An EPICENTER paper

THE XXX FACTOR

Why internet freedom hinges on pornography

Giacomo Lev Mannheimer

December 2023

EPICENTER
European Policy Information Center

ibl
Istituto Bruno Leoni

Contents

About the author **4**
Summary **6**
Introduction **8**
The history of pornography is a story of innovation **10**
The regulation of online pornography **13**
Upcoming regulations:
Age verification and preventive moderation **17**
Another path: Collaboration and innovation **28**
List of references **33**

About the author

Giacomo Lev Mannheimer is a Research Fellow at the Bruno Leoni Institute, where he primarily focuses on topics related to the regulation of the digital economy and competition. He has studied law and international economics in Milan, Madrid, Brussels, and Yale. For over a decade, he has been involved in analysing public policies and corporate strategies, working both in Italy and abroad for startups, multinational companies, consulting firms, and institutions. He is also the Coordinator of the Scientific Committee for the Milan Metropolitan Observatory and has authored articles on policy and regulation for various newspapers and magazines.

Summary

- The online pornography industry has historically been a pioneer of many innovations that have later influenced the rest of the internet. Among others, the porn industry helped develop fraud prevention techniques and security innovations, such as double confirmation processes, ahead of mainstream e-commerce platforms, as well as online security and copyright protection methods.
- Generally, regulatory efforts across the world to control internet content have often been sparked by a perceived need to restrict access to adult content. Early attempts at internet regulation in the US, such as the Communications Decency Act, 1996, faced challenges in enforcing age verification for websites and defining obscene material. This led to legal conflicts and the formulation of principles such as Section 230, arguably one of the reasons why the internet is what we know today. The United Kingdom (UK) and the European Union (EU) have also made attempts to mandate age verification and regulate content on adult websites, with the UK's Online Safety Bill, 2023, mandating age verification for accessing adult content using government-issued documents or biometric data, while the EU's Digital Services Act (DSA), 2023, aims to address these issues by providing transparency about content moderation and law enforcement, although some platforms are uncooperative with data disclosure requests.
- In recent times, several European countries have begun to speculate with increasing insistence on implementing age verification laws for individuals accessing adult websites. However, there are three key challenges associated with implementing effective age verification for adult content: challenges in ensuring compliance, the lack of a standardised approach, and potential privacy issues and conflicts with General Data Protection Regulation (GDPR) principles. Additionally, there are concerns that strict age verification measures may lead users

to resort to using virtual private networks (VPNs) to bypass controls, inadvertently directing traffic towards less regulated and less secure platforms, thereby exacerbating risks.

- The EU is also trying to regulate content moderation, demanding platforms implement stronger measures to prevent users from uploading dangerous or illegal content in the first place. For example, a proposed regulation aimed at restricting the circulation of child sexual abuse material online (Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 2022) has raised worries about the risk of indiscriminate monitoring, as it might lead to increased surveillance of a broad range of online content-sharing platforms, impacting privacy and freedom of expression of many way beyond the regulation's initial scope.
- Regulating pornography appropriately is not only just in itself, but it will also ensure that the internet remains a place of extraordinary freedom and innovation without implying impunity or unaccountability for those who use it to commit illegal acts. While proposals for age verification and content moderation on adult websites are emerging in Europe, it is important to reflect on the possible risks and the potential impact these measures could have if they are extended to the rest of the internet.

Introduction

In recent years, the regulation of online pornography has attracted increased attention worldwide. This study aims to examine the latest proposals in Europe and identifies the risks these initiatives pose to internet freedom as a whole.

The first section is dedicated to exploring the close relationship between the history of pornography and technological innovation, which has helped shape the internet as we know it. This long evolution provides the crucial context for understanding the challenges that the industry faces today and possible solutions.

The second section analyses the current state of regulation in Europe and beyond, highlighting the growing concerns of legislators and other stakeholders, particularly regarding the potential impact of unrestricted access to adult content on minors and the challenges associated with privacy protection.

In the third section, the two main areas of imminent regulation — age verification, which involves implementing systems to prevent minors from accessing adult content, and preventive moderation, which aims to limit the spread of illegal or harmful content by placing the responsibility for such restriction directly on platforms — have been examined.

Finally, in the fourth section, an alternative approach is suggested to overly pervasive regulations – one based on collaboration among governments, industry, civil society, and the technical experts representing the platforms subject to these regulations.

The ensuing discussion aims to provide a comprehensive overview of the complex issues related to the regulation of online pornography in Europe

and potential paths to balance the protection of individual rights and the safeguarding of society and vulnerable individuals.

The history of pornography is a story of innovation

Every technological revolution is a response to a social need or practical function. In the history of computing, a force that has driven significant technological transformations, in various forms, is pornography (Barss 2011).

In the era of early modems, even before the advent of the internet, though personal computers were not capable of distributing music or video, users could, with a bit of patience, distribute images. Those who wanted to exchange adult content certainly had that patience. In 1996, five of the top ten newsgroups on Usenet, one of the first large-scale virtual bulletin boards, were dedicated to adult materials (Johnson 1996).

