4
Introduction to Liability Framework

4.1 Introduction

On 22 November 1995, three buses full of policemen stormed the Munich offices of CompuServe, a prominent American company that operated online discussion newsgroups, in a surprise raid.[1] The unsuspecting employees were soon informed that the raid had to do with CompuServe's online groups that were involved in exchanging child abuse material and games harmful to children.[2] The police officers left empty-handed,[3] but the raid worked wonders. Fearing the looming legal consequences, CompuServe felt compelled to take immediate action and demonstrate their willingness to cooperate. The German prosecutor wasted no time in delivering a stern message. CompuServe must take the necessary steps to avoid liability. He sent a list of 200 groups to block.[4] CompuServe hurried to comply. But the hastily compiled list included a multitude of groups that bore only a vague connection to illegal content. Among the innocent casualties was a group dedicated to discussing breast cancer.[5] Three months later, CompuServe introduced a primitive filtering software known as CyberPatrol. This software relied on a human-maintained blacklist of URLs specifically designed to block access to any content associated with child abuse material. It soon became apparent that CompuServe's actions were in vain. The German prosecutor remained unsatisfied.

This was the time when the legal troubles of internet companies started mounting. Only a few weeks before the Munich raid, a bailiff, accompanied by two United States (US) members of the Church of Scientology, raided the Amsterdam offices of a Dutch

[1] Nico Ernst, 'Ex-CompuServe-Chef Felix Somm im Interview' *Computerwoche Tec Workshop* (17 May 2000) <https://www.tecchannel.de/a/ex-compuserve-chef-felix-somm-im-interview,401170> accessed 3 August 2023.
[2] ibid. (The index of media deemed unsuitable for young persons by the Federal Department for Media Harmful to Young Persons (BPjM) included some computer games, such as Wolfenstein).
[3] Michael Kunze, 'The Compuserve Switch-Off of USENET NewsGroups' (6 January 1996) <http://www.rogerclarke.com/II/Compuserve.html> accessed 3 August 2023.
[4] ibid.
[5] Ernst (n 1); Kunze (n 3).

provider, XS4ALL.[6] As a prelude to a copyright lawsuit for hosting third-party websites, the entourage came to take steps to preserve evidence. Meanwhile, in the US, a District Court held in *Netcom* that a telecommunication company and a bulletin board provider could be liable for users' copyright infringements in yet another case initiated by the Church of Scientology.[7] In another case, CompuServe's competitor Prodigy was held to be liable for content posted by its users under defamation law because it engaged in content moderation.[8] The world was already becoming a global village. The cover of *Time* magazine was warning people about 'cyberporn',[9] and the US Congress was intensely debating the US Communications Decency Act (CDA). This influenced popular opinion in other countries, including Germany.[10]

In Munich, despite CompuServe's efforts, the Munich police and prosecutors were not backing down. According to Kunze, a journalist for *Der Spiegel* Magazine, the entire group of German legal professionals had a bigger plan. In his view, the group set out to establish the principle that the providers are responsible for the content of others.[11] He later wrote that '[a]ll activities of the Task Force could not have happened if they were not supported by a whole bunch of local prosecutors and judges. Sticking together, chatting, doing favours forms a part of the social life in Munich'.[12]

The results came quickly.

On 26 February 1997, the prosecutor filed a criminal indictment of Mr Felix Somm, the managing director of CompuServe's German branch. To the astonishment of many, in May 1998, a judge of the Munich County Court sentenced Mr Somm to two years of imprisonment on probation and a fine of 100,000 marks,[13] a sum that, in today's currency, equated to approximately €84,500.[14] Mr Somm was found guilty of complicity in disseminating illegal material and of negligent dissemination of content harmful to minors in the form of then-popular computer games, such as Doom, Heretic, and Wolfenstein 3D. The judge's justification for the harsh judgment was clear—the internet cannot become a lawless space. He wrote:

> there is a vital interest of society that technical progress in the teleservices sector *does not lead to the creation of lawless areas* in which such high legal interests as the

[6] XS4ALL Internet, 'Press Release: Police and Members of Scientology Church Enter Offices of XS4ALL' (5 September 1995) <https://felipe.home.xs4all.nl/cos/pers.eng.html> accessed 3 August 2023.

