Intermediary Liability, Data Protection, and Platform Responsibility: Appellate Considerations in Femi Falana, SAN v. Meta Platforms Inc. (Suit No: LD/17783MFHR/2025)

Chukwuyere Ebere Izuogu

Image credit: https://url-shortener.me/31N8

Introduction

The decision of the High Court of Lagos State in *Femi Falana, SAN v. Meta Platforms Inc*. raises significant legal questions concerning the relationship between constitutional privacy rights, the Nigeria Data Protection Act 2023 (NDPA or the Act), and the responsibility of online intermediaries for user-generated content. The case arose from the publication of a video on Facebook by an unidentified third-party user falsely suggesting that the Femi Falana, SAN, the Claimant was suffering from a medical condition. Although the content was generated by a user and removed once the platform became aware of it, the Court held Meta liable for invasion of privacy and unlawful processing of personal data.

While the protection of personal dignity and informational privacy is an important constitutional objective, the reasoning adopted by the Court raises doctrinal concerns. In particular, the judgment appears to expand the scope of Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (the Constitution), blur the statutory distinction between data controllers and data processors under the NDPA, and depart from widely recognised principles of intermediary liability governing online platforms.

In this article**,** I argue that the decision is vulnerable to appellate challenge. In my view, a proper application of the NDPA, read alongside relevant comparative jurisprudence from European and United States courts, indicates that Meta should not have been classified as a joint data controller or as a data processor acting as an agent of the third-party user who uploaded the disputed content. Rather, I contend that Meta's role is more accurately characterised as that of a hosting intermediary in respect of the user generated material at issue.

Constitutional Dimensions of Privacy Protection

At the constitutional level, the Court's reasoning engages the scope of Section 37 of the Constitution. The Court construed the constitutional guarantee of privacy to include protection against the unauthorised dissemination of sensitive health information. However, Section 37 does not expressly refer to medical or health data.

The Court's interpretation therefore reflects a purposive and expansive reading of the provision. Although such an approach may align with evolving notions of informational privacy in contemporary digital environments, it remains open to debate whether the framers of Section 37 intended its protection of privacy to extend beyond spatial, communicational, and correspondence based privacy to encompass sensitive personal data such as medical information in the absence of explicit textual support.

This interpretative move carries broader implications for the development of constitutional privacy jurisprudence in Nigeria. By extending Section 37 into the domain of sensitive personal data regulation, the

judgment effectively overlays constitutional doctrine onto an area that is already governed by a specialised statutory regime in the form of the Act. Whether such constitutional expansion is doctrinally justified is therefore a question that may properly warrant appellate clarification.

Statutory Framework of the Nigeria Data Protection Act 2023

The NDPA establishes Nigeria's primary statutory framework governing the processing of personal data. The Act regulates entities that determine the purposes and means of processing personal data and creates the Nigeria Data Protection Commission as the supervisory authority responsible for enforcement.

Section 65 and related interpretative provisions of the NDPA define key actors within the data protection ecosystem. A "data controller" is defined as an individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data. A "data processor" is defined an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor. These definitions mirror the functional approach adopted in modern data protection law internationally. Responsibility under the Act therefore attaches to the entity that exercises decision-making authority over why and how personal data are processed.

Importantly, the statutory scheme distinguishes between entities that originate or direct data processing activities and those that merely provide technological infrastructure. Where an entity neither determines the purpose of processing nor processes personal data on behalf of another controller, it does not fall within either classification.

Application of the NDPA to User Generated Content

The facts of the Falana case indicate that the disputed video was created and uploaded by an independent Facebook user. The purpose of the processing, namely the creation and dissemination of the video, was determined exclusively by that user. There is no evidence that Meta instructed the user to create the content or participated in its production.

Under the statutory definitions contained in the NDPA, this distinction is decisive. Because Meta did not determine the purpose or essential means of the processing, it cannot properly be characterised as a data controller in relation to the publication. Likewise, Meta cannot be classified as a data processor because it did not process the data on behalf of the user acting as a controller. Instead, the platform functioned as a hosting intermediary providing the technological infrastructure through which users may communicate.

