptionalist approach is chosen in decisions over policy instruments to address user-provided information with illegal or unlawful content.[185] A video-sharing platform service has different obligations than other audiovisual media services[186] According to the proposal for the DSA, very large platforms should be regulated differently than more small-scale services.[187] Because providers differ, the standards that apply to different providers also differ. For example, providers are regulated based on the size and functionalities they offer. With the proposal for the DSA, the EC made this differentiation between both size and functionalities more than explicit.[188]

---

[180] For example, FOSTA-SESTA, H.R. 1865, 115th Cong. (2018 through PL 115-164). See Goldman, 'The Complicated Story of FOSTA and Section 230', *First Amendment Law Review*, 2019, pp. 288-289.

[181] Goldman, 2010, 'The Third Wave of Internet Exceptionalism', pp. 166-167.

[182] Goldman, 2010, 'The Third Wave of Internet Exceptionalism', p. 167.

[183] Goldman, 2010, 'The Third Wave of Internet Exceptionalism', p. 167.

[184] Communication COM(2017)555 final of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 28 September 2017 Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, p. 2.

[185] European Commission, 2016, 'Code of Conduct on Countering Illegal Hate Speech Online'; Communication COM(2018)236 final; Regulation (EU) 2021/784.

[186] See, Chapter IXA of Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 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*), *OJ L 95*, *15.4.2010* (data.europa.eu/eli/dir/2010/13/oj); As amended by Article 1(23) of Directive (EU) 2018/1808.

[187] Article 25 of Commission Proposal COM(2020) 825 final (*Digital Services Act*), p. 59.

[188] For example, 'very large online platforms' are regulated differently than online platforms that do not qualify as 'very large', see Article 25 of Commission Proposal COM(2020) 825 final (*Digital Services Act*). In the case of the Regulation on addressing the dissemination of terrorist content online, the size of the hosting service provider does not matter for the requirements under the Regulation. However, Member States seeking to impose a penalty, are required to take into account the size of the provider, see Article 18(2)(f) of Regulation (EU) 2021/784.

In the US, content-based regulation of providers leads to admissibility concerns under the First Amendment.[189] The impossibility of such legislation does not mean that providers can do as they wish. For example, providers could be held morally responsible for user-provided information, which may be a powerful incentive for providers to change their conduct to prevent other legislation that is not content-based.[190] While content-based restrictions are the subject of First Amendment scrutiny, this does not mean that legislation with such restrictions does not make it to the books. There are exceptionalist statutes proposed and adopted at the state level. For example, a Florida Senate bill made it into law in 2021.[191] Since 1 July 2021,[192] social media platforms, for example, "may not willfully deplatform a candidate for office who is known by the social media platform to be a candidate".[193] Providers of social media platforms that fail to comply with this legislation expose themselves to a fine of "$250,000 per day for a candidate for statewide office and $25,000 per day for a candidate for other offices."[194]

However, the Florida bill does not apply to social media platforms with less than 100 million global users every month or less than $100 million in annual revenue. In addition, this legislation also does not apply to "a company that owns and operates a theme park or entertainment complex".[195] Distinguishing between providers with and without a theme park in Florida is 'exceptionalism' (but this time for providers that also own an offline theme park) in its strangest form. Whether the legislation is enforced is questionable. On 30 June 2021, the United States District Court of the Northern District of Florida granted a preliminary injunction against the Florida social media bill, which is

> subject to strict scrutiny because it discriminates on its face among otherwise-identical speakers: between social-media providers that do or do not meet the legislation's size requirements and

---

189 Keller, 2021, 'Six Constitutional Hurdles for Platform Speech Regulation'.

190 B. Sander, 'Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law', *European Journal of International Law*, 2021, doi:10.1093/ejil/chab022, p. 17; Land, 'Against Privatized Censorship: Proposals for Responsible Delegation', *Virginia Journal of International Law*, 2020, pp. 387-388. As douek notes, such informal pressure is not always put on intermediaries publicly, see douek, 2020, 'The Rise of Content Cartels', p. 20. Such pressure, according to Keller occurs in the US and the EU. In the US governmental pressure on internet intermediaries to regulate content may violate the First Amendment, see Keller, 2019, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech', pp. 6-7. As Balkin summarises such '[j]awboning sends the message that infrastructure providers should be patriotic and cooperate with the government, rather than getting on the bad side of government officials.' see Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation', *U.C. Davis Law Review*, 2018, p. 1179.

191 2021 Fla. Sess. Law Serv. Ch. 2021-32 (SB 7072) (West).

192 At least, that was the plan which is put on hold now a preliminary injunction against the law is granted, see *NetChoice, LLC v. Moody*, 2021 WL 2690876 (N.D. Florida 2021); S. Morrison, 'Florida's social media free speech law has been blocked for likely violating free speech laws', *Vox Recode,* 1 July 2021, available at vox.com/recode/2021/7/1/22558980/florida-social-media-law-injunction-desantis (retrieved on 15 February 2022). However, appeal has been filed, see M. Masnick, 'Florida Man Governor Wastes More Florida Taxpayer Money Appealing Ruling About His Unconstitutional Social Media Law', *techdirt,* 13 July 2021, available at techdirt.com/articles/20210713/09513247161/florida-man-governor-wastes-more-florida-taxpayer-money-appealing-ruling-about-his-unconstitutional-social-media-law.shtml (retrieved on 15 February 2022).

193 106.072. Social media deplatforming of political candidates, Fla. Stat. Ann § 106.072(2) (West 2021, Westlaw Next).

194 Fla. Stat. Ann § 106.072(3) (West 2021, Westlaw Next).

195 501.2041. Unlawful acts and practices by social media platforms, Fla. Stat. Ann § 501.2041(1)(g) (West 2021, Westlaw Next).

> are or are not under common ownership with a theme park. The legislation does not survive strict scrutiny. Parts also are expressly pre-empted by federal law.[196]

An appeal is filed against the decision of the District Court. Commentators, however, do not hold their breath. Masnick, for example, criticises this appeal as "yet more of a waste of Florida taxpayer money on a frivolous legal battle".[197]

This brief overview showed how various providers are regulated exceptionally. Exceptionally compared to offline intermediaries and between the different functionalities and sizes providers of internet intermediary services. Through this exceptional regulation, providers are, for example, made responsible for policing hate speech,[198] online terrorist content,[199] and disinformation.[200] For sex trafficking content,[201] copyright violations,[202] and possible much more when new (pending) legislation is adopted.[203] However, regulating providers may lead to issues that are (again) exceptional to internet intermediaries. While the exceptionalist statutes aimed to prevent regulation from hurting innovation, economic progress, and the exercise of freedom of expression rights, new regulation may have unintended side effects. Setting out the landscape in which providers function helps to understand how regulation of providers works.[204] As the following paragraphs show, it is hard to get a clear overview of the regulatory landscape for providers. These regulations all relate in a certain way to how providers, technologically, legally, and functionally fulfil their roles as providers. The three dimensions are the topic of discussion in the next paragraph.

1.3 Carving internet intermediary regulation: three dimensions

As discussed in the previous paragraph, internet intermediary regulation differentiates between different intermediary functions. Regulation may, for example, consider the service provider's size, the monetary success of the service provider, or the actual roles and functions the provider fulfils in the internet intermediary landscape. As discussed, this exceptionalism is tied to the service provider's capabilities and, thus, how the provider relates to user-provided information. The provider relates to this user-provided information in three ways.

First, a service has a technological relationship to user-provided information. Providers differ in the technological capabilities to regulate the content of user-provided information. Due to the internet's design, some providers (for example, providers of social media platforms) are better equipped than others (for example, a telecom provider offering internet access services) to

---

196 *NetChoice, LLC v. Moody*, 2021 WL 2690876 (N.D. Florida 2021).

197 Masnick, 2021, 'Florida Man Governor Wastes More Florida Taxpayer Money Appealing Ruling About His Unconstitutional Social Media Law'.

198 European Commission, 2016, 'Code of Conduct on Countering Illegal Hate Speech Online'.

199 Regulation (EU) 2021/784.

200 European Commission, 2021, 'Code of Practice on Disinformation'.

201 FOSTA-SESTA, H.R. 1865, 115th Cong. (2018 through PL 115-164).

202 Article 17(3) of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *OJ L 130*, *17.5.2019* (data.europa.eu/eli/dir/2019/790/oj).

203 For example, Article 14 of Commission Proposal COM(2020) 825 final (*Digital Services Act*). Article 14(1) contains the obligation to 'put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content.'

204 G. Dinwoodie, 'Who are Internet Intermediaries?', *in* G. Frosio (Ed.) *Oxford Handbook of Online Intermediary Liability*, Oxford, Oxford University Press, 2020, doi:10.1093/oxfordhb/9780198837138.013.2.

regulate the content of user-provided information. Second, providers are, as already shown, grasped in legal categories laid down in case law and statutes. Providers thus differ in their legal relationship with user-provided information. Some providers, for example, may become liable for the content of user-provided information, while others have an exception from such legal liability. The technological dimension is (to a large extent) a given. The legal dimension, however, is not. The technological dimension, to some extent, guides the legal categories applicable to providers. However, the legal dimension also consists of normative claims and policy goals. The technical dimension thus limits legal concepts. The legal concepts, however, seek to influence the functional dimension. The functional dimension (how providers choose to offer their services) may also influence the legal categories because legislators may consider new types of services when drafting new legislation (internet marketplaces and app stores).

The functional dimension is not a one-way street. Providers offer capabilities to users. Users are enabled to use the service in pre-defined ways. For example, an e-mail service may allow text input but forbid (large) attachments. A chat service may prohibit users from taking screenshots of chats or images as a privacy feature. A microblogging service may limit the number of characters or words in one post. These limitations are technological – it is hard to circumvent them. The functional dimension also has a legal (or better: moral) dimension. Users of these services trust the provider to refrain from conduct contrary to the user's goal in using this service. The provider trusts that the user does not misuse the service. The functional dimension is built upon the technological and legal dimension while it adds (unspoken) assumptions about what the provider and the user can expect from each other.