[7] *Religious Technology Center v Netcom On-Line Communication Services Inc* 907 F Supp 1361 (ND Cal 1995) (*Netcom*).

[8] *Stratton Oakmont Inc v Prodigy Services Co* 23 Media L Rep 1794 (NY Sup Ct 1995) (*Prodigy*). CompuServe, in contrast, won a similar case in *Cubby Inc v CompuServe Inc* 776 F Supp 135 (SDNY 1991) exactly because it lacked elaborate content moderation policies.

[9] TIME, 'TIME Magazine Cover: Cyber Porn' (*TIME.com*, 3 July 1995) <https://content.time.com/time/covers/0,16641,19950703,00.html> accessed 3 August 2023.

[10] Kunze (n 3).

[11] ibid.

[12] ibid.

[13] AG München NJW 1998, 2836. See also Brandon Mitchener and Nick Wingfield, 'A Former CompuServe Official Is Convicted in Pornography Case' *Wall Street Journal* (29 May 1998) <https://www.wsj.com/articles/SB896371751696756000> accessed 3 August 2023.

[14] Inflation adjusted, using 'German Inflation Calculator to Factor Inflation into Any Calculation' <https://www.lawyerdb.de/Inflationrate.aspx> accessed 4 August 2023.

> protection of minors and protection against sexually motivated violence are subordinated to purely commercial interests and thus sacrificed ... As managing director, the defendant was responsible for the business division in Germany. It was his responsibility to ensure that German laws were observed. *It was therefore part of his duty of care to ensure that no indexed games were offered to customers in Germany in the proprietary service*. The fulfilment of these duties of care is to be demanded of anyone working in this position in this area ... In view of these at least discernible circumstances, *the defendant should have expected* that indexed games would also be offered in the proprietary game forums as proprietary games of the parent company.[15]

Mr Somm's case caused international outrage. The Munich County Court ruling was even more surprising given that in June 1997, after Mr Somm's criminal indictment but before his sentence by the judge, the German legislature adopted a pioneering new law which included two separate liability exemptions —the first of its kind in Europe.[16] Section 5(2) of the 1997 German law (IuKDG) provided that 'service providers are only responsible for third-party content that they make available for use if they are aware of this content and it is technically possible and reasonable for them to prevent its use'.[17] Section 5(3) provided that '[s]ervice providers are not responsible for third-party content to which they merely provide access for use'.[18] The two German liability exemptions entered into effect almost immediately on 1 August 1997.[19] The German government even held a joint European Ministerial Conference with the European Commission in July 1997 in Bonn stressing that 'rules on responsibility should give effect to the principle of freedom of speech, respect public and private interests and not impose disproportionate burdens on actors'.[20] The Bavarian judge of the County Court, however, found the federal German legislation to be inapplicable.

While the Munich Regional Court eventually reversed the decision on appeal, it took Mr Somm over two years to clear his name.

Mr Somm's over-reaction to the letter of the prosecutor became one of the first well-known documented cases of what came to be known as 'over-blocking'—the damaging removal of legitimate content caused by providers' cautious response to legal risks. This episode and early US cases provided a strong warning that some explicit legal positioning of digital services might be necessary. XS4ALL, the Dutch provider, noted in its press release following the raid that: 'This whole affair demonstrates the need for clarity concerning the legal position [*sic*] of Internet Providers. … If we as Internet

[15] AG München NJW 1998, 2836 (emphasis mine).

[16] The US passed its CDA in 1996.

[17] Information and Communication Services Act (Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste) v. 22 July 1997 (BGBl. I, 1870) (IuKDG), art 1, § 5(2).

[18] ibid art 1, § 5(3).

[19] It took years for the courts to take German liability exemptions seriously. While police and prosecutors backed off from prosecuting access and hosting service providers for offering their services, civil courts, according to one study, either applied the new rules very reluctantly or overlooked them altogether. See Lothar Determann, 'Case Update: German CompuServe Director Acquitted on Appeal' (1999) 23 UC Law SF International Law Review 109, 119.