The Court's determination that Meta is a joint controller, and therefore liable for the alleged breach of the Claimant's privacy rights on the basis that the individual who uploaded the video was not identified or joined as a party to the proceedings, risks blurring the statutory distinction between the creator of the content and the intermediary that provides the technological platform through which that content is transmitted. Such an approach may obscure the functional differences between those who originate or determine the content of a communication and those whose role is limited to providing the infrastructure that enables user generated material to be disseminated.

If adopted more broadly, such an approach could substantially expand the scope of liability under the NDPA beyond what the statutory language appears to contemplate, with important implications for the

allocation of responsibility between content originators and online intermediaries.

The judgment also appears to proceed on the assumption that Meta, as the operator of Facebook, acted as an agent of an unknown and undisclosed principal, namely the unidentified third party who uploaded the disputed content. On this basis, the Court reasoned that, under established principles of agency law, the acts of an agent bind the principal and *vice versa*, and that an aggrieved party may elect to proceed against either the agent or the principal. In the present case, the Court observed that the Claimant had elected to proceed against the alleged agent, Meta.

This characterisation, however, raises important doctrinal concerns. The presumption of an agency relationship in these circumstances appears to depart from orthodox principles of agency law. Traditionally, the existence of an agency relationship requires clear evidence of authority,[1] consent,[2] or control between the principal and the alleged agent. On the facts of the case, there was no indication that the unidentified uploader authorised Meta to act on their behalf, nor that Meta exercised control over the purpose or content of the publication.

Absent such indicia of authority or control, treating the platform as an agent of the uploader risks extending established agency principles beyond their conventional limits. If applied more broadly, such reasoning could introduce considerable legal uncertainty for online intermediaries that operate at scale and whose role is primarily to provide technological infrastructure for user generated communications, rather than to act on behalf of users in a representative legal capacity.

The Court's characterisation also presents an additional conceptual difficulty when considered within the framework of modern data protection law. If Meta were indeed acting as an agent under the control of the third-party uploader, the relationship would closely resemble that between a data processor and a data controller within the meaning of the NDPA. Under the Act, a data processor processes personal data on behalf of, and under the instructions or control of, a data controller.

However, the facts of the case do not appear to support such a conclusion. There was no evidence suggesting that the unidentified uploader exercised control over Meta's data processing operations or that Meta processed the data pursuant to the uploader's instructions, whether express or implied. In the absence of such elements of authority or direction, it becomes difficult to sustain the proposition that Meta acted as a processor on behalf of the uploader as controller.

Accordingly, characterising Meta as an agent operating under the control of the uploader appears conceptually inconsistent with the structure of the NDPA itself. Without evidence that Meta processed the personal data under the direction or authority of the uploader, the statutory criteria for classification as a data processor are not satisfied. In this respect, the agency analysis adopted by the Court risks conflating distinct legal concepts and may not accurately reflect the functional role of an online platform whose primary function is to provide the technological infrastructure through which user generated communications are disseminated.

Content Moderation and Algorithmic Systems

Although not expressly articulated by the Court, the reasoning appears to contain an implicit suggestion

[1] *Edem v. Canon Balls Ltd.* (2005) 12 NWLR (Pt. 938).

[2] *Mikano International Ltd v. Ehumad* (2013)1 CLRN 83.

that Meta derives revenue from the traffic generated by content hosted on the platform. In this context, it is important to situate the discussion within the broader operational framework of online platforms, particularly the role of algorithmic content moderation systems.

Online platforms routinely deploy automated tools to detect harmful material, enforce community standards, and respond to user complaints. These moderation systems operate across vast volumes of user generated content and necessarily involve the incidental processing of personal data embedded within such material. Their primary function is to safeguard the integrity and safety of the platform by identifying and addressing content that may violate applicable rules or policies.