In the late 80s and early 90s, bulletin board systems (BBS) gained popularity. Users could connect to an individual's computer and explore shared games, files, and programs. BBS administrators quickly discovered that the most sought-after files were pornographic, often old collections of *Playboy* or *Penthouse*. Circulation of these files was so rampant that *Playboy* sued a BBS operator for copyright infringement and won $500,000 in 1993 (Eisenberg 2013). All of this happened long before Napster, YouTube, and Spotify, and even before the web supported image viewing.

Getting users to agree to pay for adult content was not the problem; establishing a reliable payment system was the real challenge. Pornographic websites have always had an unusually high number of fraudulent transactions and chargebacks, with cancellation rates reaching as high as ten to twenty per cent of the total transactions (Lane 2000). This is one of the reasons why, aside from reputation concerns, credit card companies are wary of online pornography.

As early as 2000, American Express stopped doing business with adult content websites, publicly citing commercial reasons rather than ethical ones.[1] Even back then, the industry was one of the few that could generate profits through e-commerce, but it was simultaneously one of the sectors hardest hit by customer disputes. In the credit card market, disputes are resolved through refunds or denials. In both cases, the cost of handling disputes often far exceeds the profits generated from such transactions.[2]

In 2020, Mastercard and Visa followed American Express's lead and blocked the world's largest online pornography group, MindGeek, after a *New York Times* investigation revealed that its platforms contained revenge porn and abuse content, including of minors. The combined market share of American Express, Mastercard, and Visa in the global credit card market is 98 per cent. As a result, Pornhub and its associated sites could no longer process online payments.[3]

In the following years, MindGeek attempted to persuade Mastercard and Visa to reverse their decisions through various new policies, including better content moderation and by restricting unverified users from uploading material. Despite these efforts, in 2022, Visa and Mastercard also suspended payments for TrafficJunky, MindGeek's advertising arm.

As a result, an entire industry of third-party payment services emerged that allowed adult websites to use their merchant accounts to share the chargeback risk. The most well-known of these is CCBill (founded in 1998) and its main competitor, Epoch (founded as early as 1996). It is not unreasonable to believe that PayPal, Stripe, and Satispay were born from the ashes of these early intermediation systems. Following the 2020 ban, Pornhub now relies on Probiller, a third party that essentially intermediates between the platform and credit card issuers, concealing the purpose of transactions from the latter.

1 'Merchant regulations', *American Express*, October 2023 (https://www.americanexpress.com/content/dam/amex/us/merchant/new-merchant-regulations/Regs_EN_HK.pdf).

2 ''No' to web porn sites: American Express', *CBC News*, 8 June 2000 (https://www.cbc.ca/news/science/no-to-web-porn-sites-american-express-1.204990).

3 'Market share of Visa, Mastercard, American Express, Discover as general purpose card brands in the United States from 2007 to 2022, based on value of transactions', *Statista*, 31 August 2023 (https://www.statista.com/statistics/279469/market-share-of-credit-card-companies-in-the-united-states-by-purchase-volume/).

Due to the higher risks they faced, pornographic websites were the first to develop many of the modern fraud prevention techniques that almost all e-commerce systems use today, such as identifying charges from free email accounts and checking whether the card address location matched with the user's IP address. Today, it is common practice for websites and apps to register new users through a double confirmation process to ensure that the user is a real person and not a bot; this practice was first introduced by a pornographic website called Cybererotica (Perdue 2002). Porn producers had to develop these innovations mainly on their own because traditional companies wanted nothing to do with them. Paradoxically, the stigma surrounding the industry has been the driving force behind most of the innovations that adult content distributors have produced in the areas of e-commerce and online security.

Therefore, pornography has not only played a significant role in the adoption of new technologies throughout the history of communication and entertainment but, in the case of online pornography, difficulties in collaborating with the rest of the web industry have proved to be, well before and better than any form of regulation, a formidable engine of innovation in terms of security, rights, and copyright protection. This, as we will see in the next section, does not mean that the sector has not been subject to increasingly assertive regulatory attempts.

The regulation of online pornography

In recent years, the growing economic and social significance of online activities has led to a surge in legislative efforts to regulate the internet. In this context, many attempts to regulate the internet have stemmed from efforts to eliminate or restrict access to adult content.

One of the earliest examples is the Communications Decency Act (CDA), enacted in the US in 1996. The most controversial aspects of the law pertained to online pornography. The act imposed civil and criminal penalties on anyone who,

> knowingly makes, creates, or solicits, and initiates the transmission of any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age.

There were two primary issues. First, how can one verify the age of someone seeking to download online content from behind a screen? Second, what constitutes 'obscene or indecent' material, and what does not? As we will see, legislators continue to grapple with the same two questions even today regarding pornographic websites and the internet in general.[4]

4 The second question, in particular, has historically predated the internet and has given rise to a significant portion of US jurisprudence regarding the relationship between the First Amendment and pornography. One of the most well-known examples is *Hustler Magazine, Inc. v. Falwell*, a 1988 case in which the Supreme Court intervened in the matter of an erotic comic published in *Hustler Magazine*, at the time the most widely circulated adult publication in the US, edited by the controversial entrepreneur, Larry Flynt. The parody suggested that Falwell, a well-known former minister, and founder of the conservative Christian organisation, Moral Majority, had engaged in 'an incestuous encounter with his mother, completely drunk'. Reversing the lower court's decision, the Supreme Court upheld the magazine's right to ridicule Jerry Falwell, a public figure, rejecting his claim for defamation. For further details, please see Calvert and Richards (2001).