[20] European Ministerial Conference, 'Global Information Networks: Realising the Potential' (6 July 1997) <http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm> accessed 5 August 2023.

providers are held responsible for what our users say, that will undoubtedly [*sic*] kill freedom of speech on the net.'[21]

In the US, Congress had adopted the CDA which, among other things, tried to incentivise content moderation by giving providers near-blanket legal immunity from many types of liability for others.[22] Section 230 CDA was proposed by two senators to specifically undo the court ruling in *Prodigy*.[23] The Congress would soon also adopt section 512 of the Digital Millennium Copyright Act (DMCA) in reaction to *Netcom* and other copyright cases.[24]

In Europe, the European Commission published its communication to the European Parliament and Council in October 1996, explaining that providers will need legal assurances to operate in the internal market properly. The communication stated that:

> Internet access providers and host service providers play a key role in giving users access to Internet content. It should not however be forgotten that the prime responsibility for content lies with authors and content providers. It is therefore essential to identify accurately the chain of responsibilities in order to place the liability for illegal content on those who create it … The law may need to be changed or clarified to assist access providers and host service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability.[25]

Shortly after the US adopted the DMCA, on 18 November 1998, the European Commission tabled a proposal for a Directive on certain legal aspects of electronic commerce in the internal market—commonly known as the E-Commerce Directive (ECD). This Directive included three liability exemptions modelled after the DMCA but also took inspiration from the German horizontal approach to immunities.

When, in November 1999, the appellate court found that the Munich court's interpretation of criminal negligence was overstretched and that Mr Somm lacked any intent, the world looked very different.[26] Laws establishing a new global norm were already being written in Europe and the US. By agreeing to the liability exemptions, all parties exercise self-constraint and do their part to facilitate the emergence of an environment from which the society at large can benefit. This is the essence of the digital social contract. According to it, any criminal, administrative or civil wrongdoing is primarily the wrongdoer's responsibility, and only secondarily, a shared responsibility

[21] XS4ALL internet (n 6).

[22] Only days after the German legislature adopted its new act, the US Supreme Court in June 1997 invalidated much of the Communications Decency Act but left the liability exception in s 230 intact. See *Reno v ACLU* 521 US 844 (1997).

[23] See the historical discussion in Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell UP 2019) 57ff.

[24] *Playboy Enterprises Inc v Frena* 839 F Supp 1552 (MD Fla 1993); *Netcom* (n 7). See also Martin Husovec, 'Rising Above Liability: The Digital Services Act As a Blueprint for the Second Generation of Global Internet Rules' [2023] Berkeley Technology Law Journal (forthcoming).

[25] Commission, 'Illegal and Harmful Content on the Internet' (Communication) COM(96) 487 final, 12–13.

[26] LG München NJW 2000, 1051.

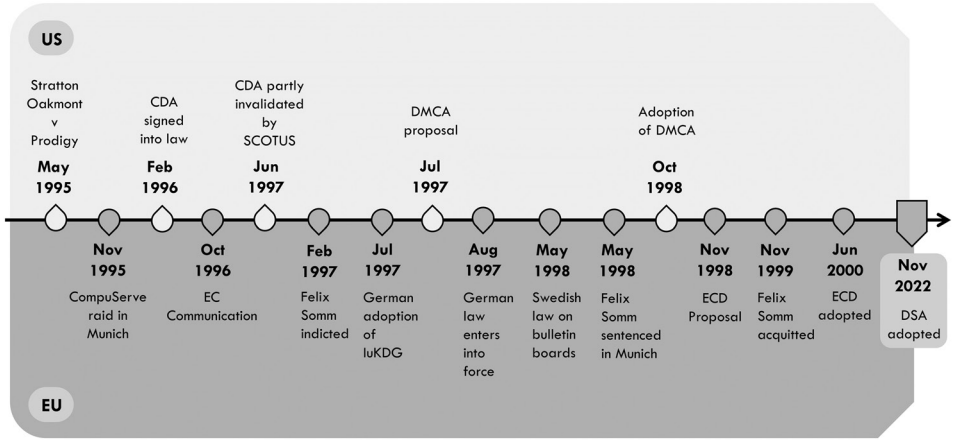

Figure 4.1 Timeline of intermediary liability rules

of other actors, such as providers, civil society, and victims. The shared responsibility means that each one has a role in enforcing the rights.

