International Journal of Law And Criminology

VOLUME Vol.05 Issue06 2025
PAGE NO. 51-58
DOI 10.37547/ijlc/Volume05Issue06-11

Functional Classification and Liability Standards of Information Intermediaries: The U.S. Dmca Model and Its Implementation Prospects in The Legal System of Uzbekistan

Umidbek Khudayberdiyevich Nurullayev

Independent Researcher, University of Public Security of the Republic of Uzbekistan, Uzbekistan

Received: 25 April 2025; **Accepted:** 21 May 2025; **Published:** 23 June 2025

Abstract: In the era of digital transformation, information intermediaries such as internet service providers, hosting platforms, and content aggregators play a central role in the dissemination, storage, and accessibility of information across digital networks. As their influence on communication, commerce, and public discourse expands, so does the legal necessity to regulate their activities, particularly with respect to civil liability for unlawful content distributed through their services.

Keywords: Digital transformation, information intermediaries, service providers, hosting platforms.

Introduction: In the era of digital transformation, information intermediaries such as internet service providers, hosting platforms, and content aggregators play a central role in the dissemination, storage, and accessibility of information across digital networks. As their influence on communication, commerce, and public discourse expands, so does the legal necessity to regulate their activities, particularly with respect to civil liability for unlawful content distributed through their services.

International legal practice recognizes various terminologies for these entities, including “information providers,” “digital intermediaries,” and “online service providers.” The dominant trend, however, is toward a functional classification of intermediaries based on the nature of their role in handling digital content. This approach allows for a more precise delineation of liability standards, balancing the rights of content owners with the technological neutrality of intermediaries.

One of the most influential legal models in this regard is the Digital Millennium Copyright Act (DMCA) of the United States, particularly Section 512, which introduces the “safe harbor” mechanism. This framework classifies intermediaries into distinct functional categories transitory digital network communications providers, caching providers, hosting providers, and information location tools—and defines the specific conditions under which each may be exempt from liability.

While the DMCA model has been widely studied and partially adopted in various jurisdictions, Uzbekistan has yet to develop a comprehensive legal framework governing the status and liability of information intermediaries. Existing sectoral legislation refers to concepts such as “internet providers” or “information distributors,” but lacks a coherent and enforceable classification system. As a result, courts and regulators face uncertainty when determining intermediary liability, often leading to inconsistencies in legal interpretation and enforcement.

In international practice, information intermediaries are commonly referred to as “information providers ”, “digital intermediaries ” or “online service providers .” In most cases, a functional classification approach is applied to determine the scope and limits of their legal liability. For example, the European Union’s E-Commerce Directive (2000/31/EC) distinguishes between different types of intermediaries such as “mere conduit” providers, “caching” services, and

"hosting" providers and introduces a "safe harbor" regime applicable to each category. Under this regime, an intermediary may be exempt from liability if it does not influence the content being transmitted, stored, or made available, and if it acts in a passive, technical capacity under specified conditions.

In U.S. law, Section 512 of the Digital Millennium Copyright Act (DMCA) establishes a "notice and takedown" mechanism for information intermediaries. This system determines whether an intermediary is liable or exempt from liability based on its active or passive role, its awareness of infringing content, and its response upon receiving notification. If the intermediary is notified of infringing content and takes appropriate action within a specified timeframe, it may benefit from immunity under the DMCA's safe harbor provisions. This mechanism allows the legal system to assess the intermediary's function on a spectrum ranging from purely technical transmission to substantive involvement in content, offering a nuanced basis for determining liability.

Article 1253.1 of the Civil Code of the Russian Federation recognizes the concept of an information intermediary and establishes general conditions regarding their liability. However, it does not provide a clear legal framework for differentiating between various types of intermediaries such as technical transmitters, caching services, hosting providers, or content aggregators. This lack of detailed classification leads to ambiguities in legal practice when assessing intermediary liability. Russian legislation applies a generalized approach to intermediaries, without considering their degree of involvement or influence over the content, as is done under U.S. law. The "notice and takedown" procedure, central to the DMCA, is not formally established in Russian law, and the criteria for exemption from liability are insufficiently defined. Furthermore, state control over intermediaries in Russia is relatively strict, and service providers are often held responsible for the content they transmit or store. As a result, the U.S. model with its functional and clearly defined classification of intermediaries has been adopted in this study as a more precise and legally coherent foundation. U.S. law regulates intermediaries based on their specific roles and degrees of influence over content, assigning tailored legal regimes and liability standards accordingly.

