



Consent, Accuracy and the Missing Journalism Exception

**An Analysis of the Decision of the High
Court of Uganda in Silver Kayondo v
Monitor Publications Limited and
Others through a Data Protection
Lens.**

August, 2026

© 2026 DPO Privacy Centre (East Africa). All rights reserved.

This publication is protected by copyright. It is made available for personal, educational and non-commercial use, provided that DPO Privacy Centre (East Africa) is acknowledged as the source in any reproduction or reference.

No part of this publication may be reproduced, distributed, adapted, translated or transmitted in any form or by any means, whether electronic, mechanical, or otherwise, for commercial purposes without the prior written consent of DPO Privacy Centre East Africa.

This publication is developed as an information resource and does not constitute legal advice.

Citation: Kityo M, “Consent, Accuracy and the Missing Journalism Exception: An Analysis of the Decision of the High Court of Uganda in *Silver Kayondo v Monitor Publications Limited and Others* through a Data Protection Lens” (DPO Privacy Centre (East Africa), 2026) accessible at www.dpoprivacycentre.com/

Contributor:



Kityo Martin

1. Introduction

The case of *Silver Kayondo v Monitor Publications Limited & Others*¹ is the first judgment in which the High Court of Uganda had to decide whether a newspaper can republish a person's public social media post without their consent. The High Court answered that question in the negative and awarded the Plaintiff UGX 10,000,000 in damages under the Data Protection and Privacy Act²(DPPA/Act) in addition to damages awarded under other causes of action arising from the same publication.

This commentary analyses the case and argues that while the Court was justified in recognising that the republication touched upon the Plaintiff's rights under the DPPA, its reasoning rests on an incomplete interpretation of the Act and the Data Protection and Privacy Regulations³(Regulations). By treating the processing as one that required consent, the judgment overlooked the broader framework governing lawful processing of personal data, failed to interrogate the principles applicable to processing of publicly available personal data and the accuracy of that data thereby resolving the dispute on an incorrect legal justification.

This comment lays out the factual background of the case, issues handled and the holding of the Court. It then analyses the reasoning adopted by the Court based on the arguments advanced by counsel, identifies areas of strength as well as aspects that warranted further consideration. It concludes by proposing recommendations on how similar disputes may be better handled in the future and advocates for legislative and institutional reforms.

2. Brief Facts

The Plaintiff posted information on his X account (formerly referred to as Twitter) analysing aspects of the World Bank's lending relationship with Uganda. The Defendants reproduced an altered portion of the Plaintiff's tweet in its print and e-newspapers, website and other affiliated platforms and further attributed to him a statement he never made.

When the Plaintiff learned of the said publication, he sued for copyright infringement, false attribution, misrepresentation, negligence, defamation and unlawful processing of personal data.

1. Civil Suit No. 222 of 2024. Decided by Justice Dr. Ginamia Melody Ngwatu, J and issued on 27th July 2026 accessible via <https://ulii.org/en/akn/ug/judgment/ugcommc/2026/354/eng@2026-07-27>
2. Cap. 97.
3. Data Protection and Privacy Regulations, 2021.

The Defendants denied liability and argued that the Plaintiff had not expressly prohibited the reproduction or communication of his posts, any attribution error had been clarified and retracted and that the publication was made in good faith without causing harm to the Plaintiff's professional relationships.

3. Issues

The court laid out seven issues for determination. This comment focuses on the sixth issue which concerned whether the defendants unlawfully processed the Plaintiff's personal data.

4. Holding

The Court started its analysis under issue six by reproducing the statutory definitions of "data collector" and "personal data" contained in Section 2 of the DPPA. The Court further relied on the case of *Nalubega Shadia v Stabex International Limited*,⁴ observing that the purpose of the DPPA is to ensure that personal data is collected, published, processed and stored only with the clear and unambiguous consent of the data subject.