Even after many years, Mr Somm's story demonstrates the struggles that providers faced during the formative period of 1995–99 and acts as a reminder of the benefits of the existing system. Figure 4.1 shows the historical progression of legal acts.

4.2 History of the ECD

In November 1998, the European Commission tabled a proposal for the ECD. The proposal followed the course outlined in the Commission's 1996 Communication on 'Illegal and Harmful Content on the Internet'.[27] While the Jacques Santer Commission prepared the proposal, it was the next Romano Prodi Commission that successfully stewarded it through the legislative process towards its adoption in June 2000. The Member States did not make significant changes to the initial proposal, but they influenced the meaning of the text through additions of various Recitals.

Throughout the legislative process, much effort was expended on resolving the debate on the scope of the country-of-origin principle. In the European Council, several Member States demanded various limitations and clarifications. For the liability exemptions in particular, Sweden wanted a bulletin board exception from the prohibition of general monitoring obligations to be able to keep its newly adopted law on bulletin boards.[28] Moreover, several Member States, including Austria, Sweden, and Denmark,

[27] Commission, 'Illegal and Harmful Content on the Internet' (Communication) COM (96) 487 final, 12–13.

[28] Working Party on Economic Questions (Information Society services), 'Report on Draft European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market Dated 11/12 November 1999' (1999) Doc 12667/99 ECO 364 CONSOM 68 CODEC 655, 6 <https://resources.law.cam.ac.uk/cipil/travaux/ecommerce_directive/ecommerce_travaux_complete.pdf#page=316> accessed 5 August 2023; Law on Responsibility for Electronic Bulletin Boards (Lag (1998:112) om ansvar för elektroniska anslagstavlor) (Swedish Bulletin Board Act).

wanted the knowledge test, which only applied to the liability exemption for hosting, to apply to all liability exemptions.[29] Denmark also had some competence concerns about the applicability of liability exemptions in the area of criminal liability.[30] France argued for mandatory client data retention to accompany the hosting liability exemption.[31] Ireland proposed to include search engines in the liability exemptions.[32]

None of these requests concerning liability exemptions were strong enough to significantly change the European Commission's proposal. However, they led to the introduction of Recitals 42 (passivity), 47 (specific measures), and 48 (duties of care)—all of which greatly influenced the Court of Justice of the European Union's (CJEU) case law on these issues years later.

Article 15(2) and Recitals 42[33] and 48[34] were introduced to appease the countries that wanted a knowledge test to underpin all of the liability exemptions. Recital 47 introduced the clarification that 'monitoring obligations in a specific case' are not in any case prohibited.[35]

An interesting historical aside is that these countries had initially sought to have the knowledge test applied across the board, in part due to 'the potential of future technological developments to permit [non-hosting] intermediaries to monitor the data they transmit' and the resulting effect that 'an exemption from liability might no longer be appropriate'.[36] To address these reservations, the revision clause in Article 21(2), which provides for the ability to amend conditions for liability exemptions in light of technical developments, was added.[37] The Swedish demand that the bulletin boards should be excluded from the prohibition of general monitoring was mollified by the Commission's argument that the Swedish law does not have to change.[38] This is interesting because section 4 of the Bulletin Board Act basically required random checks, although the exact scope was far from clear and the Swedish government itself insisted that it: 'is not intended that the activity of the supplier should be seriously hampered

[29] Working Party on Economic Questions (Information Society services) (n 28).

[30] ibid 8.

[31] Permanent Representatives Committee, 'Extract of the Summary Record of the 1853rd Meeting of the Permanent Representatives Committee on 17 and 19 November 1999' (1999) Doc 12957/99 Ext 1 CRS/CRP 44 ECO 387 CONSOM 73 CODEC 714, 4 <https://resources.law.cam.ac.uk/cipil/travaux/ecommerce_directive/ecommerce_travaux_complete.pdf#page=325> accessed 5 August 2023.