Moreover, Section 512 of the DMCA establishes a distinct "safe harbor" mechanism for each category of information intermediary. This system allows liability to be assessed based on the intermediary's level of control over the content, its degree of involvement, and its awareness of the infringing material. For instance, under the notice and takedown mechanism, if a user uploads infringing content, the intermediary can be exempt from liability provided that, upon receiving proper notification, it takes timely and appropriate action to remove or disable access to the content. This approach is not a one-sided privilege for intermediaries, but rather a balanced legal solution designed to protect both content owners and intermediaries. It promotes cooperation, fosters legal certainty, and ensures that digital platforms act responsibly while not being unduly burdened with liability for content over which they have no control .

In Uzbekistan, the concept of an information intermediary has not yet been developed as an independent legal institution. Although existing sectoral laws refer to terms such as "internet provider", "hosting service" or "information distributor" these references remain fragmented, and the legal status, scope of liability, and role in civil law relations of such entities are not clearly defined. This legal gap has led to inconsistencies in law enforcement practice, uncertainty in assigning liability, and a lack of effective oversight mechanisms. As a result, there is an urgent need in Uzbekistan to classify information intermediaries based on their function, to define their legal status, and to establish liability criteria in accordance with a functional approach. In this regard, the U.S. model, particularly the structure provided under Section 512 of the DMCA, represents a leading international practice. Adopting and adapting this model to Uzbekistan's legal system would offer a coherent framework for regulating intermediaries, ensuring legal clarity, protecting rights holders, and fostering the development of a responsible and predictable digital ecosystem.

Under U.S. law, the legal status of information intermediaries is not defined at a general or abstract level, but rather is governed by a functional classification based on the nature of their activities and the degree of control or influence over content . This regulatory approach is primarily established under the Digital Millennium Copyright Act (DMCA) and the Communications Decency Act (CDA), which rely on the "safe harbor" mechanism to limit the liability of intermediaries while ensuring the free flow of digital information. Within the framework of Section 512 of the DMCA, information intermediaries are divided into the following four specific categories:

1. Transitory Digital Network Communications Providers – These are intermediaries responsible for the automatic, continuous, and purely technical transmission of data from one point to another at the initiative of a user. Their primary function is to act as a "neutral tunnel" within the flow of information. Such providers neither store, edit, nor select the transmitted

data they merely facilitate its passage across the network. Examples include internet service providers (ISPs) such as AT&T, Verizon, or Xfinity . For instance, when a user sends a request from their device to view a video on YouTube, this request is transmitted through the ISP to YouTube's servers, and the video data is then returned to the user's device via the same provider. During this process, the ISP does not alter or retain the data in any way, nor does it interact with its content. This neutral and purely technical role defines its legal status as a transitory digital network communications provider .

2. **System Caching Providers** – These providers temporarily store data that has been transmitted at the initiative of a user, in order to make it more efficiently accessible to other users on the network for technical reasons. The data is cached for a limited duration based on specific criteria such as storage capacity, server load, or the frequency of user requests. Caching providers do not alter the data, do not interfere with its content, and always provide a reference to the original source from which the data was obtained. Their main function is to enable faster and more efficient delivery of content without requiring it to be reloaded from the source server each time . For example, when searching for a website using Google, you may have noticed a link labeled "Cached" in the search results. Clicking on this link opens a temporarily stored version of the page on Google's server. In this case, Google is acting as a system caching provider. It did not create the content, but cached it to deliver it to the user more quickly. However, if a notification is received that the cached content infringes rights, Google must promptly remove it; otherwise, it may lose its eligibility for safe harbor protection .

3. **Hosting Providers** – These are platforms that store user-uploaded content on servers for extended periods and make it publicly accessible online. Hosting providers do not create the content themselves; rather, they receive, store, and deliver it through technical means without altering its substance . Examples of such services include website hosting platforms (e.g., GoDaddy, Bluehost), video-sharing platforms (e.g., YouTube, Vimeo), and file storage services (e.g., Dropbox, Google Drive). In these cases, users upload content independently, and the provider ensures its storage and delivery without interfering with the content itself. For instance, when a user uploads a copyright-protected video to YouTube, the platform does not create the video but facilitates its distribution. Such providers serve as central technical platforms for long-term content storage and dissemination. However, from a legal perspective, they are conditionally liable and may benefit from safe harbor protection only if they meet specific legal requirements—such as acting promptly upon receiving a valid infringement notice and not exerting editorial control over the content .