A few months after its enactment, a court in Philadelphia suspended the application of parts of the CDA, arguing that it would violate users' First Amendment right to free speech. The Supreme Court upheld this decision, stating that the provisions amounted to a limitation of the First Amendment, because the act did not allow parents to decide autonomously what materials were acceptable for their children, and it did not precisely define the terms 'obscene' and 'indecent'.

Despite its overall failure, a part of the CDA, known as Section 230, remained in force and introduced the so-called 'Good Samaritan' clause into US law, which states that no provider or user of an interactive computer service should be treated as the publisher or responsible of any information provided by another information content provider. This principle became fundamental for the subsequent development of the internet, without which platforms such as Facebook or YouTube would not exist as we know them (Kosseff 2019). Once again, it was pornography that first confronted the issue, leading legislators to recognise the non-liability of websites and digital platforms for user-uploaded content.

In hindsight, the reasoning of the court's decision to nullify additional provisions of the CDA based on the idea that exemptions from the First Amendment should be limited to newspapers, radio, and television sounds somewhat dated. Justice Stevens explained that the existing precedent of allowing the government to regulate broadcast mediums did not apply to the internet because 'the internet is not as "invasive" as radio and television' (Stevens 1997). Reading this statement today, 25 years later, it sounds somehow grotesque.

Attempts at regulation have also not been lacking in Europe. In the UK, one of the major attempts was initiated by former prime minister, David Cameron, who in 2013 asked major internet service providers (ISPs) to implement filters that restrict all adult content for minors. Parliament never passed the regulations because ISPs self-regulated by giving consumers this option. However, the plan did not go exactly as expected. The 'protected' networks introduced by ISPs mainly censored specific keywords, resulting in the indiscriminate blocking of educational and anatomical content, for instance.

A few years later, Ofcom, the UK's communications regulatory authority, published a report on the experiment's results (Ofcom 2018). The adoption of the filter did not exceed 10 per cent, reaching 25 per cent only for those

ISPs that decided to activate it as the default setting for customers who had not made a decision about it. This was done without considering that, despite the filter, there were other ways to access pornography. Ofcom also highlighted a simultaneous surge in the use of VPNs between 2013 and 2015. In 2019, the government passed the Digital Economy Act, which, among other things, mandated that adult content websites request users to declare their ages. In practice, this translated to a checkbox stating, 'I am 18 years old.' One click, and you are in.

Finally, in September 2023, the Online Safety Bill was approved after a two-and-a-half-year-long process. Over the years, the length of the law has more than doubled to about 300 pages, and its scope has expanded to include age verification for accessing pornographic websites – nearly a decade after the UK government's initial attempts to introduce age verification. To prevent minors from accessing 'potentially harmful content', websites will have to verify visitors' ages, either by requesting government-issued documents or using biometric data such as facial scans to estimate their age. Special measures to restrict children's access to content require age verification, which, as it did ten years ago, has raised concerns about user privacy protection. The law has tasked Ofcom with studying the matter and creating a code of conduct to establish what methods, verifications, or estimates are required and in which contexts.

As for the EU, there is no specific and uniform regulation across all member states yet. Generally, pornography is legal but subject to rules aimed at balancing the protection of 'public morals' with freedom of expression. In most member states, illegality arises only when pornographic content is publicly displayed without safeguarding the privacy of non-consenting parties and without systems for the protection of minors. Therefore, access to pornographic images must be restricted to adults who request them, and adult websites must provide the usual neutral, initial banner warning of adult content, with the option to access it only upon a (unverifiable) self-declaration of legal age. There are also some general principles, such as the protection of minors and the prohibition of child pornography, subject to international directives and conventions, which EU member states have progressively ratified and implemented. Additionally, in recent years, different forms of regulations have been initiated – and in some cases concluded – concerning various aspects of the digital ecosystem, which, among other things, also affect adult websites.

In this regard, the recently approved Digital Services Act (DSA) also applies to adult content platforms. However, as of today, the European Commission is engaged in an investigation exercise to establish an inventory of the platforms involved, and apparently, these platforms are not particularly cooperative. Pornhub is ranked among the top fifteen most-visited websites in many EU countries, according to external estimates.[5] However, in August 2023, Pornhub stated that only 33 million Europeans visit its site every month.[6] YouPorn claimed to have just over 7 million users in the EU. The European Commission has publicly requested that platforms that have not yet disclosed their monthly traffic figures do so immediately, but the problem remains of what to do with those who do not comply or provide numbers that are difficult to believe.[7]

5 'Pornhub.com', *Similarweb*, September 2023 (https://www.similarweb.com/website/pronhub.com/#overview).
6 'EU Digital Services Act', *Pornhub*, 31 July 2023 (https://it.pornhub.com/information/eu_dsa).
7 'Brussels gears up to tame unruly porn platforms', *Politico*, 17 February 2023 (https://www.politico.eu/article/online-porn-websites-europe-regulation-age/).