The Court also summarised the Plaintiff's submissions in which counsel argued that the Plaintiff had published his posts to a curated audience of followers and that the Defendants' republication exposed the content to a different and wider audience, contrary to what was described as the "new audience theory". Counsel for the Plaintiff submitted on Section 25 of the DPPA, arguing that it confers upon a data subject the right to prevent processing of personal data. Counsel also relied on Section 7(1) of the DPPA, which prohibits collection or processing of personal data without prior consent and Section 9(1), contending that the Plaintiff's tweet disclosed philosophical beliefs and political opinions, which constitute special personal data. Since the matter proceeded ex parte, the Court did not have the benefit of submissions from the Defendants on these issues.

Having set out the statutory provisions and the Plaintiff's submissions, the Court concluded that the DPPA is concerned with protecting information relating to the identity of an individual and by republishing his tweet without his consent, the Defendants had unlawfully processed the Plaintiff's personal data.⁵

4. Civil Suit No. 665 of 2021 (Hereinafter "Nalubega Shadia v Stabex International Limited").

5. *Silver Kayondo v Monitor Publications and Others*, page 34.

5. What the judgment gets right

Section 1 extends the applicability of the DPPA to every person, institution and public body that collects, processes, holds or uses personal data within Uganda. The republication of the Plaintiff's tweet contained personal data relating to the Plaintiff. It identified him by name, nationality and occupation, all of which fall within the statutory definition of personal data under Section 2 of the DPPA. In the circumstances, the Court was right to find that the DPPA applied to the Defendants' collection and processing of the Plaintiff's personal data.

Besides alleging unlawful processing of personal data, the Plaintiff pleaded other causes of action including defamation, copyright infringement, false attribution, misrepresentation and negligence. Rather than treating these causes of action as one and the same, the Court analysed each and made separate findings. That approach was commendable given the different legal interests protected by each one of the said causes of action.

Nevertheless, the Court's task was far from straightforward. At the time of the decision,⁶ there was no Ugandan case law that had considered the application of the DPPA to the republication of personal data for journalistic use. The Court therefore had a difficult task of applying the existent data protection laws to a novel factual situation.

6. Does a "Tweet" Amount to Personal Data?

Whether a "tweet" constitutes personal data is a matter of context. It is determined on a case-by-case basis by considering the nature of the information contained in the tweet and the manner in which that information is subsequently processed, republished or shared.

Section 2 defines personal data as "information about a person from which the person can be identified, that is recorded in any form". In that regard, a tweet is a record which can have various forms of information, both personal and general information.

To understand which information in a tweet is personal data requires assessment of a single item and not automatically assuming that the entire record in which it sits amounts to personal data.

6. 27th July, 2026.

In the instant case, the Plaintiff's tweet⁷ of 10th August, 2023 contained the following information reproduced as follows;

"World Bank-Uganda

- 1. Lenders are free to dictate their lending terms*
- 2. Sovereigns/Govts have the right to protect their sovereignty*
- 3. Borrowers are not tied to specific lenders*
- 4. Lenders push values of their shareholders*
- 5. Economic size & political significance shape treatment"*

The subject matter of the tweet lays out five propositions concerning the relationship between lenders and sovereign borrowers. Standing on their own, those statements did not relate to the Plaintiff nor were they capable of identifying him in any way. Therefore, those statements were merely information.

Equally important is the manner in which the information contained in the tweet was republished. In an article titled *"Inside Uganda's Talks with World Bank"* published in its print and e-news platforms on 16th September, 2023,⁸ the Defendants quoted a portion of the information in the Plaintiff's tweet to the effect that *"Lenders push value for their shareholders"*.

The Defendants did not reproduce the Plaintiff's X/Twitter handle, profile or the platform from which the statements originated.

So the question to be answered is which information or at what point did the Plaintiff's tweet amount to personal data capable of protection under the DPPA?

That answer lies in attribution. The publication by the Defendants became information relating to an identifiable individual, namely the Plaintiff, through the attribution that accompanied the quotation in the Defendants' article.

The quotation attributed the statement from the Plaintiff's tweet by identifying him by name, nationality and occupation stating, *".....said Mr Silver Kayondo, a Ugandan Foreign Direct Investment lawyer."* It is this attribution and not the underlying commentary on the World Bank itself that brought the publication within the scope of the DPPA since it created an impression that an identifiable individual, the Plaintiff, held those views.