4. **Information Location Tools Providers** – These are platforms that guide internet users to the source of information without storing the information themselves. Their core function is to provide access by linking users to content through hyperlinks, search engine results, or web directories, rather than hosting or transmitting the content directly. Examples include search engines such as Google, Bing, and Yahoo Search, web-based directories, or collections of hyperlinks embedded within websites. These providers do not store or modify content but simply direct users to the relevant external sources, serving as navigational intermediaries in the digital environment.

Based on this principle, transitory digital network communication providers under U.S. law are not regarded as active participants influencing the content within information networks, but rather as entities that serve solely as technical intermediaries . Section §512(a) of the DMCA reflects this principle of neutrality and passivity, stating that if a provider automatically transmits information without altering or selecting it, they cannot be held liable for copyright infringement. Examples of such providers include internet service operators like AT&T, Comcast, and Verizon, which act as "information tunnels" enabling the flow of data from one user to another. These providers do not select, edit, or process information, nor do they evaluate its legal or ethical content. The data is transmitted exactly as received, without any modification. Therefore, transitory digital network providers are granted a special status as neutral intermediaries, and liability arises only if the specific conditions outlined in the law are violated.

Under U.S. law, the rights of transitory digital network communication providers in the transmission of information, as well as the conditions for the application of these rights, are clearly outlined in Section 512(a) of the DMCA. According to this provision, Internet service providers (ISPs) that merely transmit information in a technical and automatic manner are not held liable for copyright infringement, provided that specific conditions are met. In particular, under §512(a), a provider shall not be liable for transmitting infringing content if the transmission:

was initiated by a user and transmitted between selected recipients without modification by the provider;

– was temporarily stored during transmission only to the extent necessary to carry out the

transmission and solely by an automatic technical process;

- was transmitted through the provider's system automatically, without the provider selecting the content or controlling the transmission;
- was deleted automatically or removed immediately after transmission was completed;
- was not modified by the provider, and the provider did not know or could not reasonably be expected to know that the material was infringing.

Thus, Section 512(a) not only grants legal immunity ("safe harbor") to transitory digital communication providers, but also strictly limits its application to specific, narrowly defined conditions. If a provider violates any of these conditions for example, by modifying content, selecting what to transmit, or having actual knowledge of the infringement they lose the protection of safe harbor and may be held liable.

Under U.S. law, the legal status of transitory digital network communication providers is based on their role as neutral and passive technical intermediaries. In order to maintain this status, they must fulfill certain obligations clearly regulated under Sections 512(a) and 512(m) of the DMCA. The law requires the provider to transmit information solely in a technical, automatic, and unaltered manner . As this activity designates the provider as a "neutral intermediary," they are granted immunity from liability under the "safe harbor" protection. The provider must receive data initiated by the user and transmit it automatically. The information must be delivered exactly in the form it was received, through a purely technical route.

According to Section 512(m) of the DMCA, a provider must not have prior knowledge that the transmitted information infringes copyright. If the provider knew or should have known about the infringement and failed to act such as by not removing the content or halting its transmission it may be held liable, even in the absence of direct knowledge. In such cases, the provider can be deemed to have had "constructive knowledge" based on the circumstances, facts, or environment surrounding the infringement. This would disqualify the provider from benefiting from the "safe harbor" protection .

In U.S. legislation, Section 512(a) of the DMCA, which regulates the activities of transitory digital network communications providers, is recognized as a leading and exemplary legal approach in terms of clearly defining the legal status of information intermediaries, establishing a mechanism for exemption from liability ("safe harbor"), and supporting the stable functioning of the Internet infrastructure. This law has influenced a number of international legal models, in particular the EU's E-Commerce Directive (2000/31/EC) and Japan's Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers . However, despite being a comprehensive system, U.S. law still faces certain controversial and disputable issues related to the legal regulation of the activities of transitory digital network providers, which are significant not only theoretically but also practically.