Accordingly, the mere existence of algorithmic systems that process user generated content should not, without more, be taken as evidence that the platform determines the purpose of the original processing undertaken by users. Rather, such systems typically perform a technical and supervisory role aimed at maintaining platform governance and user safety within complex digital environments. Their function is reactive rather than creative.

These issues are particularly significant when viewed against the broader legal principles governing online platforms that engage in content moderation. In practice, platforms that moderate user generated content will often process personal data contained within that content. However, the act of moderation does not automatically render a platform liable as a data controller or processor.

Liability typically arises only where the platform determines the purposes and essential means of processing personal data or where it processes such data on behalf of another entity. Similarly, where moderation functions are purely technical, automated, or incidental to the operation of the service, regulators may regard the processing as ancillary technical activity rather than independent determination of the purposes of processing.[3]

Treating algorithmic moderation as evidence of controller responsibility could create adverse regulatory incentives. Platforms might become reluctant to deploy safety tools if doing so increased their exposure to liability. Contemporary digital governance frameworks therefore seek to encourage responsible moderation practices rather than penalising them.

Comparative Jurisprudence on Data Controller Responsibility

Comparative case law illustrates the importance of distinguishing between actors who determine the purposes of processing and those who merely facilitate technological infrastructure.

In the decision of the Court of Justice of the European Union (CJEU) in *Wirtschaftsakademie Schleswig-Holstein v. ULD* (Case C-210/16), the CJEU examined whether the administrator of a Facebook fan page could be regarded as a data controller. The CJEU concluded that joint controllership arose because the fan page administrator actively participated in determining the parameters of data collection and benefited from targeted statistics generated through Facebook's analytics tools. The administrator

[3]See, edpb, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.1 Adopted on 07 July 2021' < https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf > accessed 27 March 2026, p. 28.

therefore contributed to the purposes and means of the processing of personal data.

Crucially, the reasoning of the CJEU was grounded in the fact that the fan page operator actively configured the processing environment and benefited from targeted analytics. By contrast, in circumstances where a platform merely hosts user generated content without determining the purpose of the processing, controller responsibility does not arise.

The Falana case differs fundamentally from the scenario considered in Wirtschaftsakademie. The alleged personal data were generated by an independent user, and there is no evidence that Meta configured or directed the processing for the specific purpose of disseminating the disputed information.

Intermediary Liability and Comparative Digital Governance

The doctrine of intermediary liability further supports the conclusion that Meta should not have been held liable for third-party content. Across multiple jurisdictions, courts have recognised that online platforms primarily function as intermediaries that facilitate communication between users rather than as originators of the content transmitted through their services. United States jurisprudence provides a prominent example. Section 230 of the Communications Decency Act establishes that providers of interactive computer services cannot be treated as the publisher or speaker of information provided by another content provider. The landmark decision in *Zeran v. America Online, Inc.* (4th Cir. 1997) affirmed this principle, confirming that platforms are generally immune from liability for defamatory material posted by third parties. In that case, the United States Court of Appeals for the Fourth Circuit held that Section 230 protects internet service providers from liability for defamatory content posted by third parties, even where the provider has received notice of the alleged defamation. The Court reasoned that the statutory immunity applies so long as the claim seeks to treat the provider as the publisher or speaker of third-party content.

Similarly, many regulatory frameworks recognise that platforms may avoid liability where they operate as passive intermediaries or mere conduits in the transmission or hosting of user generated content. Under intermediary liability regimes reflected in instruments such as the European Union E-Commerce Directive, the Digital Services Act, and comparable frameworks in other jurisdictions, platforms that store or transmit information without selecting, modifying, or exercising editorial control over that content may benefit from safe harbour protections. These protections typically apply where the platform acts expeditiously to remove or disable access to unlawful material upon receiving notice.

