What the EU Should Put in the Digital Services Act

By Daniel Castro and Eline Chivot | January 2020

INTRODUCTION

The eCommerce Directive—a critical building block of the EU's digital economy—is in need of modernization, but updates should continue to remove obstacles to online commerce and provide legal certainty to businesses and citizens.

The Internet has been a major driver of economic growth. Internet intermediaries—web hosts, search engines, e-commerce sites, social media sites, payment processors, ad networks, and more—have played a key role in facilitating this growth and enabling firms of all sizes to maximize the benefits of the Internet economy. Many Internet intermediaries, such as Amazon, Facebook, and Google, are among the world's most successful companies—and both their success and the benefits consumers have gained through their services have been aided by legislation that shields Internet companies from excessive liability for third-party content. In the European Union, this legislation is the eCommerce Directive.[1]

The eCommerce Directive, which went into effect in 2000, created a set of standard rules for liability of online intermediaries. These rules protect online services from being unfairly targeted for the content of their users. For example, these rules ensure travel-booking and online shopping sites are not held liable for user reviews, and social networking sites are not held liable for content posted by users.

The robustness of these protections is being challenged in the EU through legislative proposals that could expose Internet companies to significant liability.[2] Growing concerns about issues such as hate speech and disinformation are pressuring policymakers to enact reforms to the policies that set the basic rules for platform liability. But substantially reducing current liability protections could cause serious negative repercussions for the EU economy, as well as for the availability of online services and products consumers currently have access to. Overly prescriptive rules and one-size-fits-all solutions could have unintended consequences, including restricting innovation, hampering growth, and limiting consumer choice.

REFORMING THE ECOMMERCE DIRECTIVE

The new European Commission's policy agenda includes the Digital Services Act: legislation that would establish new liability and safety rules for digital platforms, services, and products.[3] The Digital Services Act also outlines plans to regulate content on intermediary service providers by addressing content moderation, data sharing and usage, and regulatory oversight. The Digital Services Act could revise or repeal the eCommerce Directive, or create a new set of regulations for Internet intermediaries.

Against this background, EU policymakers aiming to update the current liability regime should carefully consider how existing rules enable both valuable user-generated content on platforms and access to online products and services consumers value, as well as the impact reducing liability protections of online platforms could have on the availability of these online products and services. This does not mean the EU should not consider changes; but it should move cautiously and incrementally. Moreover, the online ecosystem has significantly evolved since the EU adopted the eCommerce Directive in 2000, so its primary efforts should focus on updating rules and modernizing definitions so as to ensure regulations maintain a proper balance in the roles and responsibilities of online intermediaries, and protect consumers and avoid unnecessary penalties on digital platforms and other stakeholders.

With that in mind, to promote EU competitiveness in the digital economy, the EU should create a Digital Services Act that does the following:

- Clarifies the definitions of illegal information and illegal activity,
- Extends liability protections beyond "passive" services,
- Harmonizes the scope of covered online services,
- Holds companies responsible for timely removal of illegal content,
- Balances roles and responsibilities between the public and private sectors,
- Preserves the prohibition on monitoring obligations,
- Incentivizes adoption of standard technical measures,
- Increases online platform transparency,
- Harmonizes rules at the EU level to create regulatory consistency,
- Pursues nonregulatory solutions, and
- Phases in new regulation at a reasonable pace.

CLARIFY THE DEFINITIONS OF ILLEGAL INFORMATION AND ILLEGAL ACTIVITY

The eCommerce Directive requires Internet companies to take down "illegal information" and "illegal activity," but does not describe precisely what those include. EU policymakers should clarify these terms so there is no ambiguity. For example, the new framework should include and define prohibited practices such as copyright and trademark infringement, solicitation to commit a crime, incitement to violence, and the distribution of nonconsensual or child pornography.