Firstly, the civil-law clarity of the "neutral intermediary" status is one of the most contentious issues regarding transitory digital network communications providers. Under Section 512(a) of the DMCA, these entities are defined as passive subjects whose sole function is to transmit information in an automatic and technical manner, without intervening in the content. This status allows them to be exempt from liability for copyright infringement, provided they transmit data without affecting its content. However, in practice, determining this status is complex, as providers often perform technical tasks such as encryption, routing, caching, and traffic optimization. Although these processes do not directly alter the content, they can influence the speed and accessibility of data across the network. As a result, evaluating such providers strictly as passive intermediaries presents legal challenges. The DMCA does not clearly delineate the regulatory boundary between these technical services and active involvement .

Secondly, the conditions of not altering or editing information are crucial for exemption from civil liability. According to Section 512(a) of the DMCA, a provider must transmit information in an "unmodified, mechanical" form . If this condition is violated, the provider may lose safe harbor protection and be held liable for the infringement . In practice, data may be altered for technical reasons such as caching, encryption, or transcoding. These changes typically affect the format, not the content. For instance, if a video is adjusted to a lower resolution via a CDN for efficient delivery, and the substance remains intact, the provider is still considered a passive intermediary . However, if the content is changed in a visual, logical, or semantic way such as inserting advertisements or trimming sections this qualifies as editing, and the provider loses protection. Therefore, whether a technical modification affects the content is the key assessment criterion. In court practice, this boundary is not clearly defined and is evaluated case by case.

Thirdly, the distinction between user initiation and automatic transmission plays a critical role in assessing the civil liability of transitory digital network communication providers. Under Section 512(a) of the DMCA, a provider is entitled to safe harbor protection

only if the transmission was initiated by the user . Therefore, determining who initiated the data transfer defines whether the provider is a passive or active actor. If the transfer occurs directly due to user actions such as sending a request, uploading content, or opening a page the provider is considered a purely technical intermediary and is not held liable. However, in practice, content may be delivered automatically via systems like CDNs or push notifications without any user input. In such cases, the initiative may be deemed to originate from the provider's system, classifying the provider as an active participant and limiting its access to safe harbor. For instance, if a user has not consented to receive notifications but the provider sends them automatically, the initiative is not user-driven . Conversely, if the user consented during app installation to receive certain automatic messages, subsequent transmissions may be seen as an extension of that user-initiated act. Hence, determining user initiative depends on context, the degree of technical intervention, and any prior consent, all of which are essential for defining the provider's legal status under civil law.

Fourthly, the concept of "constructive knowledge" regarding infringing content is one of the more nuanced issues in determining the civil liability of transitory digital network communication providers. Under Section 512(m) of the DMCA, a provider is not required to monitor or actively supervise the content being transmitted, meaning that to maintain its passive intermediary status, the provider is not legally obligated to engage in oversight. However, in practice, if a provider is presented with clear and visible indicators of copyright or other legal infringements and fails to act, it may be deemed to have had "sufficient knowledge" . In other words, even if the provider was not directly notified, the circumstances may be considered such that the provider "should have known" about the infringement because the situation provided reasonable grounds for awareness . This legal standard is abstract and lacks a fixed threshold, making its application context-dependent. For instance, if user-uploaded content visibly includes a famous brand logo, a movie clip, or a recognizable piece of music, and the provider takes no action, a court may infer that the provider had constructive knowledge of the infringement.

In U.S. law, the civil liability status of caching service providers regulated under Section 512(b) of the DMCA is based on their role as neutral, technical intermediaries that temporarily store user-requested data to improve the efficiency of information delivery. These providers do not create, modify, or control content, but instead act as passive transit points that reduce network congestion and accelerate user access. To qualify for "safe harbor" immunity from copyright infringement liability, caching providers must meet specific legal conditions: (1) they must not alter the stored content; (2) they must preserve access to the original source; (3) caching must follow technical parameters such as server load, reuse frequency, or automated expiration rules; and (4) they must promptly remove or restrict access to infringing material upon receiving a valid notice. These strict criteria ensure that the caching provider remains a non-infringing, passive conduit, entitled to legal protection only when acting within the bounds of neutral functionality.