1.3.1 Internet intermediaries: the technological dimension

This chapter primarily deals with providers that offer internet intermediary services with functionalities related to storing, indexing, ranking, and recommending user-provided information. So-called hosting service providers are in the best position to intervene in the content of user-provided information because they have direct access to the information stored by them. So-called social media platforms are often targeted by state regulation because of this hosting role they fulfil. In contrast, an internet service provider (ISP) that provides internet access is normally exempted from such regulation because they lack such a hosting role.[205] A broader range of providers and related functions are subject to discussion to understand the differences in technological capabilities between providers and the different services they offer. Therefore, first, I discuss ISPs to contrast these providers with hosting service providers.

Internet service providers: a gateway to the internet

ISPs function as a gateway to the internet. Without ISPs, it is impossible to access any other service on the internet. ISPs may offer an internet connection through a landline (via the telephone line, coax cable or fibre optic cable) or a wireless connection (most commonly 4G or 5G internet access). Because ISPs depend on a physical infrastructure within the state's territory, they could be targeted directly by state regulation. The territorial state is not dependent on compliance or the

[205] An EU example is the proposal for the DSA. Section 2 (hosting) and Section 3 (very large online platforms) of Chapter 3 of the DSA do not concern ISPs, see Commission Proposal COM(2020) 825 final (*Digital Services Act*), p. 51 and 75. In the US, the DMCA distinguishes between different intermediary functions, compare 17 USCA § 512(a) and (c) (West 2010, Westlaw Next through PL 116-179).

help of a company abroad. The territorial state could even cut the cord in the most extreme case. When the service offered by the ISP is down, there is no access to the internet.[206]

According to Felix Wu, internet intermediary functions – broadly taken – are not technologically different from their pre-internet counterparts. For example, an ISP and traditional telephone company offer a similar service: access to a network.[207] In the case of a telephone provider, this consists of offering a connection to other telephones, while an ISP provides access to a network of other computers.[208] The only difference is the potential use of an internet connection. While a telephone service provider offers a service that allows the user to make a telephone call to another user, the potential usage of an internet connection is practically unlimited. A telephone provider gives access to others by offering voice communication; an ISP offers access to an incredible number of different services.

When it comes to ISP imposing regulations themselves, one of the concerns is that they may restrict access to other services for commercial reasons.[209] While both telephone service providers and ISPs could have commercial goals in restricting the usage of their services or physical infrastructure, for an ISP, such restrictions may be easier to monetise.[210] Technically, ISPs could, for example, restrict access to so-called *tube* services such as YouTube or prohibit videoconferencing services unless users subscribe to a more expensive service plan. As will be shown, modern ISPs have the technical capabilities to discriminate between services by filtering, restricting, and even blocking access to services. An ISP requiring a premium plan before video services can be accessed may seem far-fetched to US and European users, mainly because of so-called network neutrality regulations, which force ISPs to treat traffic equally.[211] However, in a slimmed-down and adapted form, ISPs sometimes favour some (types of) services over others. Zero-rating, for example, exempts the usage of a (group of) service(s) from counting towards monthly data limits. ISPs may favour one or more services by calculating data usage for music streaming applications, while video streaming applications would not count to the monthly restrictions.[212] Another form of favouring services over others is so-called 'paid prioritisation'. Paid prioritisation means that other providers could pay the ISP for faster connections for their users to their service. For example, an ISP may limit the bandwidth used for a specific service to a bitrate that equals HD quality. A streaming service could pay an ISP to remove these limitations to allow

---

[206] Klos, 2021, 'Westphalian Sovereignty and the 4th Industrial Revolution: In Search of Legitimate Governmental Control over Online Content', pp. 110-111.

[207] Wu, 'Collateral Censorship and the Limits of Intermediary Immunity', *Notre Dame Law Review*, 2011, p. 313.

[208] Britannica, 'Internet service provider', *Encyclopedia Britannica,* 13 March 2018, available at britannica.com/technology/Internet-service-provider (retrieved on 14 February 2022).

[209] T. Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*, New York, Columbia Global Reports, 2018, pp. 94-97.

[210] Some issues are remarkably similar. Telephone companies, for example, prohibited users to attach own, not approved, equipment which is very similar to some restrictions ISPs impose, see T. Wu, 'Network Neutrality, Broadband Discrimination', *Journal on Telecommunications & High Technology Law*, Vol. 2, 2003, pp. 157 and 159-162; T. Wu, *The Master Switch: The Rise and Fall of Information Empires*, New York, Vintage Books, 2011, pp. 101-114.

[211] Wu, 'Network Neutrality, Broadband Discrimination', *Journal on Telecommunications & High Technology Law*, 2003, pp. 141-142 and 145-146.

[212] Body of European Regulators for Electronic Communications, 'What is zero-rating?', *Body of European Regulators for Electronic Communications*, available at berec.europa.eu/eng/netneutrality/zero_rating/ (retrieved on 14 February 2022).

users to stream in 4K quality.[213] Such a difference in speed (and thus quality) may nudge users to the faster services, while services that cannot pay the ISP fees may see users leave the service.

While network neutrality rules restrict paid prioritisation and zero-rating, this does not withhold ISPs from seeking the limits of this legislation. The same is true for other means of monetisation. In October 2021, ISPs reopened the debate about whether they could impose limitations on third-party services because of the success of the Netflix series "Squid Game". Due to its popularity, ISPs saw an increase in traffic which they want to pass on the costs to Netflix.[214]

ISPs, as a gateway to the internet, are bound by network neutrality rules. These rules require services to treat all traffic equally. However, not only ISPs themselves may impose usage limitations on their network users. Sometimes states seek to regulate providers (and sometimes especially ISPs) to prohibit specific content categories. The limitations discussed in this paragraph were about service-based restrictions. How would ISPs – and other providers – carry out content-based restrictions on information?

Distinguishing between content and service-based restrictions

ISP-imposed restrictions are (mostly) aimed at complete service. Content-based restrictions by an ISP based on the actual content of the information generally do a poor job. Because of how ISPs function, service-level restrictions are the primary way ISPs can influence the spread of content categories. ISPs, for example, could block access to a service by adding the domain name to a blocklist. A user typing in an internet address (a domain name) in their browser usually results in the ISP translating the domain name to a numerical IP address which allows the browser to find the location of the service on the internet. An ISP could prevent this and thus block access to the service. Such blockades, however, are circumventable by directly entering the IP address. Next to domain name blocking, ISPs can also completely block access to an IP address, which offers a more severe restriction.[215] A third option is that an ISP limits the usage of specific protocols. Closing certain "ports" disables the usage of services that use these ports. By such a limitation, an ISP can, for example, restrict access to video conferencing software.[216]

Service-level restrictions have some severe downsides. In the first place, allowing an ISP to discriminate between services raises competition questions. According to Tim Wu, network discrimination may hamper competitive innovation by raising financial barriers for new competitors. A new service may not have a chance when competitors have an advantage because of zero-rating or paid prioritisation. Network neutrality, requiring ISPs to treat all traffic equally, in opposition, stimulates competition since there are no barriers for new providers to reach potential users.[217] In the end, an internet without net neutrality thus may lead to fewer services and

---

213 K. Trendacosta, 'Busting Two Myths About Paid Prioritization', *Electronic Frontier Foundation,* 16 April 2018, available at eff.org/deeplinks/2018/04/busting-two-myths-about-paid-prioritization (retrieved on 15 February 2022).

214 M. Sweney, 'Squid Game's success reopens who pays debate over rising internet traffic', *The Guardian,* 10 October 2021, available at theguardian.com/business/2021/oct/10/squid-games-success-reopens-debate-over-who-should-pay-for-rising-internet-traffic-netflix (retrieved on 15 February 2022).

215 As, for example, was proposed in the content of The Piratebay, see HR, 13 November 2015, ECLI:NL:HR:2015:3307, *Nederlandse Jurisprudentie* 2018/110, m.nt. P.B. Hugenholtz.

216 Wu, 'Network Neutrality, Broadband Discrimination', *Journal on Telecommunications & High Technology Law*, 2003, p. 165.

217 Wu, 'Network Neutrality, Broadband Discrimination', *Journal on Telecommunications & High Technology Law*, 2003, pp. 141-142 and 145-146.

less diversity between these services, which may indirectly harm the freedom of expression rights of (potential) users.

There are some direct concerns for freedom of expression rights as well. When an ISP limits access to services, this would also affect the information made available through this service. When the ISP intends to restrict access to a specific instance of information by disabling access to the whole service, this is the textbook example of an overbroad restriction. Not all information on the service may contain illegal or otherwise prohibited content. The ISP thus also restrict legal and lawful information by restricting access to the complete service.[218] For example, the Committee of Ministers of the Council of Europe relates network neutrality directly to access to the internet as a right protected under freedom of expression rights. Allowing ISPs to restrict access to services may also (indirectly) limit access to information.[219]

At first, ISPs were a popular target for state regulation.[220] ISPs have a visible presence within jurisdictions in the form of a physical infrastructure that offers a point of contact for state regulation.[221] While content regulation through ISPs may be highly effective, the downside for freedom of expression rights of such bucket shot regulation is acknowledged.[222] Let alone some exceptions,[223] the EU and US have regulations that exempt providers of internet intermediary

---

[218] In the context of governmental regulation, Balkin warns for collateral censorship, see Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation', *U.C. Davis Law Review*, 2018, pp. 1176-1177. However, there are little reasons to believe that ISPs conducting in such regulation themselves would not amount to similar effects. As Jonathan Zittrain puts it: 'ISPs can serve as Internet police, not only cordoning off areas from view when acting as hosts of content, but also more broadly restricting access to particular networked entities with whom their customers wish to communicate-thus determining what those customers can see, wherever it might be online.', J. Zittrain, 'Internet Points of Control', *Boston College Law Review*, Vol. 44, No. 2, 2003, p. 655.