7. Silver Kayondo, 'World Bank-Uganda' X post (10 August 2023), <https://x.com/silverkayondo/status/1689514927440941056> accessed at 19 August, 2026.

8. Deogratius Wamala, 'Inside Uganda's Talks with the World Bank' Daily Monitor (16 September 2023) <https://www.monitor.co.ug/uganda/news/national/inside-uganda-s-talks-with-the-world-bank-4370382> accessed 8 August 2026.

6.1 Political Opinions, Philosophical Beliefs or Not?

The Plaintiff's counsel relied on Section 9(1) of the DPPA to characterise the Plaintiff's comments as philosophical or political beliefs constituting special personal data. The Court left that submission unexamined without analysing whether or why the Plaintiff's observations on institutional lending and sovereign borrowing were properly characterised as political opinions or philosophical beliefs as opposed to commentary on matters of public policy or economics.

To understand what kind of information falls within the protection of Section 9, it is important to examine the provision and review its legislative history. According to Section 9, special personal data includes sensitive information relating to an individual's religious or philosophical beliefs, political opinion, sexual life, financial information, health status and medical records.⁹ It attracts greater protection under the DPPA and Section 9(3) permits its collection or processing only in the exercise of a right or obligation imposed by law on an employer, with the freely given consent of the data subject or for the legitimate activities of a non-profit, political, philosophical, religious or trade union body in relation to its members.

In the Hansard of 5th December 2018, the impugned provision was before the Committee of Parliament as Clause 5 of the Data Protection and Privacy Bill, 2015, for amendment. The Committee sought to include health status, financial information and medical records as special personal data, with religious or philosophical beliefs and political opinion having already formed part of the Bill.

A Member of Parliament (MP) noted that;

*"This data is categorised as special personal data and it is data which is related to your financial information, health status, sexual life and this data should not just be availed without prior consent. It should not be easily accessible by a researcher or any other person."*¹⁰ In support of this, the then Minister of ICT and National Guidance explained that the amendment *"stops the data collector from accessing my personal data without going through the lawful means"*¹¹

Although the MP's comments were in relation to the additional categories proposed by the committee, they reflect the broader legislative concern of protecting sensitive information classified as special personal data from unauthorised access and disclosure.

9. DPPA, Section 9.

10. Hansard of the 10th Parliament of Uganda, 5 December 2018, accessible via, <https://cmis.parliament.go.ug/cmris/views/a78d1132-7688-45f0-8d11-327688f5f054%253B1.0> at page 13.

11. Hansard of the 10th Parliament of Uganda, 5 December 2018, accessible via <https://cmis.parliament.go.ug/cmris/views/a78d1132-7688-45f0-8d11-327688f5f054%253B1.0> at page 14.

In another debate related to Clause 13 which later became Section 17, the Committee proposed to delete the paragraph that permitted further processing where the data is publicly available or has been made public by the person concerned. The then Minister of ICT and National Guidance refused the deletion illustrating that:

“..if I have shared everything about myself on my verified twitter handle and some researcher somewhere quotes my information, which I have voluntarily published, what offence is that?

Therefore, we could leave it - not to prohibit sharing of privately shared information, which has been voluntarily given out.”¹²

From the above debates on Clauses 5 and 13, it appears that Parliament intended Section 9 to protect against the unauthorised acquisition and disclosure of sensitive personal data but did not intend liability to arise merely because another person quoted or reproduced personal data including political opinions or philosophical beliefs that the data subject has voluntarily published and made available to the public.

6.2 Public v. Private Social Media Accounts

It was argued for the Plaintiff that the post was made to a curated community of followers and that republication exposed it to a public the Plaintiff had not contemplated, relying on what was referred to as the “new audience theory”.