EU policymakers should not include in the Directive's definitions content and behavior—such as certain forms of disinformation, harassment, and hate speech—that may be undesirable but are not typically illegal in Western democracies, as it would be inappropriate for the government to require companies to remove online content that would be lawful offline. Unfortunately, a number of policymakers have proposed this type of two-tiered system. For example, in 2019, the U.K. government produced the Online Harms White Paper, a proposal to create a new law to address online harms that would be overseen by an independent regulator.[4] This regulator would be authorized to establish a code of practice that provides guidance to companies on how to respond to certain activity and content, including those that are "not necessarily illegal."[5]

Many platforms can and will voluntarily impose community standards that restrict offensive and outrageous—yet lawful—speech. However, these decisions should be left to Internet platforms, in the same manner retailers, performance venues, and art galleries decide which lawful goods, performers, and artists to permit, rather than allow government to play the role of censor. Doing so would not only uphold free speech values, but allow these platforms the opportunity to use alternative measures, such as counterspeech ("the dissemination of messages that challenge, rebut, and disavow messages of bigotry or hatred"), that may be more effective at responding to certain types of problematic online speech.[6] Another reason for allowing platforms to set standards for user content rather than using laws is what speech is considered illegal varies by member state. Different countries place different limits on free speech. France and Germany, for example, have laws prohibiting anti-Semitism and other forms of hate speech, and Spain and the Netherlands have lèse-majesté laws that prohibit insulting the monarchs. While Internet platforms should take down content that is illegal in these jurisdictions, even if it would not otherwise violate their content policies, they should not be compelled to take it down for users in other countries where the content is legal.

It is important the definitions in the new framework be precise and unambiguous so as to reduce uncertainty for companies and avoid unintentionally making legitimate content illegal. Unclear definitions of

illegal content would make it more difficult for companies to determine which content they should restrict from their platforms. Moreover, this uncertainty would likely pressure Internet companies to remove lawful content, and deter users from engaging in lawful speech for fear they might run afoul of the law, thereby undermining freedom of speech.

EXTEND LIABILITY PROTECTIONS BEYOND "PASSIVE" SERVICES

The eCommerce Directive makes a distinction between "passive" and "active" online services, and only extends liability protections to service providers that "play a neutral, merely technical and passive role" toward hosted content. In practice, this means hosting providers are the primary beneficiaries of this liability protection. Policymakers should abolish this distinction for two reasons. First, the difference between passive and active service providers is vague, making unclear to many service providers whether they receive this liability protection. Second, in order to create a level playing field between different types of online services, service providers should receive this liability protection for content they neither produced nor had actual knowledge of being illegal.

The new framework should extent to more than just hosting providers, and account for the diversity of online services. For example, some services may host, cache, or transmit user content, while others may perform these actions but do so without visibility because the content is encrypted. Some services may use humans to manually moderate or manipulate user content, while others may use automated mechanisms. Extending liability protection to all of these online services would allow service providers to continue to evolve and experiment with new features in order to attract and engage more users, without concerns over these innovations causing them to lose their liability protection.

HARMONIZE THE SCOPE OF COVERED ONLINE SERVICES

The current framework does not make clear which intermediaries receive liability protections. For example, the eCommerce Directive only applies to intermediaries that qualify as "information society services"—and individual member states have been free to exclude search engines and other sites that provide indexes or directories of links. Moreover, the online services ecosystem has significantly evolved over the past two decades. The EU should update and harmonize the scope of covered online services to include a broad range of online intermediaries, including Internet service providers, cloud services, content delivery networks, domain name service providers, social media services, search engines, directories, collaborative economy platforms, online marketplaces, online advertising services, discussion boards, digital services built on electronic contracts, and distributed ledgers (i.e., blockchain).

HOLD COMPANIES RESPONSIBLE FOR TIMELY REMOVAL OF ILLEGAL CONTENT

While companies should not be liable for user content, they should always be responsible for removing or disabling access to illegal content once they learn about such material on their services. The new framework should create penalties for service providers that consistently fail to respond appropriately to illegal content notifications, whether from government, companies, or individuals. While companies should always block or remove content legitimate government authorities determine to be illegal, they deserve some latitude when making subjective decisions about whether content reported by users violates the law or their own policies.