Upcoming regulations: Age verification and preventive moderation

A common challenge faced by policymakers in the West when it comes to regulating online pornography is effectively putting their intentions into action. This is not coincidental. As we saw at the beginning of this study, the history of pornography is marked by constant innovation and stigmatisation, and both of these characteristics do not facilitate effective regulation. However, these challenges have not pushed Western regulators to find alternative ways to regulate adult content on the web. The primary objectives remain the same – enforce user age verification and implement platform-level content controls. On both these fronts, initiatives are moving swiftly on both sides of the Atlantic, but the perennial issues persist – lofty goals and ineffective means.

Age verification

Since January 2023, anyone residing in Louisiana who opens an adult website has been informed that state laws require proof of legal age to access the site. Those wishing to access the content are redirected to a state-administered website where they can upload their identification. In recent months, three other US states – Mississippi, Virginia, and Utah – have adopted the Louisiana approach by enacting their own age verification laws. Additionally, eleven public administrations, from Virginia to California, have proposed legislation requiring users to confirm their age before viewing adult material.

In all the involved states, laws have been proposed or passed with broad consensus (in Utah and Arkansas, they were passed unanimously) and

they have been signed into law by both Democratic and Republican governors. Age verification for pornographic content has thus become a bipartisan issue, and unlike previous efforts to limit its distribution, these laws are not merely symbolic. In Utah, Mississippi, and Virginia, the world's largest platform, Pornhub, temporarily ceased operations. During this brief period, users attempting to visit the site were greeted by a video of a porn star, fully clothed, explaining the platform's decision not to operate in that state.

The fact that Pornhub resorted to such an extreme measure may be surprising. In recent years, the platform has verified the age of approximately half a million content uploaders, a policy implemented after a *New York Times* article revealed that the site has repeatedly hosted videos of abuse and non-consensual activities. However, the scale of implementing age verification for each site user is quite different. The Free Speech Coalition, which represents the adult industry sector in the US, has initiated legal action against Louisiana and Utah and could do the same in other states that have enacted similar laws. It argues that age restrictions, aside from potentially violating the First Amendment, are ineffective because people can still use VPNs and access illicit platforms that are not subject to control.

On the other side of the Atlantic, the situation is no less convoluted. Within the EU, the Audiovisual Media Services Directive requires the adoption of adequate measures, including age verification, to protect minors from harmful content. Furthermore, Article 8.2 of the GDPR implicitly establishes the need for 'controllers' to set a minimum age requirement for minors to provide valid consent for data processing in the context of information society services where consent is required legally for data processing.

The first country to attempt to turn the age verification debate into concrete regulatory proposals was France. In October 2021, the parliament unanimously approved Decree No. 2021–1306, published based on the powers granted by Article 23 of Law No. 2020–936, which aims to protect victims of domestic violence. Article 23 and the decree stipulate that any 'operator of public online communication' offering adult content to the public must implement an age verification system. In case of violations, the law introduces a process that is led by the national audiovisual regulator (Arcom), which can impose penalties and, through a judge's order, even suspend the service.

While the choice of age verification mechanism used is left to the platforms, the law recommends the use of credit cards, a system that, as previously highlighted, was adopted and then abandoned by the UK due to technical difficulties and privacy compliance issues. Some senators also suggested using FranceConnect, a digital identification tool developed by the government for accessing certain public services, such as tax collection and healthcare insurance.

Even before its approval, various experts expressed concerns, including the French privacy regulator, Commission Nationale Informatique and Libertés (CNIL) (CNIL 2021). The CNIL pointed out that Article 23 applies to any service and essentially extends to almost any site or platform that allows user-generated content, even if adult content is not its primary activity. The obligation that visitors to any site offering adult content, even incidentally, should provide age verification was not justified by the legitimate purpose of protecting minors. According to the CNIL, accessing online communication services without being obligated to identify oneself and being able to use pseudonyms contributes to the freedom of information and user privacy protection, and any limitation should be adequately proportionate to the intended objective.

In its opinion, the CNIL also draws attention to the fact that implementing technical processes aimed at verifying user ages could involve the processing of personal data, which should comply with the GDPR. These technical processes should meet the requirements set out in Article 5.1c of the GDPR – they must be proportionate to the intended purpose. The CNIL also references the European Data Protection Board's guidelines on consent, which emphasises online service providers' obligation to verify user ages and secure parental consent and make 'reasonable efforts' in this regard, taking into account available technologies.

The CNIL suggests the following additional criteria for age verification processes to be fully compliant with privacy laws:

- The collection of users' personal data solely for age verification purposes should not be allowed. CNIL notes that this would be contrary to GDPR principles, as it would pose a significant risk that such data could be used to deduce sexual orientation, real or presumed, inferred from the content consumed, or that third parties could gain access to such a database, which would have a disastrous impact on the individuals involved.

- Any age verification system must be operated by a third party that conducts anonymised verification, preventing this third party from (i) identifying the platform in question and (ii) sharing users' personal data with that platform. This third party should comply with all data protection regulations, especially regarding information about data processing risks and rights.
- In any case, no GDPR-compliant age verification system should involve (i) the collection of government documents due to identity theft and misuse risks; (ii) age estimation based on browsing history; and (iii) biometric data collection as per Article 9 of the GDPR since, in such a case, consent would not be freely given but rather a mandatory condition for accessing content.