[219] Paragraph 3 and 4 of Committee of Ministers, 'Declaration of the Committee of Ministers on network neutrality (Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies)', *Council of Europe,* 29 September 2010, available at rm.coe.int/09000016805ce58f (retrieved on 14 February 2022). See also Committee of Ministers, 'Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (Adopted by the Committee of Ministers on 13 January 2016, at the 1244th meeting of the Ministers' Deputies)', *Council of Europe,* 13 January 2016, available at rm.coe.int/09000016805c1e59 (retrieved on 14 February 2022).

[220] At least in Germany, France and Great Britain, see J. Goldsmith & T. Wu, *Who Controls the Internet: Illusions of a Borderless World*, New York, Oxford University Press, 2008, p. 73.

[221] Goldsmith & Wu, 2008, *Who Controls the Internet*, pp. 73-74; Zittrain, 'Internet Points of Control', *Boston College Law Review*, 2003, pp. 672-673.

[222] For example by the ECtHR, see *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 66, ECHR 2012-VI, 18 December 2012, ECLI:CE:ECHR:2012:1218JUD000311110; *Cengiz and Others v. Turkey*, no. 48226/10 and 14027/11, § 64, ECHR 2015-VIII, 1 December 2015, ECLI:CE:ECHR:2015:1201JUD004822610; *Kablis v. Russia*, no. 48310/16 and 59663/17, § 94, 30 April 2019, ECLI:CE:ECHR:2019:0430JUD004831016; *Engels v. Russia*, no. 61919/16, § 33, 23 June 2020, ECLI:CE:ECHR:2020:0623JUD006191916; *Vladimir Kharitonov v. Russia*, no. 10795/14, § 38, 23 June 2020, ECLI:CE:ECHR:2020:0623JUD001079514; *OOO Flavus and Others v. Russia*, no. 12468/15, 23489/15 and 19074/16, § 36-39, 23 June 2020, ECLI:CE:ECHR:2020:0623JUD001246815.

[223] ISPs may be required by court order to end or prevent specific infringements, see Article 12(3) of Directive 2000/31/EC (*Directive on electronic commerce*). In Canada a new proposal for legislation targeting online harms, ISPs are explicitly targeted, see Government of Canada, 'Consultation closed: The Government's proposed approach to address harmful content online - Discussion guide', *Government of Canada,* 29 July 2021, available at canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html (retrieved on 15 February 2022); Government of Canada, 'Consultation closed: The Government's proposed approach to address

services from legal obligations to regulate user-provided information containing illegal or unlawful content directly or indirectly.[224] ISPs in the EU and the US (at least on the state level) are subjected to network neutrality regulations to prevent ISPs from imposing restrictions on what services may use their network.[225] Such net neutrality regulations changes who controls the network. Typically, de provider decides. Network neutrality regulation shifts this to the users. The user of a service and the service provider decide what is requested and transmitted – not the ISP.[226]

ISPs and other internet intermediary services must be distinguished for network neutrality regulation. Network neutrality regulation does not apply to all types of internet intermediary services. Only providers that offer internet access services (ISPs) must adhere to network neutrality regulations.[227] For example, social media platforms do not qualify as access providers and thus are not legally required to uphold network neutrality. The rationality behind this distinction is technological: where ISPs restricting the usage of an internet connection can have severe consequences in terms of user access to internet services, gatekeeping by social media platforms does not have a similar effect. Restrictions imposed by these providers do not extend to the whole

---

harmful content online - Discussion guide - Technical paper', *Government of Canada,* 29 July 2021, available at canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html (retrieved on 15 February 2022). See also, M. Geist, 'Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation', *Michael Geist,* 30 July 2021, available at michaelgeist.ca/2021/07/onlineharmsnonconsult (retrieved on 14 February 2022).

[224] For the EU, see Article 12 and 15 of Directive 2000/31/EC (*Directive on electronic commerce*). For the US, see 47 USCA § 230(c)(1) (West 2018, Westlaw Next through PL 116-91); 17 USCA § 512(a) (West 2010, Westlaw Next through PL 116-179).

[225] For the EU-context see, Article 3 of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, *OJ L 310*, *26.10.2015* (data.europa.eu/eli/reg/2015/2120/oj). In the US, network neutrality was put under pressure by the Trump Administration, see J. Kastrenakes, 'Trump's new FCC chief is Ajit Pai, and he wants to destroy net neutrality', *The Verge,* 23 July 2017, available at theverge.com/2017/1/23/14338522/fcc-chairman-ajit-pai-donald-trump-appointment (retrieved on 15 February 2022). In December 2017, the FCC adopted a policy that largely departed from the core principles of net neutrality J. Kastrenakes, 'The FCC just killed net neutrality', *The Verge,* 14 December 2017, available at theverge.com/2017/12/14/16776154/fcc-net-neutrality-vote-results-rules-repealed (retrieved on 15 February 2022). However, President Biden signed an executive order in July 2021 in which the FCC is asked to restore net neutrality provisions, see R. Lawler & A. Robertson, 'Biden signs executive order targeting right to repair, ISPs, net neutrality, and more', *The Verge,* 9 July 2021, available at theverge.com/2021/7/9/22569869/biden-executive-order-right-to-repair-isps-net-neutrality (retrieved on 15 February 2022).

[226] A. Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, Vol. 24, No. 2, 2018, p. 201.

[227] In the EU, it concerns services "that provides access to the internet, and thereby connectivity to virtually all end points of the internet", see Article 2(2) and 3 of Regulation (EU) 2015/2120. In the US, this is more complicated now an ISP does not necessarily fit in existing definitions. Therefore, the FCC argued that it has the power to classify ISPs under 'telecommunications services' which allows the FCC to impose network neutrality regulation, see K.A. Ruane, 'Net Neutrality: Selected Legal Issues Raised by the FCC's 2015 Open Internet Order', *in* D. Lambert (Ed.) *Net Neutrality and the FCC: Legal Issues and Matters of Debate*, New York, Nova Science Publishers, 2015, pp. 4-10. In 2017 the FCC reclassified ISPs which prohibits the FCC for imposing network neutrality regulation, see Kastrenakes, 2017, 'The FCC just killed net neutrality'. The pendulum, however, may swing back now the FCC is asked to reclassify ISPs as 'telecommunication services', see Lawler & Robertson, 2021, 'Biden signs executive order targeting right to repair, ISPs, net neutrality, and more'. Due to its technical nature and little meaning for content regulation these statutes and regulations will not be discussed at large.

of the internet. Users may still access the service, and the content of the information offered – only not through this specific platform. The user can directly type in this link in the browser and visit the website. ISPs and social media platforms are thus different in this respect. Imposing network neutrality to providers offering social media platform services would be unnecessary. Equally, it would be silly to make an ISP liable as a distributor of illegal content due to their lack of technological control over the actual content of the information transmitted.

The different providers offer functionalities on these different layers, giving them various degrees of control over the content of user-provided information. How providers relate to user-provided information can be best understood by dividing the internet into so-called layers. As Bridy notes, state regulation encourages or discourages providers functioning on these layers from enacting content-based restrictions.[228]

The OSI model and the layers of the internet

Providers both rely on and offer technological functions to the internet. The Open Systems Interconnection (OSI) model helps understand how these providers function by dividing the internet infrastructure into layers. The OSI model distinguishes between seven layers that function independently from each other. Independent means that the different layers do not have access to what happens in the other layers. However, the higher layers do require the existence of the lower layers. Without cables making up the physical layer (Layer 1), no data link layer enables data transmission (Layer 2).[229] Layering offers standardisation which enables all kinds of devices to communicate. The standardisation in layers allows users to choose what devices they connect to the network. Next, this standardisation allows the development of all kinds of applications that use the network.[230]

The seven layers (the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer)[231] do not require an elaborate discussion. A simplified OSI model of three layers suffices to explain the technological capabilities of the different providers regarding user-provided information. Riordan groups the seven layers into the physical, network, and application layers. The physical layer includes all hardware (severs and cables). The network layer includes all computer code that enables computers to communicate and transmit information to other computers. The application layer includes all code related to offering an application service.[232] The user can interact with the service and see the content of the information. In other words, the content of information becomes visible on the application layer.

In the OSI model, there is not one layer that specifically enables regulating the content of user-provided information. Therefore, layering itself does not provide the possibility to impose

---

[228] Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, 2018, p. 205.

[229] Wikipedia, 'OSI model', *Wikipedia,* 15 February 2022, available at en.wikipedia.org/wiki/OSI_model (retrieved on 15 February 2022). When it comes to explaining technology, there is no better resource available than Wikipedia.

[230] J.B. Speta, 'A Common Carrier Approach to Internet Interconnection', *Federal Communications Law Journal*, Vol. 54, No. 2, 2002, pp. 246-247.

[231] Wikipedia, 2022, 'OSI model'.

[232] J. Riordan, *The Liability of Internet Intermediaries*, Oxford, Oxford University Press, 2016, pp. 33-34 and 36-37.

such regulation.[233] While it would be possible to add an independent layer that directly enables content regulation, its effects would be negligible. Since all layers function independently, there is no technological obligation to use such a layer. Technically requiring this layer would cause pre-existing devices and services to lose or break functionalities while limiting newly developed ones to the content regulation layer's capabilities.[234]

With or without a content regulation layer, there will be differences between providers in terms of capabilities in carrying out content-based regulation. Most providers that (can) regulate the content of user-provided information are application layer services. Bridy refers to this layer as the "human-experiential layer" because the application layer is what users see.[235] This concentration of regulation on the application layer is provided by how the internet infrastructure functions. Because providers functioning on the lower layers do not have access to the content of the higher layers, it is technically not feasible to regulate the actual content of the information transmitted on the network layer.[236] For this reason, Balkin argues that the highest layer of the OSI model, the so-called application layer, is the most suitable layer to carry out regulation of user-provided information. Besides, these providers often provide so-called edge services.[237]

These edge services operate (as the name suggests) at the edges of the internet. As understood in this contribution, these edge services are closest to the user. The user understands that the edge service provider offers the service to the user.[238] The edge services are also best-known to different users. Facebook, for example, is a social media network (or platform) functioning at the edge of the internet. Other examples of edge services fitting this definition are Google, Netflix, and Amazon. As noted, defining these edge services is that these services have the most direct contact with the user who uses the service. Consequently, in the users' view, the responsibility for regulating user-provided information lies with the edge service providers.[239] When a user's post is removed on Facebook, nobody suspects that any other provider is responsible for this intervention other than Facebook. Not the hosting service, the payment service, or the ISPs are looked at when user-provided information is regulated, but the platform to which the user provided its information.