The eCommerce Directive directs service providers to take action "expeditiously," but that term is not defined precisely and should be clarified.[7] The new framework should specify a timeframe for companies to respond in cases of serious harm—such as content that incites terrorism—but these timeframes should be reasonable and practical. Policymakers should avoid creating excessive penalties for service providers not responding within short timeframes that may be impractical to comply with. For example, Germany's Network Enforcement Act, known as "NetzDG," which came into effect in January 2018, requires social media sites to remove illegal content flagged by users within 24 hours or face fines of up to €50 million.[8] The French Parliament also passed a similar law in 2019 that allows for fines of up to 4 percent of global revenue.[9] These time constraints are impractical even for large platforms—and even more unworkable for smaller ones. EU policymakers should resist copying such proposals because requiring service providers to respond too quickly, or holding them liable for occasionally failing to block flagged content they initially do not believe to be unlawful, will likely cause them to block more content than necessary.

In addition, requiring online services to remove illegal content under tight deadlines would force many companies to use automated content-moderation systems rather than humans. While this may be appropriate and reliable in many cases, it may not be in others. Content-moderation technology is constantly evolving and improving, but today there are limitations, and many systems cannot detect nuance and subtlety of meaning, which would likely result in these systems mistakenly blocking legitimate content.

The United Kingdom's Online Harms White Paper also proposes imposing personal civil and criminal liability on senior executives of online services when their companies fail to respond appropriately to removing objectional user content.[10] Such penalties would constitute a significant financial and reputational risk that could both make it harder for these companies to attract top executives, and hinder entrepreneurship. Moreover, imposing

civil penalties on companies themselves, rather than on the executives, should suffice to achieve the desired objectives and keep businesses focused on protecting users from illegal online content rather than on protecting their executives from potential sanctions.

BALANCE ROLES AND RESPONSIBILITIES BETWEEN THE PUBLIC AND PRIVATE SECTORS

One critical aspect of any updates to the EU's liability framework lies in the division of the roles and responsibilities between the public and private sectors. The primary responsibility of online service providers should be to remove or disable access to content determined to be unlawful by the government, and to moderate all other content according to their own terms of service. Online service providers should not be tasked by the government with deciding whether user-generated content is legal. That should remain the responsibility of the government. This does not mean companies should ignore problematic content on their platforms. On the contrary, online services can and should make interim decisions about whether user content meets their internal content guidelines—and respond appropriately and promptly, especially when trusted partners report illicit activity on their platforms. But regulators should not hold companies responsible for correctly predicting whether government authorities will agree or disagree with their determinations. If companies were held liable for incorrectly predicting whether government authorities would find certain content to be unlawful, they would likely err on the side of caution and take down lawful content. Government should also not take on the role of setting guidelines for online content that would otherwise be legal if published offline, as this would unnecessarily suppress free speech online. Government should also not dictate the technology the private sector should use to moderate content, and instead allow companies to use their technical talent and resources to evaluate the best options. Finally, companies and users should have a right to appeal a government's decision to order content be removed, and be able to use this mechanism without restriction.

PRESERVE THE PROHIBITION ON MONITORING OBLIGATIONS

Not only does the current law limit the liability of online platforms for the content posted by their users, but it also does not obligate them to actively monitor their systems for illegal content. This is an important provision because many online platforms do not have the resources or capabilities to actively monitor all user content. Such a requirement could force online platforms—driven by fear of sanctions for unintentionally allowing offending content to slip through their moderation process—to err on the side of more-restrictive content-moderation policies, or even eliminate user-generated content altogether. Given the popularity of these features today,

this type of change would almost certainly reduce the value of online platforms for consumers. Therefore, any new framework should maintain the prohibition of active-monitoring obligations.

INCENTIVIZE ADOPTION OF STANDARD TECHNICAL MEASURES

The new framework should incentivize companies to employ standard technical measures (such as automated filtering systems) to mitigate illegal content. Policymakers should not increase the liability exposure of service providers that use these voluntary measures to detect and remove illegal content online. And online platforms exercising editorial control of user content should not be considered evidence they have actual knowledge of illegal content uploaded by users. To do otherwise would discourage companies from actively self-policing their own services for fear of losing their liability protection. The likely result of preventing services from actively moderating online speech would either be service providers restricting user-generated content entirely or refraining from all content moderation and giving free rein to users, thereby allowing social media sites to grow larger and more toxic, and streaming sites to include more pirated and terrorist content.