It should be noted that while U.S. law particularly DMCA §512(b) provides a foundational legal basis for exempting caching service providers from civil liability, the practical application of these provisions remains imprecise and incomplete. The law sets out general conditions such as the requirement that caching providers must not modify the content, must ensure redirection to the original source, and must act promptly upon notice of infringement. However, the statute does not clearly define how or within what timeframe these conditions must be fulfilled to be considered "adequate," nor does it clarify to what extent technical processing remains "non-impactful," or what exactly constitutes "expeditious" removal . These ambiguities create legal uncertainty in determining the exact liability status of caching service providers. In judicial practice, courts interpret these standards differently, which affects a provider's ability to claim safe harbor protection and increases the risk of civil liability. The case Field v. Google Inc. serves as a key precedent illustrating these legal uncertainties in practice. In this case, Blake Field alleged that Google's caching of materials from his personal website and their subsequent display in search results infringed his copyright. Although Field did not use a "robots.txt" file to technically prohibit caching, he claimed that Google stored and served his content for an extended period without his consent. Google countered that it had stored the content temporarily, automatically, and in an unaltered form, and that the display occurred only at the initiative of the user's search query. The court evaluated Google's conduct and concluded that: (1) Google did not alter the content and stored it as-is; (2) the cached content was delivered automatically in response to user action; (3) Google had not been technically instructed to avoid caching (e.g., via robots.txt); and (4) Google had no knowledge of any infringement and performed caching based on objective technical criteria. Thus, the court deemed Google a passive intermediary eligible for safe harbor

protection under §512(b), highlighting the nuanced and context-dependent nature of caching provider liability.

Therefore, Google was recognized as a caching provider eligible for "safe harbor" protection and was not held civilly liable. However, a critical aspect of this case is that the court's reasoning largely relied on vague legal concepts. Terms such as "information was stored automatically," "processed due to technical necessity," and "insufficient notice" are not precisely defined within the statute itself. Had Field placed a file on his website explicitly prohibiting Google from caching (e.g., a robots.txt directive), the outcome might have been different. Similarly, if Google had stored the content for an extended period or had altered the content in any way, the court could have deemed Google an active participant, which would have disqualified it from safe harbor protection. Thus, this case demonstrates that the ability of caching service providers to benefit from safe harbor often depends on specific technical and legal circumstances. While the statute provides general rules, their application is subject to judicial interpretation, which introduces uncertainty in defining the civil legal status of such intermediaries.

Providers that engage in the long-term storage of user-directed content on servers—such as website hosting services (e.g., GoDaddy, Bluehost), video content platforms (e.g., YouTube, Vimeo), and file hosting services (e.g., Dropbox, Google Drive) are granted a specific legal status under Section 512(c) of the DMCA. This provision establishes a "safe harbor" that limits their civil liability for copyright infringement. However, this legal protection is not automatic; it applies only if the provider strictly complies with a set of prescribed conditions.

U.S. law does not regard hosting providers as directly liable parties, but rather as technical platforms that serve as intermediaries in storing and transmitting user-generated content. In this framework, if a hosting provider does not exercise direct control over the content uploaded by users, does not modify that content, and takes timely and appropriate action after receiving formal notice of infringement, it may be exempt from liability. This approach acknowledges that the provider's role is not to create content, but to store and deliver it on a technical level. Section 512(c) of the DMCA outlines specific conditions for eligibility under this safe harbor protection, including the following:

– he content must have been uploaded by a user;

– the provider must not control or edit the content;

– the provider must not have actual or reliable knowledge of any infringement within the content;

— upon receiving formal notification of infringement, the provider must act promptly to remove or disable access to the content in accordance with the "notice and takedown" procedure.

This mechanism enables hosting providers to maintain technical neutrality in their activities related to collecting, storing, and delivering content. At the same time, it creates a predictable and clearly defined legal environment for entities operating in the information sphere. A notable example illustrating this is the case of Viacom Int'l Inc. v. YouTube, Inc. In this dispute, Viacom accused YouTube of unlawfully distributing copyrighted videos uploaded by users. YouTube, in its defense, presented itself not as a content creator but as a platform acting as a technical intermediary storing data at the initiative of users. It emphasized that it did not edit the content, was not actively involved, and took action only after receiving formal notice of infringement, in line with the DMCA's "notice and takedown" procedure. The court, considering YouTube's conduct, found it to be a neutral technical intermediary rather than an active participant, and ruled that it was entitled to safe harbor protection under DMCA §512(c).