---

[233] An so-called 'Identity Layer' that offers the possibility to users to verify their identity could offer some control, see Lessig, 2006, *Code Version 2.0*, pp. 50-52. Riordan adds on top of the OSI model layers an eight layer which contains the actual content in a human readable format: the content layer, see Par. 2.30 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 34.

[234] Lessig, 2006, *Code Version 2.0*, p. 145. Of course, different internet intermediary services may depend on such a layer making it impossible to use this service without such a layer. When I discuss a 'content regulation layer', this may also mean an 'identity layer', since regulation depends on 'who did what where', see Lessig, 2006, *Code Version 2.0*, p. 54. Of course, it would be possible to regulate ISPs to prohibit connections that do not use layers that allow for content regulation.

[235] Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, 2018, p. 205.

[236] Note 119 of Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2037.

[237] Note 119 of Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2037.

[238] This definition does not follow the normal technological definition of edge service.

[239] Note 119 of Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2037; Ruane, 2015, 'Net Neutrality: Selected Legal Issues Raised by the FCC's 2015 Open Internet Order', p. 4. Edge services (or providers) can also be referred to as 'content and application' providers, see Yemini, 'The New Irony of Free Speech', *Columbia Science and Technology Law Review*, 2018, p. 149.

Non-edge services should refrain from imposing content-based restrictions because of the potential collateral effects. As functioning on the network layer service, the ISP does not have direct access to the content of the transmitted information. The actual content of information only shows at the application layer, allowing manipulation of the content.[240] ISPs that engage in content-based regulation violate their technological neutrality and usually restrict complete services. Because of the lack of control over the information and the risk of overregulation, ISPs should maintain neutrality. This concept is also known as the end-to-end principle, meaning that the internet's core should only be preoccupied with transferring bits and bytes. Functional interventions on the information provided to the service should occur at the edge of the internet.[241]

As Bridy puts it, "the core of the network is agnostic about the type of data it carries, and it treats all the data it carries the in same way."[242] The end-to-end principle and the related principle of neutrality allow developers to build all types of services and programmes without requiring the providers that offer these core functionalities of the internet to adjust their services.[243] Of course, the technological design of the internet and the normative propositions underpinning this design are not a given. According to Lessig, the regulatability of the internet could be increased by "complement[ing] the core with technology that adds regulability".[244] However, Lessig feels more for a second option that "regulates applications that connect to the core" and not the core itself.[245] In other words, Lessig argues that regulation should take place on what Lessig refers to as the "application space".[246] These services (comparable with the application layer and edge service providers) have a similar level of control over user-provided information as traditional information intermediaries.[247] The providers functioning on the application layer are, according to Riordan, the most suitable target for regulation. These services "exercise the most direct control over application content."[248] As noted, the providers that offer application layer services often offer their services at the edges of the internet.[249]

There are also non-edge service providers that have technological control over the content of information available on edge services. For example, edge services that do not possess hosting capabilities (required to store information) depend on other providers. While these hosting service providers could be technologically able to control specific instances of information, they do not function as edge services when other providers are dependent on these hosting services. Besides, these hosting services normally do not have a direct relationship with the user that provided the

---

[240] Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, 2018, p. 205.

[241] Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, 2018, p. 199.

[242] Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, 2018, p. 200.

[243] Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, 2018, pp. 200-201.

[244] Lessig, 2006, *Code Version 2.0*, p. 145.

[245] Lessig, 2006, *Code Version 2.0*, p. 145.

[246] Lessig, 2006, *Code Version 2.0*, p. 145.

[247] However, the consequences of removal on intermediary services on the internet more far-reaching than when a traditional intermediary would because removal of content applies to a platform and not just one medium, see Wu, 'Collateral Censorship and the Limits of Intermediary Immunity', *Notre Dame Law Review*, 2011, p. 314.

[248] Par. 2.57 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 40.

[249] Par. 2.34 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 35.

information. The user who uses the service (usually) does not know that the hosting service can technically regulate the content of the information that the user provided to another service operated by another provider. The same is true for so-called caching providers who provide services to speed up access to other services by caching (maintaining copies of the information and software necessary to provide the service) as close to the (potential) user as possible, which increases the availability of the service. While they are technically one of the closest services to the user, they do not qualify as an edge service provider as meant in this paragraph. When functioning as a caching service, the provider of this service depends on the edge provider to provide the information. Like the ISP, the expectation is that a caching provider refrains from content-based regulation.[250] As a rule of thumb, I propose thus that content-based regulation of (user-provided) information should occur on the service that is most recognisable for the user as the regulator.

In sum, the technological dimension of internet intermediary service providers leads to the conclusion that regulation of the content of (user-provided) information should only be enacted on the application layer and at the edge of the internet.[251] Goldman argues that providers that are (legally or functionally) restricted in their available remedies should not be imposed with content-based regulation by regulators since this would likely lead to overregulation.[252] As argued by Balkin, regulating providers on the physical or network layer may have significant adverse effects.[253] Providers offering application layer services are the most suitable targets for content-based regulation of user-provided content.[254] Legislation in the US and the EU reflects this in the legislation enacted to regulate providers: ISPs cannot impose content-based restrictions while application layer services have a much broader discretion.[255] The following paragraph discusses the legal categories used to regulate providers.

---

[250] For example, to remove something from Google's search engine cache part of the (normal) procedure is to first contact the content provider, see Laidlaw, 2015, *Regulating Speech in Cyberspace*, p. 217. Caching services engaging in content regulation may lead to severe freedom of expression rights restrictions since content regulation by caching services normally leads to a termination of services, see Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, pp. 2038-2039. The passive role of caching providers is also reflected in legislation, see for example, Recital 42 and Article 13 of Directive 2000/31/EC (*Directive on electronic commerce*); Van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, 2011, pp. 1462-1463 and 1482; 17 USCA § 512(b) (West 2010, Westlaw Next through PL 116-179).

[251] Basically, both layering and the end-to-end design of the internet seeks to maintain "[…] 'end-to-end' functionality: that application control is remitted to the computers at the ends of the network and the network transmission and inter-networking protocols are kept as simple as possible.", see Speta, 'A Common Carrier Approach to Internet Interconnection', *Federal Communications Law Journal*, 2002, p. 246.

[252] Goldman, 'Content Moderation Remedies', *Michigan Technology Law Review*, 2021, pp. 49-50.

[253] Note 119 of Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2037.

[254] Par. 2.57 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 40.

[255] Bridy, 'Remediating Social Media: A Layer-Conscious Approach', *Boston University Journal of Science and Technology Law*, 2018, p. 209.

1.3.2 Internet intermediaries: the legal dimension

The legal concepts founded in the 1990s[256] and in the early 2000s[257] to address the roles fulfilled by providers may not be fully applicable to the roles fulfilled by providers in the 2020s. For example, the e-Commerce Directive of 2000, harmonising in which circumstances providers may (at least) be exempted from liability for the content of user-provided information in the EU, distinguishes between three separate roles providers can fulfil.[258] In contrast, the general rule of the US liability regime laid down in Section 230 of the Communications Decency Act of 1996 applies to all "interactive computer services",[259] which is much broader than the three roles distinguished in the EU.

None of the legislation mentioned here relies on "internet intermediary" as a legal concept. Nor is there a (legal) definition of internet intermediary to be found in legislation. According to Dinwoodie, concepts such as "interactive computer services" and "hosting service provider" may partly form a 'proxy' for the concept of an internet intermediary.[260] Dinwoodie argues that, as a concept, "internet intermediary" leaves little room to emphasize the differences between different intermediary roles. There is not simply one type of provider. In addition, such terminology neglects that providers may fulfil many different intermediary functions. Because of this multitude of functions, one provider is (potentially) subjected to multiple regulatory and thus liability regimes.[261] As discussed in the introduction of this chapter, this paragraph sees to generic legislation that applies to providers that deal with user-provided information in the broadest sense. Of course, exemptions on this generic legislation exist as a *lex specialis*,[262] as discussed in Chapters 3 and 4 of this dissertation.

Internet intermediary services and the general safe harbour regime of the EU

The e-Commerce Directive relies on the broader "Information Society services", which are 1) "normally provided for remuneration", 2) "at a distance", 3) "by electronic means", and 4) "at the individual request of a recipient of services".[263] Of course, also non-internet intermediary services fall within the definition of "Information Society services".[264] The exemptions from liability for user-provided information for intermediary services laid down in articles 12 (mere conduit), 13

---

256 Of course, the US statutes and the EU directive listed here are updated over time but still rely on concepts originating from the 90's, see 47 USCA § 230 (West 2018, Westlaw Next through PL 116-91); 17 USCA § 512 (West 2010, Westlaw Next through PL 116-179). Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, *OJ L 241*, *17.9.2015* (data.europa.eu/eli/dir/2015/1535/oj).

257 Directive 2000/31/EC (*Directive on electronic commerce*).

258 'Mere conduit', 'caching' and 'hosting', see Article 12 to 14 of Directive 2000/31/EC (*Directive on electronic commerce*).

259 47 USCA § 230(c) and (f) (West 2018, Westlaw Next through PL 116-91).

260 Dinwoodie, 2020, 'Who are Internet Intermediaries?', p. 38 and 41.

261 Dinwoodie, 2020, 'Who are Internet Intermediaries?', pp. 47-48.

262 In the US see, for example, protection of intellectual property law on the internet as laid down in 17 USCA § 512 (West 2010, Westlaw Next through PL 116-179). Intellectual property law is exempted from protection by Section 230, see 47 USCA § 230(e)(2) (West 2018, Westlaw Next through PL 116-91). A similar exemption can be found in the EU, see Recital 65 and Article 17(3) of Directive (EU) 2019/790.