Despite the CNIL's opinion, the law was approved and is currently in force. On 13 December 2021, the president of Arcom (then called Higher Audiovisual Council, CSA) formally requested a few pornographic websites (Pornhub, Tukif, xHamster, Xvideos, and XNXX) to take necessary measures within fifteen days to prevent minors from accessing their platforms, citing the ineffectiveness of the self-declaration process. The platforms appealed, and after years of legal battles, in July 2023, the Paris court postponed its final decision on the legality of the law until the Constitutional Council made a ruling.

To avoid further legal delays, the French government is now seeking to empower Arcom to act more swiftly. After the verdict's postponement, French senators supported a bill that would enable Arcom to compel internet service providers, search engines, and app stores to block adult sites that do not provide adequate age verification, effectively shifting the responsibility from the platforms to the broader internet ecosystem. The bill is set to be debated in the National Assembly by the end of 2023.

Over the years, the CNIL has returned to the issue, offering in-depth analyses of the various proposed age verification systems and potential alternative solutions (CNIL 2022). According to the authority, age verification, in practice, involves the following three separate operations:

1. Producing 'proof' of one's age, which can be issued by various entities that, in some way, know the user. These entities could be specialised identity providers or third-party organisations such as a bank or an e-commerce platform.

2. Transmitting this certified age proof to the visited site, allowing it to grant or deny access to the requested content.
3. On receiving the proof, the visited site can then grant or deny access to the user.

These three aspects entail significant data protection and privacy concerns, especially for the ability to use the internet without revealing one's identity or direct identification data. Entrusting these functions to different parties would provide a triple layer of privacy protection:

- The entity providing age proof knows the user's identity but does not know which site they are visiting.
- The entity sending age proof to the site may know the site or service the user is visiting but does not know the user's identity.
- The site or service knows the user's age (or only their legal age) and is aware that they are visiting the site, but it does not know their identity and, ideally, the age verification service used.

Throughout 2023, the issue has become increasingly topical in European countries such as Italy and Spain. In Italy, the Italian Data Protection Authority requested information from Pornhub, and age verification is identified as one of the potential violations of privacy laws.[8] Just a few months earlier, the same authority and the Italian telecommunications regulator, AGCOM, established a joint panel intending to promote a code of conduct that encourages digital platforms to implement age verification systems. In Spain, the Spanish Data Protection Agency (AEPD) announced the development of an age verification and content filtering system based on the presentation of identification documents, believing that the existing legal framework already allows companies to require age verification for their users.

Despite this new and strong wave of attempts to introduce age verification systems for pornographic sites, the concept remains questionable in theory and complex to implement. Concerns regarding underage users' uncontrolled access to adult content are understandable and widespread; less common is an understanding of the significant limitations and new risks that various proposed age verification tools present.

8 'Pornhub under the lens of the Garante. The Authority requests clarifications on user profiling and tracking systems', *Garante per la Protezione dei Dati Personali*, 11 July 2023 (https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9908249).

As emphasised by CNIL, the use of tools such as credit cards, facial recognition forms, or identity documents is insufficient to mitigate the risks associated with current mandatory age verification proposals:

1. Effectiveness: In theory, mandating age verification is not difficult. In practice, ensuring compliance is practically impossible. As seen in the UK, users may shift to using VPNs and other systems to circumvent controls, with the paradoxical risk of fueling traffic to less monitored and less secure platforms and applications.

2. Uniformity: Acting based on the criteria that have inspired regulations such as the DSA, and setting criteria for identifying sites and platforms to be regulated ex-ante, would greatly complicate compliance, and risks leaving those less visible less monitored and essentially irresponsible. Moreover, a form of global control is currently simply inconceivable.

3. Privacy: Currently, the primary age verification systems on the market are fundamentally at odds with the GDPR, the fundamental regulation for personal data protection in Europe. In particular, the GDPR requires adherence to the principle of proportionality, where there should be a correspondence between the number and type of personal data requested from a service user and the risk associated with the unavailability of that data. Can one truly believe that access to adult content is more dangerous for a minor than the existence of a vast database cataloguing the personal data of everyone accessing pornographic websites, categorised by site and frequency of access?

Preventive moderation

We have already discussed Section 230 of the Communications Decency Act and its importance for the development of the internet. As previously mentioned, in the US, Section 230 establishes that online platforms that host third-party content are not responsible for what these third parties post (with some exceptions[9]). This third-party content can include reader comments on a news website, tweets on Twitter (now X), posts on Facebook, photos on Instagram, or reviews on TripAdvisor. For example, if a reviewer on TripAdvisor posts a defamatory review, the subject of the

9 For example, in 2018, two laws were enacted. These were Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) and the Stop Enabling Sex Traffickers Act (SESTA), which amended certain parts of it, extending platforms' liability for advertising related to prostitution services posted by third parties.

review could sue the reviewer for defamation, but, thanks to Section 230, they cannot sue TripAdvisor.

Section 230 has another side to it, as it allows platforms to limit access to any content they consider contrary to their internal policies. In other words, platforms can decide what is acceptable or not, and they can choose to host or moderate content accordingly. This means that when individuals who are suspended or banned from these platforms claim that their right to freedom of expression has been violated, it does not hold. Platforms are shielded from any liability for user-generated content, and they can moderate it as they see fit.[10]

This protection has undoubtedly allowed the internet to thrive. Websites such as Facebook, Reddit, and YouTube have billions of users; if they had to monitor and approve every single piece of user-generated content, they simply would not function. No platform will take on the legal responsibility of pre-moderation, but on the other hand, a site that moderates nothing will quickly be overrun by spam and unwanted content.