[32] ibid.

[33] This was introduced very late in the legislative process in December 1999. Council of the European Union, 'Draft Minutes of the 2233rd Council Meeting (Internal Market) on 7 December 1999' (2000) Doc 13858/99 PV/Cons 83 MI 126, 7 <https://resources.law.cam.ac.uk/cipil/travaux/ecommerce_directive/ecommerce_travaux_complete.pdf#page=370> accessed 5 August 2023.

[34] Probably to appease the Swedish delegation, the political agreement was reached in December 1999 to include what has become Rec 48 as a clarification accompanying art 15 ECD, which allows applicability of 'duties of care'. See ibid 8.

[35] COREPER, 'Outcome of Proceedings Dated 1 December 1999' (1999) Doc 13655/99 ECO 402 CONSOM 76 CODEC 749, 21 <https://resources.law.cam.ac.uk/cipil/travaux/ecommerce_directive/ecommerce_travaux_complete.pdf#page=333> accessed 6 August 2023.

[36] COREPER, 'Report on the Draft European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market' (1999) Doc 13657/99 ECO 403 CONSOM 77 CODEC 750, 6 <https://resources.law.cam.ac.uk/cipil/travaux/ecommerce_directive/ecommerce_travaux_complete.pdf#page=361> accessed 6 August 2023.

[37] ibid.

[38] ibid.

by the act. If the number of messages is so large, that it is too cumbersome to check them all, it can be acceptable to provide an abuse board, to which users can complain of the existence of illegal messages'.[39] The Swedish request thus probably lead to Recital 48 which vaguely speaks of 'duties of care'. Denmark's reservations regarding the legal basis of criminal liability were dismissed by the European Commission's Legal Service and were not pressed by the other Member States.

The political agreement was reached in February 2000, and the Directive was approved by the European Parliament in June 2000 with a transposition deadline of January 2002. A series of landmark cases on this new system of liability exemptions soon followed—*Promusicae* in 2008,[40] *Google France* in 2010,[41] *eBay* in 2011[42] and *YouTube* in 2021[43]—all decided by the Grand Chamber of the CJEU.

4.3 Two Generations of Rules

The CDA (section 230) and the Digital Millenium Copyright Act (DCMA) (section 512) in the US, the Informations- und Kommunikationsdienste-Gesetz (IuKDG) (section 5) in Germany and the ECD (section 4) in the EU all represent the first generation of digital services regulation. They tackled the crucial question of the time: when is a provider liable for its users' content? While they offered various responses, ranging from almost 'never' to 'if they acquire knowledge', they united in the effort to provide assurances to firms about liability risks.

4.3.1 The ECD as the first generation

The first generation of rules regulates the behaviour of platforms by a legal threat of liability for the actions of others; if you do not remove content or behave in such and such way, you might be liable alongside your users. The conditional immunity model[44] defined roughly two decades of platform regulation in Europe between the

[39] The Swedish government provided the quoted text in the proposal to the parliament. Government Bill (1997/98:15) Responsibility for electronic bulletin boards (Ansvar för elektroniska anslagstavlor) <https://www.regeringen.se/contentassets/25d815028bfc4ba4bcef3234291d6ddb/ansvar-for-elektroniska-anslagstavlor/> accessed 6 August 2023. S 4 of the Swedish Bulletin Board Act says: 'The supplier of electronic bulletin board shall, in order to be able to fulfill the obligations according to article 5, supervise the service to an extent which is reasonable considering the extent and objective of the service'. According to Rosen, five years after the law was adopted, it was not once applied by the courts. See Jan Rosén, 'Server Copyright Liability - Notes on the Swedish Act on Liability for Intermediaries and two Recent Decisions of the Swedish Supreme Court' [2002] 42 Scandinavian Studies in Law 147, 150.

[40] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* ECLI:EU:C:2008:54 (*Promusicae*).

[41] Joined Cases C-236/08–C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2010:159 (*Google France*).

[42] Case C-324/09 *L'Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474 (*eBay*).