INCREASE ONLINE PLATFORM TRANSPARENCY

Instead of providing additional content standards, policymakers should require online services to provide more transparency about their policies and processes for responding to illegal content and the appeals processes available to users. Companies should release regular reports on their actions, such as the number of takedown requests received, the results of those requests, the number of appeals, and the time it took to respond to those requests. More transparency can help service providers dealing with particular problems, such as counterfeit products for online retailers, and identify best practices. However, similar services should not necessarily be legally obligated to replicate these measures, as not all companies have the same resources and technology available. Imposing additional requirements on companies without considering their differences could jeopardize the ability of many companies to operate. Moreover, policymakers should allow businesses to maintain their independence to determine their own policies, as long as those policies are compliant with the law.

This type of transparency can encourage more responsible behavior among online service providers by helping identify bad actors. It can also help responsible companies ensure they are using service providers with a good track record of responding appropriately to objectionable content. For example, the Internet security company Cloudflare finally bowed to public pressure and decided to stop providing service to 8chan (a discussion

board notorious for spreading child pornography and hate speech, including manifestos of mass shooters) after acknowledging the site's role in inspiring acts of mass violence, and the original site is no longer accessible (although 8chan operators have launched a successor).[11]

However, the new framework should not impose additional algorithmic transparency obligations on platforms that use automated processing and filtering technologies to moderate their content. Specifically, the new framework should not require companies to disclose proprietary details about their automated moderation systems, as these details could both expose intellectual property and aid those bad actors attempting to circumvent the rules. In addition, the new framework should not mandate companies use explainable algorithms, as that could prohibit the use of certain advanced artificial intelligence (AI) systems, thereby lowering the effectiveness of the automated moderation tools, as there are typically trade-offs between accuracy and explainability in AI.[12]

HARMONIZE RULES AT THE EU LEVEL TO CREATE REGULATORY CONSISTENCY

One of the major barriers to a digital single market is the patchwork of national rules for Internet services. For example, German and French laws differ on online hate speech. Further fragmentation would only introduce more complexity and uncertainty for companies, as policies may conflict with other countries' laws, and interpretations may diverge between national authorities. In addition, fragmentation prevents EU companies from scaling, which is a key success factor for companies operating in the digital economy. EU policymakers should take the opportunity to use the Digital Service Act to harmonize rules at the EU level to create a consistent regulatory process and avoid increasing policy fragmentation across member states.

As illegal online content is a cross-border issue, it should be addressed at the EU level, but EU policymakers should not allow the goal of a harmonized framework to enable individual member states to enforce their content regulations outside their borders. Within the EU itself, some member states criminalize certain types of speech, while others do not. EU policymakers should keep in mind enforcing one country's restrictions on online content outside of that particular country will infringe on freedom of speech and limit access to information in other nations. Where there are differences across the EU, member states' takedown requests should only apply domestically. A new framework should also be respectful of the global nature of the Internet by avoiding cross-border conflicts between both jurisdictions outside the EU that have tight speech standards and those that operate according to different standards. It should not require one platform to remove content globally based on either a national jurisdiction's or the EU's standards. Going down this path would open other

nations to extending their own policies about Internet content regulation to Europe, thereby limiting free speech and access to information to individuals in the EU.

PURSUE NONREGULATORY SOLUTIONS

The Digital Services Act should consider mutually supportive approaches such as voluntary practices, self-regulation, co-regulation, and co-governance between government and Internet companies in order to ensure none of the parties involved bears the burden of being both judge and jury. Self-regulation and co-regulation enable concerned parties to learn, share lessons, and profit from the experience of others, while improving existing practices or developing new ones. These practices could take many forms, such as codes of conduct, declarations, labels, charters, agreements, and standards. Self-regulation allows companies to operate autonomously while being legally compatible, while co-regulation involves requirements that are laid down in the wake of a legislation, or supported or codesigned by policymakers. They may not include sanctions, and are based on a partnership. These approaches ensure a flexible implementation of measures that involve the responsibility of all parties, simplify rules, speed up adjustments, and reduce legislative burden. It is through voluntary measures and collaboration with the European Commission, such as through the code of conduct on countering illegal hate speech online and the code of practice on disinformation, that a number of technology companies have in the last two years been making rapid and significant progress to combat online harms.[13] For example, the EU code of practice on disinformation is a voluntary framework between the European Commission and signatories such as Facebook, Google, and Twitter that has set an example of how governments and civil society can work with industry in the digital economy, act in coordination with technology experts to tackle complex issues such as disinformation campaigns, increase transparency of political ads, take election integrity initiatives, and address the challenges of evolving technologies while harnessing their benefits.