Under U.S. law, specifically DMCA §512(d), the civil legal status of providers of information location tools such as search engines or hyperlink directories is defined as that of conditional intermediaries who are not directly liable for the content to which they refer, but may bear liability under certain circumstances . These providers do not create or host the content themselves; rather, they assist users in locating information by directing them to the appropriate online sources. From a civil liability standpoint, they are not considered direct infringers, but rather intermediary entities whose liability depends on their knowledge and response to infringing content. If such a provider is unaware of any infringement at the linked location and, upon receiving formal notification, promptly removes or disables the link, it will be shielded from civil liability. However, if the provider deviates from this neutral intermediary role by, for example, failing to act after becoming aware of an infringement it may then be held liable .

In Uzbekistan's legal system, the civil status and functional classification of information intermediaries remain underdeveloped. Although terms such as "Internet provider," "information distributor," and "information service provider" appear in existing laws including the Laws "On Informatization," "On

Electronic Commerce," "On Mass Media," and in certain ministerial regulations they are largely declarative in nature and fail to establish clear legal status, liability standards, or criteria for active versus passive roles. As a result, entities involved in temporary technical transmission and those engaged in permanent data storage are treated identically under the law. This leads to a misallocation of liability, ambiguity in judicial practice, and failure to recognize the intermediary's neutral role. For example, a provider that merely transmits data automatically without exercising control over the content may still be held liable in the same manner as a hosting provider, despite their fundamentally different functions.

In Uzbek legislation, the civil law status and functional classification of information intermediaries are insufficiently developed. While terms such as "Internet provider," "information distributor," and "information service provider" appear in laws like the Law "On Informatization," the Law "On Electronic Commerce," the Law "On Mass Media," and certain regulatory acts, these terms are primarily declarative in nature and do not provide clear legal definitions regarding the intermediary's status, liability, or criteria for determining active versus passive conduct. As a result, entities engaged in temporary technical transmission of data and those involved in permanent storage are treated under the same legal framework. This leads to incorrect allocation of liability, legal uncertainty in judicial practice, and failure to acknowledge the neutral role of intermediaries. For example, an automated transmission provider despite having no control over content could be held liable in the same way as a hosting provider.

In contrast, the United States through Sections 512 of the DMCA provides a clear functional classification of intermediaries (including technical transmission providers, caching providers, hosting services, and information location tools), introducing a "safe harbor" regime for each type. Uzbekistan's legal system, however, lacks such a functional approach and conditional liability model. This absence contributes to uncertainty in judicial practice and increases legal risks for digital service providers. Therefore, it is proposed that the U.S. model be adapted into national legislation by: clearly defining categories of intermediaries; establishing legal conditions limiting liability for each type (such as non-modification of information, lack of initiative, implementation of the notice-and-takedown procedure, etc.); and distinguishing between active and passive intermediary functions. This reform is both timely and necessary.

CONCLUSION

The U.S. DMCA model, particularly Section 512, offers a comprehensive and functionally nuanced legal framework for regulating the civil liability of information intermediaries. By classifying intermediaries into distinct roles transitory communications providers, caching providers, hosting providers, and information location tools the DMCA establishes tailored "safe harbor" regimes that balance the rights of content owners with the need to maintain technological neutrality and the free flow of digital information.

In contrast, Uzbekistan's legal system lacks such a functional classification and continues to treat fundamentally different types of intermediaries under a uniform legal regime. This results in legal uncertainty, inconsistent enforcement, and misallocation of liability, especially in cases involving passive intermediaries with no editorial control over content.

To address these gaps, it is recommended that Uzbekistan adopt a legal framework modeled after the DMCA's functional approach. This would involve:

- introducing precise definitions and categories of information intermediaries;
- establishing differentiated liability regimes based on the degree of control and involvement with content;
- implementing procedural safeguards such as the notice-and-takedown system;
- recognizing the distinction between active and passive intermediary functions.

By aligning with international best practices, Uzbekistan can foster a more predictable, fair, and innovation-friendly digital environment while ensuring adequate protection of intellectual property rights and legal accountability where appropriate.