263 Article 1(1)(b) of Directive (EU) 2015/1535.

264 For example, a webshop is not necessarly an internet intermediary service providers.

(caching) and 14 (hosting) read in conjunction with article 15 (the prohibition to impose a general obligation to monitor) of the Directive form the focal point of this discussion.

As noted, many well-known providers perform activities that transcend the three roles of the Directive, which raises the question of whether these activities fall within the safe harbour of the Directive. To recall, in the EU, providers fulfilling one of the three roles distinguished in the Directive can profit from a 'safe harbour' which shields the intermediary from liability for information provided or requested by a user as long as they fulfil a set of criteria. These criteria thus vary between the different intermediary roles.[265] Unlike mere conduit and caching providers, hosting service providers can regulate user-provided information by permanently removing or restricting access to information. In debates over increased regulation of providers, this mainly concerns hosting service providers. As the EC notes, "[i]llegal content on online platforms can proliferate especially through online services that allow upload of third party content."[266] In a later recommendation, the EC emphasised that "[p]roviders of hosting services play a particularly important role in tackling illegal content online, as they store information provided by and at the request of their users and give other users access thereto, often on a large scale."[267]

The safe harbours offered by the Directive are not absolute – they only apply to providers of intermediary services that fit the definition and uphold the requirements regarding user-provided information. For hosting services, this requirement is that "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".[268] When the provider gains knowledge of or becomes aware of the illegal or unlawful content of the user-provided information, then the provider must "acts expeditiously to remove or to disable access to the information".[269] These requirements will be discussed more extensively in Chapter 4. For now, it is sufficient to note that the safe harbour does not apply to providers that 1) have knowledge/awareness of the illegal or unlawful content of user-provided information and 2) do not act expeditiously to disable access to this information. Article 14 only applies to "an information society service is provided that consists of the storage of information provided by a recipient of the service".[270] For mere conduit services ("transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network")[271] and caching services ("consists of the transmission in a communication network of information provided by a recipient of the service")[272] different requirements apply.

It is not easy to demarcate between the different roles – both factually and legally. For example, the ECJ in 2010 confused scholars and providers with its *Google France* ruling. The ECJ ruled that hosting services cannot rely on the safe harbour when they are not "neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or

---

[265] Articles 12 to 14 of Directive 2000/31/EC (*Directive on electronic commerce*).

[266] Communication COM(2017)555 final, p. 4.

[267] Recital 15 of Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, *OJ L 63*, *6.3.2018* (data.europa.eu/eli/reco/2018/334/oj).

[268] Article 14(1)(a) of Directive 2000/31/EC (*Directive on electronic commerce*).

[269] Article 14(1)(b) of Directive 2000/31/EC (*Directive on electronic commerce*).

[270] Article 14(1) of Directive 2000/31/EC (*Directive on electronic commerce*).

[271] Article 12(1) of Directive 2000/31/EC (*Directive on electronic commerce*).

[272] Article 13(1) of Directive 2000/31/EC (*Directive on electronic commerce*).

control of the data which it stores."[273] The ECJ seems to suggest that hosting services could only rely on the safe harbour of Article 14 as long it has no involvement in the content of user-provided information. Unfeasible for providers that are often involved in user-provided information. This involvement, for example, exists in offering recommendations of user-provided information with content that may interest the user. As Van Eecke observes, Recital 42 of the Directive caused this confusion because its wording suggests that the requirement of a "mere technical, automatic and passive nature" also applies to hosting services. Such an interpretation would obscure between mere conduit, caching, and hosting service. For hosting services, the bar would be raised to rely on the safe harbour. Van Eecke does not view such a criterion as viable now, "hosting providers will almost necessarily have some degree of involvement with their users."[274] Hosting service providers that offer the possibility for users to upload user content or social networking functionalities to encounter and interact with information from other users go beyond such a "mere technical, automatic and passive nature".[275]

The ECJ clarified in *L'Oréal v. eBay* that only providers that, due to their active role, gain "knowledge of, or control over, the data"[276] lose protection under Article 14. While this would strengthen the safe harbour, this does not resolve the so-called "Good Samaritan-paradox".[277] This paradox expresses that providers of internet intermediary services are discouraged from engaging in voluntary moderation of information with illegal content because this may be too active to rely on the safe harbour laid down in Article 14 of the Directive. Providers may fear that they would gain knowledge of or control over the illegal content they failed to moderate.[278]

While the EC emphasized that voluntary monitoring would not cause providers of hosting services to lose their safe harbour, the EC argued that "in such cases the online platform continues to have the possibility to act expeditiously to remove or to disable access to the information in question upon obtaining such knowledge or awareness."[279] The EC tries to assure hosting service providers that they ought not to worry about liability resulting from moderation out of their own initiative. This assurance, according to Kuczerawy, is "somewhat confusing and perhaps even misleading"[280] since "the EC attempts to convince hosting providers that they will not lose the protection – as long as they act according to the expectations of policy makers."[281] The lack of "Good Samaritan"-protections combined with the request of the EC to proactively take down user-provided information with illegal or unlawful content forces providers to choose between passivity or an active approach accompanied by perfect moderation.

---

[273] Judgement of the Court (Grand Chamber) of 23 March 2010 in *C-236/08, C-237/08 and C-238/08, Google France SARL and Google Inc. v. Louis Vuitton Malletier SA*, ECLI:EU:C:2010:159, in particular Rec. 114.

[274] Van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, 2011, pp. 1482-1483.

[275] Van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, 2011, pp. 1482-1483.

[276] Judgement of the Court (Grand Chamber) in *C-324/09* (*L'Oréal v. eBay*), in particular Rec. 116.

[277] Van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, 2011, pp. 1483-1484.

[278] Kuczerawy, 2018, 'The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?'; Van Hoboken & Keller, 2019, 'Design Principles for Intermediary Liability Laws', p. 8.

[279] Communication COM(2017)555 final, p. 12.

[280] Kuczerawy, 2018, 'The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?'.

[281] Kuczerawy, 2018, 'The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?'.

In sum, the EU framing of providers of internet intermediary services in the e-Commerce Directive is highly ambivalent. The Directive suggests that hosting service providers should keep their distance from the content of user-provided information to count on the safe harbour as an internet intermediary. On the other hand, the EC encourages providers to actively moderate illegal, unlawful, and even harmful information. While the EC signals that providers ought not to worry about liability for moderation as long as they remove information with illegal or unlawful content,[282] the EU regime does not offer an exemption for liability from under- and over-removal. Providers may become liable for information with illegal content they accidentally fail to remove. Besides, the e-Commerce Directive does not offer a safe harbour for user claims against the removal of content that is not unlawful.[283]

Internet intermediaries in the US: the general rule of immunity

In contrast to the EU approach, Section 230 does not distinguish between different services – all providers that offer interactive computer services can rely on the immunities provided under this section. The definition of interactive computer service is

> any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.[284]

All kinds of services that make use of the internet are thus considered interactive computer services by the US courts, including hosting services, internet marketplaces, and dating websites.[285] Providers of intermediary services that fall within this definition, according to Section 230(c)(1), can "not be treated as the publisher or speaker of any information provided by another information content provider."[286] Wilman characterises the protection offered by Section 230 as "extreme" but not as absolute since there are exceptions made to the statute and case law.[287] Chapter 3 of this dissertation discusses the exceptions.

Next to Section 230(c)(1) exempting providers from liability for user-provided information, Section 230(c)(2)(A) offers protection to providers that actively intervene in the

---

[282] See, for example, European Commission, 2021, 'Code of Practice on Disinformation'; European Commission, 2016, 'Code of Conduct on Countering Illegal Hate Speech Online'.

[283] Klos, "Wrongful moderation': Aansprakelijkheid van internetplatforms voor het beperken van de vrijheid van meningsuiting van gebruikers', *Nederlands Juristenblad*, 2020/2976; Van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, 2011, pp. 1467-1468; Kuczerawy, 2018, 'The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?'.

[284] 47 USCA § 230(f)(2) (West 2018, Westlaw Next through PL 116-91).

[285] Holland, 'In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism', *University of Kansas Law Review*, 2008, pp. 374-375; Gillespie, 2018, *Custodians of the Internet*, p. 34.

[286] 47 USCA § 230(c)(1) (West 2018, Westlaw Next through PL 116-91).

[287] Par. 6.41 of Wilman, 2020, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*, p. 187.

content provided by their users.[288] Section 230(c)(2)(A) reads that "[n]o provider or user of an interactive computer service shall be held liable on account of"[289]

> 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;[290]

As Goldman notes, it is rare for providers of internet intermediary services to rely on Section 230(c)(2)(A) since it does not offer similar far-reaching protections as Section 230(c)(1). Goldman argues that providers also can rely on their terms of service, which allows them to intervene in user-provided information.[291] In addition, as discussed in the third chapter, the 'free speech clause' of the First Amendment also extends to providers that make editorial decisions regarding user-provided information.[292] However, it could be argued that Section 230(c)(2)(A) may offer protection for civil liability when a provider fails to remove content excluded from Section 230 protection, such as sex trafficking advertisements.[293] Goldman, however, questions whether this argument would hold up in court.[294] Section 230(c)(2)(A), however, reveals the legislator's view of providers as providers that make far-reaching decisions in what user-provided information they do and do not permit on their service.

Evaluation: EU versus the US approach

The approaches in the US and the EU know fundamental differences. Internet intermediaries are 'framed' in legal definitions which have legal meaning. Because the safe harbours and immunities provided by legislation link to the legal definitions, providers may ensure they fall within these legal categories. Altering these definitions may cause internet intermediary providers to change their conduct. Ultimately, this may have consequences for what users may and may not do on their services. The same, of course, is valid for the immunities and safe harbours offered to these categories of providers.