[43] Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503 (*YouTube and Cyando*).

[44] The model requiring at least knowledge to trigger liability, Husovec (n 24).

ECD (2000) and the DSA (2022). The legal rules were mostly reduced to coordinating liability for third-party content. During this period, the provider's only legal responsibility was to do everything necessary to avoid liability. Any extra efforts were voluntary and depended mainly on the business environment, public opinion, and political pressures, but very little on additional legal risks.[45] Thus, the liability system only punished failures of reactive behaviour, and any proactive behaviour was entirely voluntary.

The ultimate value that liability exemptions protect is decentralised speech. The internet's genius is in allowing anyone to speak their minds without seeking approval. The digital ecosystem weakened the power of traditional gatekeepers, such as TV and radio stations, newspapers, and book publishers, over our public sphere. Obviously, this creates challenges because editors were previously deputised to act as filters for the lawfulness, trustworthiness, and quality of information. Now that information is not always edited upfront, providers of digital services are deputised to act as ex post quasi-editors by engaging in content moderation. Without editors, the ecosystem shifts from filtering the content's quality upfront to managing its distribution. Even though such expectations towards digital providers reappoint them as gatekeepers, decentralised content is still allowed to flourish unless controls are too tight. And that is exactly why the control cannot be too tight. Imposing incentives that reinstate upfront editorial control automatically takes away the newly gained ability of individuals to speak and read what is not edited.

Without sympathy of the law, there would be no internet as we know it. In a world where technology facilitates decentralisation while the law disincentivises it, no rational actors would have created spaces or tools without editorial control. A liability regime for the actions of others is a key—albeit not the only—incentive to keep the decentralised architecture of the global network afloat.[46] Unless legislatures want to reinstate editors, some form of conditional immunity (or liability) is necessary. Figure 4.2 depicts the richness of the digital ecosystem and its players.

The ECD provided for three liability exemptions: conduit, caching, and hosting. Each represents a separate type of conditional immunity, that is, legal immunity that requires at least knowledge of providers to allow for liability for others. The conduit immunity is the most generous and applies to infrastructure services like internet access providers. It protects conduits from pressures to block websites or users without court orders. The caching immunity applies to services that facilitate communication flows by temporarily storing the websites of others. It protects caching services from having to act upon illegal content before it is removed from its source. And finally, the most

[45] Martin Husovec, 'Accountable, Not Liable: Injunctions Against Intermediaries' [2016] TILEC Discussion Paper No 2016-012 <http://www.ssrn.com/abstract=2773768> accessed 7 August 2023.

[46] In the literature, van Schewick argued most convincingly that technical architecture influences innovation and a decentralised environment for speech—Barbara van Schewick, *Internet Architecture and Innovation* (MIT Press 2010). Her work directly relates to the net neutrality debate, which posits that Internet access providers should not engage in discriminatory practices when routing traffic through their networks.

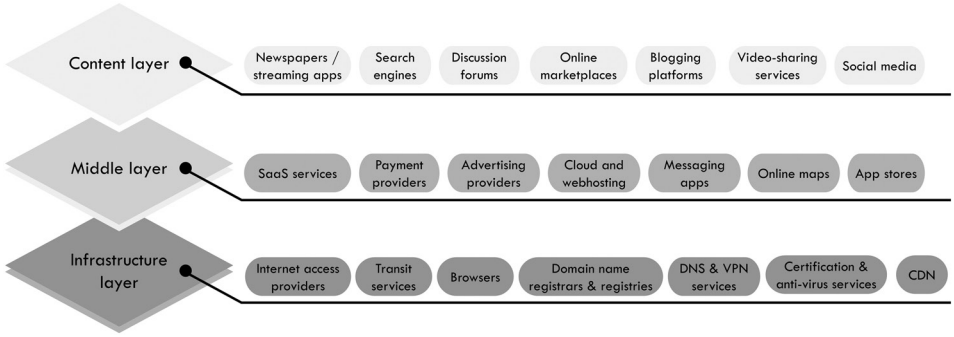

Figure 4.2 The internet tech stack

prevalent is the hosting immunity that protects the application layer of the internet, which stores the content of others. Hosts are protected from liability before they are notified or otherwise learn about illegal content. Given the prevalence of these services, hosting immunity creates the baseline choreography of digital enforcement—that of 'notice and action', although more commonly known as 'notice and takedown'.