In Nigeria, intermediary liability principles appear in more limited and sector specific forms. The Copyright Act 2022, for instance, provides a notice and takedown framework in relation to copyright protected works that have been made available on an online platform without the authorisation of the copyright owner. Under this regime, a rights holder may issue a notice requiring the platform to remove or disable access to the infringing material. In addition, the Internet Code of Practice and the Guidelines for the Provision of Internet Service issued by the Nigerian Communications Commission (NCC) contain intermediary related obligations requiring Internet Access Service Providers (IASPs) and Internet Service Providers (ISPs) to act expeditiously to remove unlawful content once notified.

However, the scope of these frameworks remains limited. The Copyright Act applies only to works

protected by copyright that have been shared in violation of the copyright owner's right to make the work available by wire or wireless means. The instruments issued by the NCC, on the other hand, apply specifically to IASPs and ISPs rather than to online platforms more broadly. Notwithstanding these limitations, these regulatory approaches provide useful guidance on how intermediary liability may be structured in Nigeria. They reflect a general policy orientation that recognises the role of intermediaries as facilitators of communication, while placing emphasis on notice-based mechanisms that require platforms acting as mere conduits, caching services, or hosting providers to remove or disable access to unlawful content once properly notified.

Implications for Nigeria's Digital Ecosystem

The broader implications of the Falana decision extend beyond the immediate parties to the dispute. Nigeria's digital economy increasingly relies on platforms that enable communication, commerce, and innovation. Expanding platform liability beyond established intermediary liability principles may therefore introduce regulatory and legal uncertainty for technology companies operating within the jurisdiction.

The decision also has the potential to broaden the exposure of online platforms to privacy and data protection claims, particularly where disputes are framed through the lens of constitutional privacy rights and sensitive personal data rather than traditional causes of action such as defamation. Where platforms may be held liable for third party content despite acting expeditiously to remove it once notified, the resulting litigation risk could incentivise overly restrictive moderation practices or deter investment in Nigeria's digital ecosystem.

Such outcomes would sit uneasily with the broader policy objective of promoting a dynamic and innovative digital economy while maintaining robust protection for the rights and interests of data subjects. A carefully calibrated legal framework that recognises both objectives remains essential for the sustainable development of Nigeria's digital environment.

Grounds Supporting Appellate Review

Against the background of the foregoing analysis, several aspects of the judgment appear to warrant careful appellate reconsideration. These issues arise both at the level of constitutional interpretation and in the application of the substantive statutory framework governing data protection and digital intermediaries.

First, the Court's interpretation of Section 37 of the Constitution appears to extend the scope of constitutional privacy protection beyond its traditionally understood limits. While the protection of personal dignity and informational privacy is an important constitutional value, the reasoning adopted by the Court arguably expands Section 37 into the domain of sensitive personal data regulation without clear textual foundation. The regulation of personal data is now addressed through a specialised statutory regime under the NDPA. Appellate clarification may therefore be necessary to determine the proper relationship between constitutional privacy guarantees and the statutory framework governing the processing of personal data.

Second, the classification of Meta as responsible for unlawful processing of personal data raises questions of statutory interpretation under the Act. The statutory framework adopts a functional approach that allocates responsibility to entities that determine the purposes and essential means of processing personal data or that process such data on behalf of another controller. In the present case, the disputed material was created and uploaded by an independent user. On the available

facts, there is limited indication that the platform determined the purpose of the processing or acted on behalf of the user in carrying out that processing activity. The attribution of joint controller responsibility in these circumstances therefore raises questions as to whether the statutory definitions were applied consistently with the structure and intent of the Act.

Third, the reasoning of the Court appears to give limited weight to the intermediary character of online platforms and to widely recognised principles governing intermediary liability for user generated content. Across multiple jurisdictions, digital governance frameworks distinguish between the originators of content and the intermediaries that provide the technological infrastructure through which that content is transmitted. The absence of a clear engagement with these principles may have contributed to an analytical framework that attributes responsibility to the online platform for content over which it neither exercised editorial control nor determined the underlying purpose of the processing.