The US chose to keep it simple and only defined one category of internet intermediary services in their generic legislation. Providers that offer an "interactive computer service" can rely on the protection of Section 230(c)(1), which offers immunity for liability as a publisher or speaker for user-provided information. As long as a provider is not "responsible, in whole or in part, for the creation or development of information"[295] offered to the service, Section 230(c)(1) offers

---

[288] 47 USCA § 230(c) (West 2018, Westlaw Next through PL 116-91). The goal of Section 230 was to encourage internet intermediaries to set standards themselves, see Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, pp. 64-66. Section 230, thus, does not require internet intermediaries to be 'neutral' towards the content users provided to them, see Gillespie, 2018, *Custodians of the Internet*, pp. 30-31; E. Harmon, 'No, Section 230 Does Not Require Platforms to Be "Neutral"', *Electronic Frontier Foundation,* 12 April 2018, available at eff.org/deeplinks/2018/04/no-section-230-does-not-require-platforms-be-neutral (retrieved on 15 February 2022).

[289] 47 USCA § 230(c)(2) (West 2018, Westlaw Next through PL 116-91).

[290] 47 USCA § 230(c)(2)(A) (West 2018, Westlaw Next through PL 116-91).

[291] Goldman, 2020, 'An Overview of the United States' Section 230 Internet Immunity', p. 160.

[292] In contrast, 'must-carry' rules prohibiting removal of content are considered unconstitutional, see Keller, 2019, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech', pp. 2 and 9-12.

[293] 47 USCA § 230(e)(5) (West 2018, Westlaw Next through PL 116-91).

[294] Goldman, 'The Complicated Story of FOSTA and Section 230', *First Amendment Law Review*, 2019, p. 283.

[295] 47 USCA § 230(f)(3) (West 2018, Westlaw Next through PL 116-91).

protection for liability for user-provided information.[296] Chapter 3 discusses the specific criteria. For now, it is sufficient to conclude that providers that offer an interactive computer service may rely on Section 230, which protects a (very) broad range of internet intermediary activities.

As noted, the EU e-Commerce Directive relies on the broader definition of "Information Society services".[297] While this comes close to an interactive computer service defined in the US, the EU distinguished between three roles these Information Society services could fulfil. Although the Directive does not define what an intermediary is, the Directive places these three roles under the subheading "Liability of intermediary service providers"'[298] Section 230, unlike the e-Commerce Directive, does not distinguish between mere conduit, caching, and hosting services. Section 230(c)(1) and (2) could also apply to non-hosting services (for example, an ISP that offers filtering of harmful websites on behalf of the user but mistakenly over blocks websites). The majority of the issues discussed here, however, concern interactive computer services that involve hosting. While the usability of the immunities provided under Section 230 may differ amongst different services, the general US approach toward internet intermediary liability gives one definition, including all different internet intermediary functions.[299] This difference in scope is not of concern for this dissertation. The following chapters mainly focus on providers that involve hosting user-provided information.

There is uncertainty over how active a hosting service may get under the e-Commerce Directive. The rule laid down in Section 230 perceives interactive computer services not as "mere technical, automatic and passive"[300] providers but as (potentially) actively involved in the content of user-provided information. As noted, Section 230 offers protection for 'Good Samaritan' moderation of user-provided information while the e-Commerce Directive does not.[301] While the Directive stimulates hosting services providers to take down user-provided information after they become aware of its illegal content, it discourages intermediaries from engaging in content moderation themselves. The ECJ requires hosting service providers not to become too involved when they wish to rely on the safe harbour of Article 14.[302] Hosting providers must prevent gaining

---

[296] During my PhD-project following twitter account of EU and US legal scholars was very helpful. In some cases, they would 'retweet' content provided by other users. Which means that they would share content that other users posted on twitter. In a way these twitter accounts functioned as an intermediary between those users and me.

[297] Article 1(1)(b) of Directive (EU) 2015/1535.

[298] See Section 4 of Directive 2000/31/EC (*Directive on electronic commerce*).

[299] Of course, this may be different in statutes that see to a specific category of content, see 17 USCA § 512(a), (b), and (c) (West 2010, Westlaw Next through PL 116-179).

[300] Judgement of the Court (Grand Chamber) in *C-236/08, C-237/08 and C-238/08* (*Google France*), in particular Rec. 114.

[301] Van Eecke, 'Online service providers and liability: A plea for a balanced approach', *Common Market Law Review*, 2011, pp. 1483-1484.

[302] In *Google France* the ECJ argued that:

> in order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.

see Judgement of the Court (Grand Chamber) in *C-236/08, C-237/08 and C-238/08* (*Google France*), in particular Rec. 114. A year later in *L'Oréal v. eBay* the ECJ adopted the similar but slightly changed criteria that in that when:

control or knowledge of the content of user-provided information to rely on the safe harbour. In the EU, passive hosting service providers may rely on the safe harbour offered by Article 14. At the same time, providers that are too active may lose safe harbour protection. While this passive/active distinction may be more a dichotomy than a clear distinction, it is not beforehand clear when an internet intermediary becomes too active. Providers, however, may be active on one part of their service and more passive on other parts. Providers may rely on the safe harbour for the passive parts while forfeiting this right for other parts of the service on which they became too active.[303]

Section 230 and the e-Commerce Directive codify different expectations legislators have of providers of internet intermediary services. The EU in the Directive seems to assume that internet intermediaries have minimal involvement with user-provided content. While the Directive does not prohibit active involvement of hosting services in user-provided information, they may lose their safe harbours protection which offers a powerful incentive to not moderate.[304] The argument could be made that forfeiting the safe harbour does not mean that the provider no longer qualifies as a provider.[305] Service providers, however, are often dependent on safe harbours to prevent legal liability for user-provided information. Since the safe harbour of the Directive is tied to some passivity, this suggests that providers are not expected to become active towards user-provided information. As noted, this is different in the context of Section 230, which left open how active moderation of user-provided information could be by offering exemptions for liability arising from moderation but also from not moderating.[306]

However, Section 230 and the Directive are not so different regarding their expectation of providers of internet intermediary services with respect to filtering out illegal or unlawful content before publication. While the expectations were not made explicit,[307] Section 230(c)(1) does not require a provider to review all user-provided information before admission. Without Section 230, the fear exists that providers would overregulate user-provided information or cease to moderate out of fear of liability.[308] Some services even may close services out of fear of liability.[309] Of course, these fears are not without critics arguing that Section 230 immunities may be too overstretched

---

> the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale.

see Judgement of the Court (Grand Chamber) in *C-324/09* (*L'Oréal v. eBay*), in particular Rec. 116.

303 J. van Hoboken, et al., *Hosting intermediary services and illegal content online: An analysis of the scope of article 14 ECD in light of developments in the online service landscape*, Luxembourg, Publications Office of the EU, 2018, doi:10.2759/284542, pp. 7, 14 and 31-36.

304 Article 14 of Directive 2000/31/EC (*Directive on electronic commerce*).

305 The provider still qualifies as an "Information Society service".

306 Kosseff, 2019, *The Twenty-Six Words That Created the Internet*, pp. 64-66.

307 Gillespie, 2018, *Custodians of the Internet*, pp. 43-44. See also, on the question whether Section 230 (should) protect 'bad actors' or 'Bad Samaritans', see Citron & Wittes, 'The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity', *Fordham Law Review*, 2017, pp. 416-417.

308 Gillespie, 2018, *Custodians of the Internet*, p. 43.

309 Goldman, 'The Complicated Story of FOSTA and Section 230', *First Amendment Law Review*, 2019, pp. 288-289.

to include bad actors, antitrust conduct, and (potential) avoidance of other legislation.[310] Chapter 5 discusses these criticisms. For now, it is sufficient to state that Section 230 assumes that internet intermediaries may engage in content moderation and does not require them to do so.

As Wilman notes, there is no active encouragement for providers offering interactive computer services to engage in content moderation by offering a safe harbour for moderation decisions. As Wilman puts it, "Section 230(c)(2) principally only removes a potential disincentive for intermediaries to do so."[311] However, incentivising providers to remove content could run into constitutional (in the EU) or human rights issues (both the EU and the US) – especially in the US. According to Keller, this is already the case when the legislation would "foreseeably cause platforms to restrict legal speech".[312] While the encouragement does not consist of a carrot or a stick, it is the best the US legislator could do to offer a moderation-friendly environment for providers of internet intermediary services.

Section 230 presupposes that a provider of an internet intermediary service is not in the position to take full responsibility for all content of user-provided information. However, they can moderate unrestrained behaviour by taking measures against user-provided information with illegal or undesirable content. Section 230 protects providers against liability for user-provided information with only a few exemptions. The e-Commerce Directive has a similar view on internet intermediary services. Like Section 230, the Directive protects providers from the requirement to proactively screen for illegal and unlawful content.[313] The EU approach diverges from Section 230 by making the liability of hosting service providers conditional to having "actual knowledge of illegal activity or information" or being "aware of facts or circumstances from which the illegal activity or information is apparent".[314] While not expressed in Article 14, the expectation codified in the Directive is that hosting services do not have knowledge or awareness of user content by default. Knowledge or awareness is the exception. As the case law of the ECJ shows, hosting services providers are expected to uphold some passivity towards user information to rely on safe harbours.[315] A different explanation in which knowledge and awareness would be the default would render the safe harbour provided by Article 14 useless.

As discussed in the following paragraph, providers fulfil a broad range of intermediary roles and functions on the internet. How these different approaches work out for these providers and their users are discussed in Chapters 3 and 4. The definitions and categories used to define internet intermediary roles codify the policy assumptions in the different intermediary roles. The US and EU approaches are similar in the expectation that internet intermediaries were (and are) not able to check all the content of the information provided and requested by users beforehand. The US and the EU consider that internet intermediary activities are different from traditional intermediary activities in volume. However, how service providers should deal with this user

---

310 For example, Gillespie, 2018, *Custodians of the Internet*, pp. 43-44; Citron & Wittes, 'The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity', *Fordham Law Review*, 2017, pp. 419-423; Pasquale, 'Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power', *Theoretical Inquiries in Law*, 2016, pp. 494-496.