4.3.2 The DSA as the second generation

Regulation through liability exemptions has its limits. The horizontal liability exemptions are about creating breathing space for speech and markets while allowing enforceability of the rights of victims, but they do not address specific challenges. The rules of the first generation—sections 230 CDA, 512 DMCA, 4 ECD—all suffer the same insufficiency. They excel at coordinating expectations to encourage investment but fail at offering tools to solve a wide range of societal problems that emerge along with the use of these services. The past years have drawn contours of many societal challenges that require solutions, ranging from the protection of children to problems with hate speech or terrorism and subversive activities that try to attack the basis of our democratic systems.

All these problems are exacerbated by the 'special features' of the internet as a medium: its lack of editorial approval, low barriers to entry, including the zero cost of services across the board, the incredible speed and scale of distribution, its broad social and geographical inclusiveness, and resilience of communications. The regulators are thus rightly considering how to address these challenges. As the introduction shows, it is understood at the time of writing that strict liability for someone else's content is a death sentence for decentralised speech. It means rewinding the clock to the pre-internet area, where editors are responsible for what they make available to readers. Any regulation needed to be more tailored.

To avoid this, the second generation of rules, such as the DSA, does not intend to change the underlying liability for someone else's content. Instead, they try to create a set of independently enforceable due diligence obligations (Chapter 9.4). Those obligations are of a systemic nature, which means that the prescribed outcomes are owed

to the public.[47] A violation does not lead to responsibility for the communication of the content of others. It has separate legal consequences. Instead of endlessly trying to redraw the line between editors and mere intermediaries, the DSA spells out the legislature's specific expectations.

The DSA regulates the choreography of digital enforcement, which is guaranteed by liability exceptions. It regulates the process through which content moderation decisions are taken. Actors who have previously earned trust with the quality of their work are asked to be given better treatment. The decision to restrict the content taken by platforms must be explained. Content creators who are affected must be notified and offered reasons for content moderation decisions, which they can appeal to internally and, if necessary, externally. Some providers are asked to think about the risks posed by the design of their services.

This shift in focus from *liability* to *accountability* means the discussion primarily moves to a debate about the right systems and procedures to achieve appropriate aggregate outcomes. The DSA's due diligence obligations treat providers as accountable for operating systems but not liable for the individual harms caused by their users. The liability exemptions make sure that individual harms are not attributed to providers so the debate can move on to how to manage risks. Even the DSA's tool for the largest players, risk mitigation, implies that some failures are inevitable and acceptable. This is in stark contrast with how rules that set the basic legal expectations for liability operate. When liability rules are violated, platforms are exposed to liability, regardless of whether something is an occasional slip-off or a systemic problem.

The DSA's liability exemptions and accountability obligations are mutually compatible as long as they are based on the same principles. One can easily imagine accountability obligations that undermine liability exemptions. For instance, a rule that providers must verify the authenticity of all goods that other people trade on the provider's platform also clashes with the liability arrangements. Firstly, any fine enforcing it is a form of liability imposed for storing third-party information—that is, a liability for failing to verify. Secondly, it imposes a general obligation to monitor the authenticity of the content. Thirdly, it creates an obligation to acquire knowledge, which removes the applicability of the liability exemption for hosts.[48]

Thus, while accountability is inherently proactive because it asks providers to think about potential risks in advance, it must remain targeted. Otherwise, accountability risks turning into strict liability. The DSA's approach is to keep relying on reactive liability exemptions while increasing accountability in ways that avoid general monitoring. This means that accountability is always targeted to duties in specific cases. In the legal design, to assure this is the task of the prohibition of general monitoring, which I discuss next.

[47] But it can still be privately enforced (ch 19).

[48] In the European system, the European legislature is the only one that can undermine liability exemptions. The DSA pre-empts any national attempts to impose such due diligence obligations.