Today, Section 230 is under attack like never before, and this latter aspect related to content moderation is the main reason for increasingly frequent proposals to reform or, in some cases, repeal it altogether. Some of its critics argue that it gives platforms too much immunity, making the internet increasingly extreme and polarised. Others claim that it has made platforms too influential and capable of suppressing and censoring content based on their whims or political biases. Depending on whom you ask, internet platforms are either using the powers Section 230 has granted them too much or too little. In both cases, the platforms are accused of hiding behind it to shield themselves from taking any responsibility.

In the US, the federal government, Congress, and the Supreme Court have intervened several times in recent years to introduce changes to Section 230, and the debate has not yet ended. In 2018, a group of Republican senators led by Ted Cruz proposed that Section 230 should only apply to online platforms if they are ‘neutral public forums’, alluding to the idea that Facebook, for example, might not be neutral and may pursue a progressive

10 Paragraph (C)(2) of Section 230 states that ‘no provider or user of an interactive computer service shall be held liable for (...) any action voluntarily taken in good faith to restrict access or availability of material that the provider or user considers to be obscene, lewd, lascivious, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected or not’.

political agenda.[11] In May 2020, after Twitter labelled one of his tweets as 'potentially misleading', Donald Trump signed an executive order directing the Department of Justice to amend Section 230 to allow an online service provider to restrict access to user-generated content only if the provider had terms of service that explicitly prohibited such content, the action was consistent with those terms, the provider provided a reasonable explanation to affected users, and the affected user had an opportunity to appeal the decision. In May 2021, shortly after taking office, President Biden revoked Trump's executive order. This, however, does not mean that Biden is a supporter of Section 230; during his presidential campaign, he even expressed the intention to repeal it.[12]

Due to the federal government's inaction, some Republican-led states have taken independent steps against Section 230. In 2021, Florida passed the Stop Social Media Censorship Act, which prohibits platforms from suspending the accounts of politicians or media outlets. In the same year, Texas passed HB 20, which prohibits platforms from removing or moderating content based on the user's viewpoint. Neither of these laws is currently in effect, as both are awaiting constitutional judgments by the Supreme Court.

Meanwhile, Europe is facing similar political issues but with a different legal and governance framework. The EU's approach to intermediary liability was first established by Directive 2000/31/EC, also known as the e-Commerce Directive (ECD), similar to Section 230; the ECD provides full liability protection for so-called 'passive' online services. The directive also prohibits member states from imposing general monitoring obligations on providers of information society services, defined as a 'service normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services.' The full protection provided by the ECD does not extend to online services that play an 'active' role in organising content. Although it does not contain an explicit distinction between 'active' and 'passive' services, Articles 13 and 14 of the directive stipulate that active services should promptly remove illegal or harmful content once they become aware of it.

11 'User clip: Ted Cruz questions Mark Zuckerberg', *C-Span*, 10 April 2018 (https://www.c-span.org/video/?c4722670/user-clip-ted-cruz-questions-mark-zuckerberg).

12 'Biden wants to get rid of law that shields companies such as Facebook from liability for what their users post', *CNBC*, 17 January 2020 (https://www.cnbc.com/2020/01/17/biden-wants-to-get-rid-of-techs-legal-shield-section-230.html).

Faced with the new challenges posed by the growth of large online platforms, the European Commission has recently reformed the legal framework provided by the ECD through the DSA, which came into effect in August 2023. The DSA retains the provisions of the ECD but adds a range of new obligations for online service providers, including:

- Compliance with orders from EU member states to remove illegal content from their platforms and provide information collected about the users of the online service.
- Due diligence obligations, including identifying points of contact for EU member states, appointing a legal representative in the EU, annual reporting on content moderation, and the creation of internal systems for dispute resolution.
- Suspension of users who frequently post illegal content.
- Transparency regarding the funders of advertising content.

Regarding intermediary liability, the DSA focuses on increasing transparency with regards content moderation decisions while maintaining the ban on general monitoring obligations. However, the generally positive feedback the DSA has received is not shared by many civil rights organisations, with several expressing concerns about the impact of the new rules on freedom of expression, primarily due to the extremely pervasive role granted to national governments and the European Commission in enforcing the new regulations. This is especially relevant in the case of the pornography sector, which is often subject to checks and legal actions due to the presence of illegal content.

There have been attempts at regulating certain problematic aspects of pornography at the community level. An example is non-consensual intimate imagery (NCII), which refers to uploading videos or images to pornographic platforms without the consent of the individuals involved. During discussions on the DSA in early 2022, there was a proposal to introduce Article 24b, which, with the aim of limiting NCII, would require anyone uploading content to adult platforms to verify their accounts with a phone number and an email address. The article would also have required platforms to hire and train specialised moderators to remove content reported by victims ‘without undue delay’.

In the end, the European Parliament set aside the idea, as it conflicted once again with the right to privacy and freedom of expression of users.[13]

A few months later, in May 2022, the Commission proposed a new regulation on the possession and exchange of child sexual abuse material (the so-called child sexual abuse material (CSAM) regulation), with the aim of harmonising the legal framework to provide 'legal certainty for providers regarding their responsibility to assess and mitigate the risks and, where necessary, to detect, report, and remove such abuse on their services' (European Commission 2022). Among other things, the regulation would require certain 'particularly risky' platforms to proactively screen their content to prevent the presence of child pornography at the source.