311 Par. 4.41 of Wilman, 2020, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*, p. 115.

312 Keller, 2021, 'Six Constitutional Hurdles for Platform Speech Regulation'.

313 Article 15 of Directive 2000/31/EC (*Directive on electronic commerce*).

314 Article 14(1)(a) of Directive 2000/31/EC (*Directive on electronic commerce*).

315 See Judgement of the Court (Grand Chamber) in *C-236/08, C-237/08 and C-238/08* (*Google France*), in particular Rec. 114; Judgement of the Court (Grand Chamber) in *C-324/09* (*L'Oréal v. eBay*), in particular Rec. 116.

content is different. While the US approach is to take away the legal hurdles to not disincentivise providers to become active, the EU e-Commerce Directive codifies the assumption that providers, as a rule, do not have knowledge or awareness of the content provided by their users and thus have a passive relationship with user-provided information. Noteworthy is that the legislation and its interpretation by the ECJ are different from the policy articulated by the EC. In the proposal of the DSA in December 2020, the EC seeks to codify its policy that providers are encouraged to moderate.[316] The DSA proposal also includes a legal definition of 'internet intermediary'.[317] However, as discussed in Paragraph 4.3, this does not change what is expected from providers.

1.3.3 Internet intermediaries: the functional dimension

The concept 'internet intermediary' covers many companies, functions, and activities. As mentioned, it is not always easy to distinguish a company from its intermediary roles and its specific functioning and activities. Intertwining different intermediary functions and non-intermediary activities makes it difficult to consider when a provider functions as an internet intermediary service. Besides, different intermediary functions are governed by different (legislative) norms, as mentioned above. Neither the technological nor de legal dimension provides the whole picture of how internet intermediary services providers relate to user-provided information. The technological dimension only sets out the technological possibilities of providers. The legal dimension complements this by setting out what intermediary roles are regulated and what legal obligations providers have regarding the services they offer. Neither of these dimensions sets out what providers of intermediary services functionally do. The technological dimension clarifies what providers *can*, while the legal dimension sets the boundaries for the legal liability of providers for user-provided information. Therefore, this paragraph offers a functional approach by distinguishing different internet intermediary roles and functions and setting out different intermediary activities.[318]

As with the previous paragraph, the focus lies on regulating user-provided information either by providers or by the state through providers. All providers of internet intermediary services have a level of control over user-provided information and thus could intervene in what, how, and when specific content is allowed. In setting out how different services relate to user-provided information, Balkin distinguishes between three intermediary functions. These functions lead to varying degrees of control, involvement, and legal and technological possibilities to regulate what their users may or may not do their services. Balkin distinguishes between basic internet services, payment services and content curators.[319] Balkin's approach complements and forms an alternative to the two technological approaches discussed in paragraph 1.3.1.[320] As noted above, internet content regulation should only take place on the application layer at the edges of the internet. Besides, only providers that offer hosting services fit the legal categories expected to intervene in user-provided information directly. Balkin's classification of internet intermediary services in "basic internet services", "payment services", and "content curators" serve as a

316 Commission Proposal COM(2020) 825 final (*Digital Services Act*).

317 Dinwoodie, 2020, 'Who are Internet Intermediaries?', pp. 38-39.

318 See, for the functional approach of the EU, Par. 2.35 of Wilman, 2020, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*, p. 26.

319 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2038.

320 Note 119 of Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2037.

framework to understand how the internet intermediary service that is offered relates to technological control and legal responsibilities.[321]

While sometimes internet content regulation is technically possible and legally allowed, some providers should refrain from regulating user-provided information because of the character of the service they offer. Balkin, for example, argues that e-mail providers should remain neutral and non-discriminatory with respect to the information sent and received by their users.[322] Grouping intermediaries based on their functional involvement with information helps to understand and discuss (new proposals for) regulation for intermediary liability for user-provided information with illegal or unlawful content.[323] Besides, differentiating between the intermediary roles contributes to understanding the regulatory capabilities of intermediaries with respect to internet content irrespective of technological and legal constraints.

Basic internet services

As discussed, internet content regulation normally takes place on the application layer. The application layer offers the possibility to manipulate the content of the information as shown to the users.[324] The application layer is also the most visible layer for users regarding what service is responsible for interventions on user-provided information. When something happens to an account of specific information provided by the user, the application layer service is often the first point of contact. The application layer is the most visible layer for users. Every internet user can name a few platforms (social media, media sharing platforms). Everyone with an internet connection uses gateways (search engines) to find information. When placing an order on their favourite web shop, a transaction network (payment provider) is used to make the payment.[325]

In contrast, the physical and network layers are usually invisible to users. A user does not see how a server in a data centre on the other side of the world transfers information through a patchwork of cables and internet nodes. A user usually lacks awareness of the domain controllers translating readable website addresses into numbers pointing to the correct (physical) computer. The user typically does not notice that a hosting service hosts a website. The only times a user actively thinks about the ISP is when the monthly bill is due or when the internet connectivity malfunctions. Users of internet intermediary services would not think to address these services when confronted with user-provided information that is removed or made inaccessible.

The most invisible group of internet intermediary services, what Balkin calls basic internet services, form the technical infrastructure of the internet. According to Balkin, hosting, telecommunication, domain name, and caching and defence services are basic internet services.[326] Riordan adds cloud services and certificate authorities to this list.[327] Hosting services are services that consist of hosting the data that is required for other services to function. Telecommunication services are services such as ISPs that provide access to the internet. Domain name services offer a service that consists of registering (such as universiteitleiden.nl) and resolving domain names. Domain names allow users to enter user-friendly addresses in their browsers that point to the

---

321 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2038.

322 Note 119 of Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2037.

323 Par. 2.40-2.43 of Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 36-37.

324 Par. 2.29-2.30 and 2.40-2.43 of Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 34 and 36-37.

325 Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 40-46.

326 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2038.

327 Par. 2.46-2.56 of Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 38-40.

website's location. Caching and defence services provide a faster connection, availability, and security features.[328] Certificate authorities function as the notaries of the internet: they issue certificates that confirm that the connection between the user's computer and the server is secured.[329] Cloud services partly overlap with hosting but add other computing services such as caching and defence functionalities to their service.[330] Cloud services can optimise the availability of websites or applications hosted elsewhere.[331] One of the most well-known caching and defence services, Cloudflare, has 'cloud' in its name for a reason.[332] Cloud services are examples of services that may provide network and application layer functionalities.[333]

A provider offering hosting services must not engage in content regulation by making decisions about what is not allowed on the hosting service. Especially when it comes to user-provided information stored on the service by another provider, the hosting service provider should refrain from extensive moderation. An ISP, in its turn, must not engage by itself in filtering instances of information or restricting access to services because of the information available on these services.[334] As noted, regulation of user-provided information on the physical and network layer tends to lead to overregulation because of the lack of control of the providers active on these layers.[335] Unplugging a server might mean that hundred or even thousands of websites are unplugged in the process. Completely blocking a service because of the availability of information with illegal or unlawful content also blocks access to the available legal information. Taking down a whole server or website may only be suitable when it dedicates itself exclusively to information with illegal or unlawful content such as sexual child abuse imagery. Interventions on the physical or network layer are not a suitable option when the aim is to take down one post or a few images on a host that generally provides services for user-provided information with legal content.[336]

While basic internet services should remain neutral regarding the information offered to or through them, Balkin makes an exception for one type of service: domain name services. A domain name must be unique for the system to function. For example, universiteitleiden.nl cannot be registered by two parties at the same time because users would never know on which website they would end up. Neutrality resulting in two users registering the same domain name for their website would mean chaos. Domain name controllers, according to Balkin, should, however, remain neutral with respect to the usage of the domain name.[337] Domain name controllers, thus,

---

328 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2038.

329 Par. 2.56 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 40.

330 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2038.

331 Par. 2.51 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 39.

332 See, cloudflare.com.

333 Par. 2.51 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 39.

334 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, pp. 2038-2039.

335 Par. 2.45 and 2.48 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 38.

336 See, again, For example by the ECtHR, see *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 66, ECHR 2012-VI, 18 December 2012; *Cengiz and Others v. Turkey*, no. 48226/10 and 14027/11, § 64, ECHR 2015-VIII, 1 December 2015; *Kablis v. Russia*, no. 48310/16 and 59663/17, § 94, 30 April 2019; *Engels v. Russia*, no. 61919/16, § 33, 23 June 2020; *Vladimir Kharitonov v. Russia*, no. 10795/14, § 38, 23 June 2020; *OOO Flavus and Others v. Russia*, no. 12468/15, 23489/15 and 19074/16, § 36-39, 23 June 2020.

337 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, pp. 2038-2039.

should not refrain from offering services because of the content of information that is made available on or through the service that uses the domain name.[338]

In sum, regulation of the physical and network layer can both lead to overregulation. While the providers that offer the physical and network layer services *can,* they *should not* regulate user-provided information. The difference with internet content regulation on the application layer is that physical and network layer services that regulate user-provided information tend to block entire services, not specific information with illegal or unlawful content.

Payment services

Besides basic internet services, Balkin distinguishes between payment services and content curators.[339] In the taxonomy provided by Riordan, payment services and content curators both function on the application layer.[340]

Payment services are exceptional since, as Balkin notes, "payment systems are not, strictly speaking, layers of internet traffic".[341] There is not an internet layer that deals with payment. Monetary transactions, offline and online, are subjected to other types of regulation.[342] Riordan views payment systems as a subclass of marketplaces on the application layer. Riordan subdivides marketplaces into internet marketplaces (including online marketplaces such as eBay, ticket portals, 'retail emporia' such as Amazon, and app stores) and transaction networks.[343] The last category, transaction networks, is what Balkin seems to have in mind when referring to payment providers. Transaction networks, according to Riordan, encompass "the services and software with which value is transferred between internet users."[344] Riordan counts, for example, card issuers and payment networks (such as Mastercard), online payment systems (for such as PayPal) and micropayment providers to transaction networks.[345]

Technically speaking, payment systems function in the application space and form a clear example of an edge service. When a payment system refuses a user to create an account to make or receive payments or rejects a payment, it is often transparent what provider is responsible for this rejection. Due to their role, there are good reasons to require prudence from payment services regarding internet content regulation.