REFERENCES

United States Code, Title 17 (Copyright Act), §512(k)

Edwards, Lilian & Waelde, Charlotte (eds.), Law and the Internet, 3rd ed., Hart Publishing, 2009. - P. 123

Edwards, Lilian & Waelde, Charlotte (eds.), Law and the Internet, 3rd ed., Hart Publishing, 2009. - P. 123

Marsoof A. 'Notice and takedown': a copyright perspective //Queen Mary Journal of Intellectual Property. – 2015. – T. 5. – №. 2. – P. 183-205.

Reichman J. H., Dinwoodie G. B., Samuelson P. A Reverse Notice and Takedown Regime to Enable Pubic Interest Uses of Technically Protected Copyrighted Works //Berkeley Tech. LJ. – 2007. – T. 22. – P. 981.

17 U.S.C. § 512 (DMCA Safe Harbor Provisions) §512(a–d).

Eric Goldman, "Internet Law: Cases and Materials"

(2022). - P. 273–274. “Service providers acting as passive conduits — mere technical intermediaries — qualify for §512(a) safe harbor because they do not select, alter or store the transmitted content. They function as neutral ‘pipes’ through which data flows.”

MacCarthy, M. (2021). Intermediary Liability in Digital Markets. In I. K. Gotts (Ed.), Antitrust Issues in the Evolving Digital Marketplace. - P. 115–118. American Bar Association.

Edwards, L., & Waelde, C. (Eds.). (2009). Law and the Internet (3rd ed., - P. 127128). Caching intermediaries retain data temporarily to improve transmission efficiency. They do not alter the content, nor do they decide what to store. Any access must be directed to the original source, preserving source integrity and transparency.

Mano, M. (2020). Internet Intermediaries and Copyright Law: An EU and US Perspective - P. 103-104. For instance, when Google stores cached copies of websites for user access, it acts as a system caching provider under §512(b). If notified of infringing material, Google must remove the cached copy promptly to retain safe harbor protection.

Canali D., Balzarotti D., Francillon A. The role of web hosting providers in detecting compromised websites //Proceedings of the 22nd international conference on World Wide Web. – 2013. – P. 177-188.

Hörnle, J. (2021). Internet Law and Regulation (2nd ed., pp. 201–204). Hosting providers such as YouTube or Facebook allow users to upload content independently. Although they do not initiate the transmission or modify content, they may incur conditional liability if they fail to act upon notification of unlawful material.

Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007), - P. 1118-1120.

Digital Millennium Copyright Act, 17 U.S.C. §512(a)(1).

Digital Millennium Copyright Act, 17 U.S.C. §512(a)(2).

Digital Millennium Copyright Act, 17 U.S.C. §512(a)(3).

Digital Millennium Copyright Act, 17 U.S.C. §512(a)(4).

Digital Millennium Copyright Act, 17 U.S.C. §512(m)(1).

Edwards, L., & Waelde, C. (Eds.). (2009). Law and the Internet 3rd ed., p. 123.

Gotts, I. K. (Ed.). (2021). Antitrust Issues in the Evolving Digital Marketplace (p. 117).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng

Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Sender Act No. 137 of 2001. https://www.japaneselawtranslation.go.jp/en/laws/view/3610/en

Balkin, J. M. (2004). Digital Speech and Democratic Culture: A Theory of Intermediary Liability. New York University Law Review, 79(1), 1–58.

Digital Millennium Copyright Act, 17 U.S.C. §512(a).

Digital Millennium Copyright Act, 17 U.S.C. §512(c)(1).

Goldman, E. (2022). Internet Law: Cases and Materials (pp. 274–275).

Eric Goldman, Internet Law: Cases and Materials, 2022, pp. 273–274

17 U.S.C. §512(a)(1)

Войниканис, А.А. (2019). Правовое регулирование ответственности интернет-провайдеров за нарушения авторских прав. Москва: Юнити-Дана, с. 47–48.

Riordan, J. (2016). The Liability of Internet Intermediaries. Oxford: Oxford University Press, pp. 283–285.

UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013)

https://www.law.berkeley.edu/files/Field_v_Google.pdf

Travis J. Miller, Search Engines and the DMCA Safe Harbor: A Functional Analysis, Berkeley Tech. L.J., Vol. 26, 2011, pp. 99–100

Shestakov D.V., Интернет-посредники и авторское право, СПб, 2018, с. 124