The intent, of course, is laudable. The challenge, however, is in establishing appropriate boundaries to ensure its compatibility with the prohibition of general and indiscriminate monitoring introduced in the European legal framework by the ECD and confirmed by the DSA. The legal service of the European Council, when asked to provide an opinion on the regulation proposal, pointed out serious risks of collision with the right to privacy and freedom of expression.

Specifically, the legal opinion of the Council emphasises that the limitation to particularly risky platforms is not a significant limitation, as it still requires a general screening of users. The opinion also warns that the net effect of this approach risks leading to a situation where all providers of interpersonal communication services are subjected to surveillance orders. The document notes that:

> Interpersonal communication services are used by almost the entire population and can also be used for the dissemination of CSAM and/or the solicitation of minors. Surveillance orders directed at these services would entail a variable but in almost all cases very broad, scope of automated analysis of personal data and access to personal and confidential information concerning a very large number of persons who are not, even indirectly, involved in sexual offences against minors.

This concern is further supported by the fact that the proposed regulation does not provide substantial guarantees to prevent the risk that the

13 'Europe has traded away its online porn law', *Wired*, 27 April 2022 (https://www.wired.co.uk/article/digital-services-act-deepfake-porn).

cumulative effect of indiscriminate surveillance orders by national authorities in different member states may cover all active interpersonal communication services in the Union. Moreover, since issuing a surveillance order against a specific provider carries the risk of encouraging the use of other services, there is a clear risk that, to be effective, surveillance orders would have to be extended to other providers, effectively leading to permanent surveillance of any form of online content sharing.

Another path: Collaboration and innovation

The online pornography industry finds itself in a challenging position. On the one hand, the digital sector and potential suppliers and partners as a whole are rather reluctant to acknowledge its value, even though they are fully aware of its historical and current contribution to the internet. On the other hand, adult content is the preferred target of policymakers when it comes to attempting to limit or regulate access and consumption of online content.

This study hypothesises that, paradoxically, it is precisely this condition of social isolation and pressure, coupled with broad and urgent demand, that has driven the innovations that, as we have seen, have marked and continue to mark online porn history. Fundamental elements of online security that are now considered integral to the rest of the internet, such as payment security and content moderation, were essentially developed by the pornography sector before anyone imposed it, suggested it, or made it easy.

This does not mean that the online pornography industry is without problems. Child pornography and the non-consensual sharing of intimate material are far from being resolved. At the same time, it is undeniable that unrestricted access to adult content, regardless of age, poses risks that, with a bit of goodwill, can be better mitigated.

The point is not what but how. As we have seen, adult content was the first target of internet regulations. This is partly due to politicians' tendency to promise the impossible without fully understanding the dynamics of what they are trying to regulate and without giving sufficient consideration to the side-effects of the proposed solutions. Moreover, the adult industry

has undoubtedly done everything in its power to fuel mistrust and lack of understanding by adopting an ambiguous and uncooperative approach that has lasted for decades.

However, something is changing in this regard. A few months ago, MindGeek (now renamed Aylo and including platforms such as Pornhub, Youporn, Xhamster, and others) was acquired by a Canadian fund with an unequivocal name: Ethical Capital Partners.[14] The fund, created just a year ago, has publicly stated that it aims to clean up its image and that of the industry in general, starting with the ethics and accountability of its management. At the same time, the new owners believe that the moderation and security tools developed by the company are best practices that can be reused by the rest of the internet. Thus, the focus will be on transparency and sharing.

If this approach is followed by concrete actions, it could catalyse the entire industry, as it has the potential to start a new chapter in the regulation of pornography and the web in general. On the other hand, institutions should adopt a different approach, focusing on the goals to be achieved but also taking into account some of the following fundamental principles:

1. The internet is global in nature. Imposing national constraints is ineffective at best and counterproductive at worst. Similarly, focusing regulation on so-called more collaborative and transparent platforms runs the risk of making them bear the burden of compliance, directing traffic towards much less controlled and secure environments.

2. Privacy is not a trifle. Most attempts to strengthen control over users and content on adult platforms have clashed with privacy issues. In many cases, these attempts has led proponents and commentators to criticise the balance between that right and the right, for example, of a revenge porn victim to not have their intimate videos circulate online. However, these comparisons are not correct. The privacy right, in these cases, concerns all users and 'legitimate' content and assumes importance precisely because it refers to such a personal sphere as visiting an adult website.

3. The Good Samaritan clause has many merits. The US Section 230 and the European rules inspired by the e-commerce directive

14 'ECP announces acquisition of MindGeek, parent company of Pornhub', *Aylo*, 16 March 2023 (https://www.aylo.com/newsroom/ecp-announce/).

have made the development of the platform economy possible, generating hundreds of millions of jobs and fueling much of the world's economic development over the past twenty years. This does not mean that it cannot and should not be improved, but the first goal of those who want to improve it should be to do no harm. The fact that the accusations against the Good Samaritan principle come from opposing sides (those who want it to be much more incisive on one side and much less on the other) is a sign that it is perhaps not too far from the right balance.