Payment systems may even be (one of the most) potent internet content regulators.[346] With the help of these payment systems, an internet marketplace can verify the domicile of a customer

---

338 In the past, for example, GoDaddy which also offers domain name controller services, refused to offer services to Gab and the Daily Stormer, see S. Byford, 'Gab.com goes down after GoDaddy threatens to pull domain', *The Verge,* 28 October 2018, available at theverge.com/2018/10/28/18036520/gab-down-godaddy-domain-blocked (retrieved on 14 February 2022); T. Ong, 'Neo-nazi site Daily Stormer threatened by hosting providers and possible hackers', *The Verge,* 14 August 2017, available at theverge.com/2017/8/14/16142384/daily-stormer-site-go-daddy-hosting-providers-hackers-anonymous (retrieved on 15 February 2022).

339 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2038.

340 Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 40-42 and 44-46.

341 Note 119 of Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2037.

342 Par. 2.85 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 45.

343 Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 44-46.

344 Par. 2.83 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 45.

345 Par. 2.84 of Riordan, 2016, *The Liability of Internet Intermediaries*, p. 45.

346 PayPal, for example, banned accounts related to Trump after the US Capitol was invaded by his supporters, see L. Hautala, 'PayPal and Shopify remove Trump-related accounts, citing policies against supporting violence', *cnet,* 7 April 2021, available at cnet.com/news/paypal-and-shopify-remove-trump-related-accounts-citing-policies-against-supporting-violence (retrieved on 15 February 2022).

or prevent the shipment of goods that are legal in one jurisdiction to a jurisdiction that does not allow these goods. On the other end, customers can profit from payment systems that verify the trustworthiness of an internet marketplace, expecting that payment systems cease services to malicious actors. However, the usage of these regulatory capabilities can also combat forbidden sales or other illegal transactions.[347]

Considering the role of payment systems, Balkin argues that they should refrain from content regulation with only a few exceptions.[348] Payment systems have an enormous potential to influence the exercise of freedom of expression rights. What if a payment system bars transactions to perfectly legal websites because the content is deemed indecent or undesirable by the payment service provider? Balkin, therefore, concludes that payment services must not impose regulations on other providers on what is allowed by refusing payments.[349] Balkin argues that payment systems should only be allowed to intervene when the usage of their services facilitates illegal transactions or other conduct that violates criminal law.[350]

Content curators

The third group of service providers, content curators, are different. Content curators, according to Balkin, "act as curators and personalizers, they cannot really avoid making decisions about content."[351] Neutrality, thus, is not a feasible and even a silly standard for providers of such intermediary services. A lack of neutrality is what characterises content curators. Curation, as noted, encompasses activities that see to "[s]elect, organize, and present (online content, merchandise, information, etc.), typically using professional or expert knowledge."[352] Curation, thus, involves decisions about what information is shown to who, where, and when based on its content.

Balkin groups search engines and social media platforms under content curators that make decisions regarding user-provided information. According to Balkin, search engines and social media platforms perform three functions: firstly, they enable the public to participate. Secondly, content curators organise the public debate. Without search engines and social media platforms, it would be harder to participate in the public debate, and it would be much harder to find information. A third function, according to Balkin, is that search engines and social media platforms, as content curators, offer curation of public opinions. For example, both search engines and social media platforms may offer personalisation of information based on its content.[353] Balkin, however, also includes content moderation in this broad definition of content curation by pointing out that community guidelines allow content curators to enforce norms to safeguard a civil discussion.[354]

Both curation and moderation are application layer activities. Search engines (as gateways), for example, may personalise the results of their users. Internet marketplaces could learn what

---

347 Par. 2.86 of Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 45-46.
348 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2039.
349 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2039.
350 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2039.
351 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2041.
352 Lexico, 'Meaning of curate in English'.
353 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2041.
354 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2041.

their users buy and recommend new products or advertisements to their users.[355] Regarding content moderation, online platforms and marketplaces (allowing third-party sellers) seem to stand out: they can best decide what is allowed and what is not and are often legally required to do so.[356] Technically, there is little reason to assume that only application layer providers engage in content moderation. Content-based interventions are possible when there is technological control over the application layer.

A functional approach toward internet intermediary service providers

The expectation is that providers that offer platform and gateway functionalities engage in content curation.[357] Next to these two functionalities, the expectation exists that providers that function as an internet marketplace are involved in the content of user-provided information.[358] In contrast, providers that offer transaction networks (or payment services) carrying out content-related interventions pose a risk similar to content-based interventions by basic internet services. Like basic internet services, payment services are 1) unmissable and 2) more likely to impose restrictions on a service or account level.[359]

Large internet companies usually do not limit themselves to one intermediary function. For example, Amazon, Apple, and Google offer services within multiple groups. Google and Amazon both offer cloud services.[360] Amazon, Apple, and Google all three offer payment services,[361] and all these providers engage in content curation on a multitude of different platforms.[362] Sometimes these functionalities provided by services are related to each other (all online platforms rely on hosting services). These services are not necessarily related to each other, such as payment services. A provider may offer a payment service for users in and outside its ecosystem. The payment service provider may restrict its usage by setting standards on what goods and services can be purchased. The payment service is no longer just an ancillary functionality; it becomes a stand-alone service forming new points of regulation.

A functional approach thus requires reviewing what functions are ancillary to the provider's primary service. For example, in the case of a social media platform, hosting is a necessary but subordinate function to social media networking functions. Hosting is unmissable for social media platforms, but it becomes obsolete when the provider cancels its social networking functions. Restricting providers of social media platforms from curating or moderating because they also fulfil a basic internet service role would be too strict. The opposite is true for payment services used by services offered by the same provider and outside the service. In the latter case, content-based regulation through payment services also leads to the regulation of information on services other services than those offered by the provider.

The functional approach thus requires uncovering how intermediary functions relate to each other. Providers that offer a service fulfilling a subordinate function and have little direct involvement in the content of user-provided information offered on or to other services must

---

355 Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 40 and 43-46.

356 Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 40-44.

357 Balkin, 'Free Speech is a Triangle', *Columbia Law Review*, 2018, p. 2041.

358 Par. 2.78-2.82 of Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 44-45.

359 Par. 2.85-2.86 of Riordan, 2016, *The Liability of Internet Intermediaries*, pp. 45-46.

360 See cloud.google.com and aws.amazon.com.

361 See pay.amazon.com, apple.com/apple-pay, and pay.google.com/about.

362 See amazon.com, apple.com/app-store, play.google.com.

refrain from content-based regulation. They are functionally not the designated service providers to engage in such moderation. However, this does not mean that these providers are always technically incapable or have no legal obligations to engage in such moderation.

Conclusion

As Dinwoodie noted, terminology such as "internet intermediary" offers little precision.[363] As discussed in this chapter, providers differ in terms of their technological capabilities, legal obligations, and functional involvement regarding the content of user-provided information. According to Dinwoodie, alternative terminology such as "online service provider" and "internet service provider" may be more suitable to describe the actors that function as internet intermediaries.[364] In this chapter, I distinguished between the provider of an intermediary service, the internet intermediary service provided, and the specific activities, roles, and functions these providers may fulfil. Unlike catch-all terminology such as "internet intermediary", this distinction in provider, service and activities allows discriminating between the different roles the providers fulfil. As noted, providers may be active in content moderation on one part of their service while remaining passive on other parts. In addition, providers may provide services that are passive per se due to their technological nature or legal responsibilities. A provider offering e-mail and social networking services is potentially subject to different (legal) norms. While providers of internet intermediary services can vastly differ from traditional information intermediaries, they could also be remarkably similar in terms of control. Providers thus could differ extensively from each other in terms of control over user-provided information. Even one provider offering two different services may have various levels of control over the content of the information.

Distinguishing between different providers, intermediary services, and the roles they fulfil is thus essential in the case of integration of services or when roles are interwoven but can be used independently of each other (in the case of usage of a payment service outside of the marketplace). In the case of usage of a payment service outside the providers' ecosystem, content-based regulation through this payment service could also affect the content on other services.

As discussed in the introduction, the main interest of this dissertation is in the providers that function as content curators. As discussed in this chapter, content curators are providers that can exercise direct control over the content of user-provided information. This criterion of direct control is stricter than only allowing application layer or edge service providers to regulate the content of user-provided information. For example, payment service providers – normally – do not have direct access to the content of the information while they do function on the application layer service. Providers that function as content curators (such as online platforms and search engines) know no technological constraints in how they moderate or curate user-provided information. Unlike services that operate on the physical or the network layer of the internet, they have the technological capabilities to regulate user-provided information. Content curators are, unlike other services, not legally required or functionally obligated to remain neutral towards user content.[365] Content curation services providers offer a service directed at the user to

---

[363] Dinwoodie, 2020, 'Who are Internet Intermediaries?', p. 45.

[364] Dinwoodie, 2020, 'Who are Internet Intermediaries?', p. 45.

[365] The Directive only 'protects' intermediaries of a "mere technical, automatic and passive nature", see Recital 42 of Directive 2000/31/EC (*Directive on electronic commerce*). This is – unfortunately – sometimes explained as 'neutrality. For example, in Judgement of the Court (Grand Chamber) in *C-324/09* (*L'Oréal v. eBay*), in particular Rec. 116; Judgement of the Court (Grand Chamber) in *C-236/08, C-237/08 and C-238/08* (*Google France*), in particular Rec. 114. In these judgements an "active role" is confused or at least conflated with "neutrality".

help the user encounter information with relevant content. Providers that offer internet intermediary services encompassing curation have a vital function. Because of this importance, it is necessary to set out how these curators regulate user-provided information.