Fourth, the judgment's treatment of the relationship between platform operations, content moderation, and responsibility for data processing raises broader questions regarding the allocation of liability within complex digital ecosystems. Contemporary regulatory approaches generally encourage responsible moderation practices by platforms while recognising that such moderation activities are often reactive and technical in nature. An interpretation that treats the existence of moderation systems or platform infrastructure as evidence of controller responsibility may inadvertently create regulatory disincentives for the deployment of safety mechanisms that are widely regarded as essential for maintaining safe online environments.

Finally, comparative jurisprudence indicates that courts in other jurisdictions have adopted a careful and activity specific approach when determining responsibility for data processing in digital environments. Such analysis typically focuses on identifying the actor that determines the purpose and essential means of the specific processing activity in question. Applying a similar analytical framework within the Nigerian context may lead to a different allocation of responsibility between content creators and the platforms that host their communications.

Taken together, these considerations suggest that the judgment raises questions of doctrinal coherence and regulatory policy that extend beyond the immediate facts of the dispute. Appellate review may therefore provide an important opportunity to clarify the interaction between constitutional privacy rights, the statutory framework established under the Act, and the principles governing intermediary responsibility within Nigeria's evolving digital regulatory environment.

Conclusion

The decision in *Femi Falana, SAN v. Meta Platforms Inc.* marks a notable development in Nigeria's evolving jurisprudence on digital rights, privacy protection, and the legal responsibilities of online platforms. By addressing the intersection between constitutional privacy guarantees and the statutory regime governing personal data, the judgment reflects the growing importance of legal frameworks capable of responding to disputes arising within contemporary digital communication environments.

However, aspects of the Court's reasoning raise significant doctrinal and policy questions. The disputed material was created and uploaded by an unidentified third party, and the available facts do not suggest that the platform acted as an agent of the

uploader or determined the purpose of the processing in question. In these circumstances, Meta's role appears more accurately characterised as that of a hosting intermediary that provides the technological infrastructure through which users communicate. The evidence that the content was removed following notification further reflects a form of reactive moderation that is widely recognised within modern digital governance frameworks as an appropriate mechanism for addressing unlawful or harmful material.

Against this background, the classification of the platform as a joint controller under the Act raises interpretative concerns regarding the functional allocation of responsibility under modern data protection law. The statutory framework attaches primary responsibility to actors that determine the purposes and essential means of processing personal data. Extending such responsibility to entities that merely host user generated communications risks weakening this functional distinction and expanding liability beyond the boundaries contemplated by the legislation.

More broadly, the case highlights the need for doctrinal clarity at the intersection of constitutional privacy protection, statutory data protection, and intermediary responsibility. As Nigeria's digital economy continues to expand, the development of a coherent and predictable legal framework governing platform responsibility will become increasingly important. Appellate consideration of the issues raised in this case may therefore provide a valuable opportunity to clarify the proper allocation of responsibility for user generated content while ensuring that the interpretation of privacy rights remains consistent with the structure and objectives of the statutory regime governing personal data.

Disclaimer

SSKÖHN NOTES is a resource of the law firm STREAMSOWERS & KÖHN deployed for general information and does not constitute legal advice neither is it a substitute for obtaining legal advice from a legal practitioner.

INTERMEDIARY LIABILITY, DATA PROTECTION, AND PLATFORM RESPONSIBILITY: APPELLATE CONSIDERATIONS IN FEMI FALANA, SAN V. META PLATFORMS INC. (SUIT NO: LD/17783MFHR/2025)

Chukwuyere Izuogu, LL.M (Hannover), CIPP/E
Partner

chukwuyere@sskohn.com

STREAMSOWERS & KÖHN is a leading commercial law firm providing legal advisory and advocacy services from its offices in Lagos, Abuja, and Port Harcourt. The firm has extensive experience in acting for Nigerian and international companies, government, and industry regulators in the firm's various areas of practice.

Contact us at:
852b Bishop Aboyade Cole St,
Victoria Island,
Lagos
Tel: +234 1 271 2276; **Fax:** +234 1 271 2277
Email: info@sskohn.com; **Website:** www.sskohn.com