4. Pornography is legal. Morality should certainly be able to influence individual choices, but not the law. Pornography, as long as it is consensual, is a phenomenal form of entertainment and should not receive different treatment from other forms of entertainment.

5. Innovation is not by decree. As we have seen, pornography has been an extraordinary engine of innovation in protecting its content and users. Instead of imposing technological solutions on the sector, institutions should define the goals to be achieved and allow companies to reach them within a reasonable timeframe with solutions developed in line with their infrastructure and strategies.

With respect to age verification, one can only hope that the forthcoming regulation on this issue in Europe – specifically in France, Italy, and Spain – takes these principles into account and follows the approach of CNIL, which aims to ensure a high level of data protection and privacy in accordance with GDPR principles while also limiting minor's access to inappropriate content. Collaboration between different entities and the adoption of concrete, effective technological solutions will be crucial in achieving this goal.

Regarding the application of the DSA and the CSAM Regulation, the text of the latter raises concerns about the de facto obligation placed on platforms to monitor content, with the reference to 'particularly risky platforms' not providing much reassurance without a clear and comprehensive definition. Such an approach may lead to a situation where any provider of interpersonal communication services ends up having to (or wanting to) carry out general and preventive monitoring of their platforms to avoid violating the regulation. This could involve extensive automated analysis of personal data and accessing the personal and

confidential information of people who are certainly not involved in child sexual exploitation crimes. Finally, the proposed regulation does not offer sufficient guarantees to ameliorate the risk that the indiscriminate application of monitoring orders by different national authorities could cover all interpersonal communication services in the EU, with the paradoxical effect of punishing those entities that want to offer compliance and cooperation.

History teaches us that for any technological or regulatory problem, pornography, as a 'boundary' sector, normally addresses it a few years ahead of the rest of the internet. As we have seen, it has been a pioneer in copyright protection. It was the first to develop user consent collection systems for the collection and use of personal data several years before the GDPR. It had to comply with laws on the production and distribution of adult material, leading to the implementation of content moderation protocols that have inspired the rules applicable to other platforms today. It had to introduce anonymous and secure payment systems, influencing the adoption of similar measures in e-commerce and online payment platforms.

Thus, regulating pornography appropriately is not only just in itself, but it is also useful to ensure that the internet remains a place of extraordinary freedom and innovation without necessarily implying impunity and unaccountability for those who use it to commit illegal acts. While proposals for age verification and content moderation on adult websites are emerging in Europe, it is important to reflect on the possible risks and the potential impact of these measures if they are extended to the rest of the internet.

For example, mandatory age verification could significantly increase the amount of sensitive data held by third parties and the frequency at which it is collected, exposing users to privacy breaches and abuse. Similarly, the goal of content moderation on online pornography sites is to prevent the spread of harmful or illegal material, but a general monitoring obligation beyond pornography sites could result in censorship and limitations on freedom of expression. While it is essential to address issues related to age verification and content moderation on online pornography sites, it is equally important to consider the risks that may arise from inappropriate regulation and the potential extension of this approach to the rest of the internet. Protecting privacy and freedom of expression, and the need to avoid excessive control of online content, are all crucial aspects to consider.

The next major technological challenges – artificial intelligence and the metaverse, among others – will generate new problems that, in turn, will require the development of new rules. Hopefully, with the goodwill of both the industry and institutions, the future will value technological solutions produced by the sector, leading to the creation of a simple, non-discriminatory regulatory framework built around them, which is effective in combating pathological aspects without compromising the fundamental rights of its users.

List of references

Barss, P. (2011) *The Erotic Engine: How Pornography has Powered Mass Communication, from Gutenberg to Google*. Woodbridge: Anchor Canada.

Calvert, C. and Richards, R. (2001) Larry Flynt uncensored: A dialogue with the most controversial figure in First Amendment jurisprudence. *Commlaw Conspectus* 9: 159–74.

CNIL. (2021) Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy. In *8 Recommendations from the CNIL*. Paris: CNIL.

CNIL. (2022) *Online Age Verification: Balancing Privacy and the Protection of Minors*. Paris: CNIL.

Eisenberg, B. H. (2013) A speedbump on the information superhighway: pushing copyright law into the online era: Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993). *The Florida Historical Quarterly* 92(2): 337–50.

European Commission. (2022) *Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse*. Brussels: European Commission.

Kosseff J. (2019) *The Twenty-Six Words that Created the Internet*. 2019. Ithaca: Cornell University Press.

Johnson, P. (1996) Pornography drives technology: Why not to censor the internet. *Federal Communications Law Journal* 49(1): Article 8.

Lane F.S. III. (2000) *Obscene profits: The entrepreneurs of pornography in the cyber age*. New York: Imprint.

Ofcom. (2018) *Addressing harmful online content. A perspective from broadcasting and on-demand standards regulation*. London: Ofcom.

Perdue L. (2002) *EroticaBiz: How sex shaped the internet*. Wallingford: iUniverse.

Stevens J.P. (1997) *Slip opinion on 'Attorney General of the United States, et al. v. American Civil Liberties Union et al.'*. Washington: Syllabus of the Supreme Court of the United States.

EPICENTER
European Policy Information Center

ibl
Istituto Bruno Leoni