PHASE IN NEW REGULATION AT A REASONABLE PACE

Updating regulation, rather than adding more regulation, is often desirable—and that is certainly the case with updating the eCommerce Directive. The European Commission should uphold its recent commitment to the “one in, one out” principle when creating new laws and regulations, and proceed with creating new rules at a reasonable pace, while also striving to cut unnecessary and outdated regulations.[14] EU policymakers should recall that a number of new initiatives that have been recently implemented, such as the Copyright Directive, or are in the process of being adopted, such as the proposed EU draft regulation on online terrorist content, have introduced new responsibilities and obligations for Internet

intermediaries—and the effects of these measures are not yet known. Introducing new requirements through a Digital Services Act before identifying and addressing the caveats of these existing pieces of legislations would be unwise. EU policymakers should conduct various impact assessments to explore options before moving ahead with regulations, given the online environment's host of complex issues (e.g., liability, disinformation, and hate speech) which there is no single, simple solution.

CONCLUSION

The eCommerce Directive is a critical building block of the EU's digital economy, but it is in need of modernization. As EU policymakers pursue updates as part of the Digital Services Act, they should continue to uphold the original goal of the eCommerce Directive to remove obstacles to online commerce and provide legal certainty to businesses and citizens. Moreover, the new framework should ensure platforms are not held legally responsible for the content of their users—and individuals are held legally responsible for the content they produce just as they would be in the offline world. By updating the rules for how service providers respond to objectionable content, the EU can foster a safer and more secure online environment for its citizens and businesses.

REFERENCES

1. "Directive on electronic commerce," Directive 2000/31/EC of the European Parliament and of the Council, June 8, 2000, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN.
2. "Leaked document: EU Commission mulls new law to regulate online platforms," *NetzPolitik.org*, July 16, 2019, https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/.
3. Ursula von der Leyen, "A Union That Strives for More: My Agenda for Europe," Political Guidelines for the next European Commission, n.d., https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.
4. "Online Harms White Paper," Department for Digital, Culture, Media & Sport and Home Office, June 26, 2019, https://www.gov.uk/government/consultations/online-harms-white-paper.
5. Ibid.
6. Abraham H. Foxman and Christopher Wolf, *Viral Hate: Containing Its Spread on the Internet* (Palgrave MacMillan: New York), 2013.
7. "Directive on electronic commerce," Directive 2000/31/EC of the European Parliament and of the Council, June 8, 2000, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN.
8. "Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under 'Facebook Act'," Global Legal Monitor, July 11, 2017, https://www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/.
9. "French lawmakers vote to target online hate speech in draft bill," *Reuters*, July 5, 2019, https://www.reuters.com/article/us-france-tech-regulation/french-lawmakers-vote-to-target-online-hate-speech-in-draft-bill-idUSKCN1U01UQ.
10. "Online Harms White Paper," Department for Digital, Culture, Media & Sport and Home Office, June 26, 2019, https://www.gov.uk/government/consultations/online-harms-white-paper.
11. Matthew Prince, "Terminating Service for 8Chan," August 4, 2019, https://blog.cloudflare.com/terminating-service-for-8chan/.
12. Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI" (Center for Data Innovation), March 26, 2018, https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/.
13. "Code of Practice on Disinformation," European Commission, September 26, 2019, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation; "The EU Code of conduct on countering illegal hate speech online," European Commission, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.
14. "The von der Leyen Commission: for a Union that strives for more," European Commission, September 9, 2019, https://europa.eu/rapid/press-release_IP-19-5542_en.htm.

ABOUT THE AUTHORS

Daniel Castro is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

Eline Chivot is a senior policy analyst at the Center for Data Innovation. Based in Brussels, Eline focuses on European technology policy issues and on how policymakers can promote digital innovation in the EU. Eline earned master's degrees in political science and economics from Sciences Po, and in strategic management and business administration from the University of Lille.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C. and Brussels, the center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The center is a nonprofit, nonpartisan research institute proudly affiliated with the Information Technology and Innovation Foundation.

contact: info@datainnovation.org

datainnovation.org