The “new audience theory” originates from European Union (EU) copyright jurisprudence on the communication of works to the public. In the case of *Svensson v Retriever Sverige AB*,¹³ the Court of Justice of the European Union (CJEU) held that a further communication of a work requires fresh authorisation only where it is directed at a public the rights holder did not have in mind when authorising the original communication and that no such public arose where the works in question were freely accessible without restriction.¹⁴ The Plaintiff’s reliance on this theory was doctrinally problematic because it is rooted in copyright law rather than data protection law. Copyright operates on a logic of authorisation and the relevant enquiry is how far the rights holder’s licence extends. The DPPA operates differently since Section 7 sets out the bases upon which processing is lawful and where processing rests on one of them its lawfulness does not depend on the composition of the audience that ultimately receives the data. Nothing in the DPPA provides that

¹². Hansard of the 10th Parliament of Uganda, 5 December 2018, accessible via <https://cmis.parliament.go.ug/cmisis/views/a78d1132-7688-45f0-8d11-327688f5f054%253B1.0> at page 18.

¹³. Case C 466/12 (Hereinafter ‘Svensson v Retriever Sverige AB’).

¹⁴. *Svensson v Retriever Sverige AB* at paragraphs 24, 26 and 27.

processing becomes unlawful merely because it reaches a different audience, though the circumstances in which a data subject published may bear on what he could reasonably expect.¹⁵

If the Plaintiff's submission were to be understood as a factual claim and not a legal test, the evidence adduced did not support the contention that his posts were directed to a limited audience. The Plaintiff averred that as at 6th February 2024 he had approximately 33,500 followers on X, 11,842 on LinkedIn and 4,689 on Facebook. He further averred that his personal website attracted about 10,000 monthly visitors. He also averred that his versatile digital media footprint earned him several paid media requests to offer expert analysis.

A critical assessment of this evidence shows that the contents of a public account on X, LinkedIn or Facebook are not confined to followers of a given user. The content posted on these public accounts is open to both users who are signed up and those who are not signed up on those platforms. It can be viewed, shared and reposted by other users beyond what the user can contemplate. The position would be different had the Plaintiff's accounts been private. Such accounts would have access controls, restrictions on resharing or reposting, follower approval before viewing posts and other platform restrictions¹⁶ which would have supported the argument that the publication was intended for a limited audience. However, the Plaintiff did not lead evidence to that effect. In those circumstances, the submission that the Plaintiff's posts were intended only for a curated audience becomes difficult to sustain in light of the fact that the Plaintiff's accounts were public.

7. The Lawfulness of the Processing

7.1 Collection of Publicly Available Personal Data

Section 11(1) of the DPPA requires personal data to be collected directly from the data subject, subject to the exceptions in Section 11(2). Section 11(2)(b) permits collection of personal data from another source where the data subject has deliberately made the information public.

This exception was relevant to the present case because the Plaintiff had published information about his occupation, name and nationality on his public social media accounts and website. The Defendants could have relied on Section 11(2)(b) to justify obtaining the said information from public sources, that is to say, social media, rather than directly from the Plaintiff.

¹⁵. Regulation 10, Regulations.

¹⁶. See X, 'About public and protected Posts' X Help, <https://help.x.com/en/safety-and-security/public-and-protected-posts> accessed 29 August 2026; Facebook, 'Basic Privacy Settings and Tools' Facebook Help Centre, <https://www.facebook.com/help/1297502253597210> accessed 29 August 2026; LinkedIn, 'Manage your account and privacy settings' LinkedIn Help, <https://www.linkedin.com/help/linkedin/answer/a1337839/managing-your-account-privacy-settings?lang=en> accessed 29 August 2026.

However, Section 11(2)(b) has its limitations. It addresses the source of collection and not the lawfulness of the processing itself. Had the Defendants relied on it, they still had to root their republication of the Plaintiff's personal data separately in a lawful basis under Section 7 of the DPPA.

7.2 Consent and its Exceptions

Section 7(1) of the DPPA identifies consent as the primary lawful basis for processing personal data, provided that such consent is freely given, specific, informed and unambiguous in accordance with Section 2. The Court was therefore right to begin its analysis from the question of consent and rightly relied on *Nalubega Shadia v Stabex International Limited*¹⁷ in reaffirming that position.

However, the judgment appears to treat the absence of consent as sufficient to establish the unlawfulness of the processing yet Section 7(2) provides for circumstances in which personal data may be lawfully processed without the data subject's consent. The existence of these alternative lawful bases means that the absence of consent does not mean that processing of personal data is unlawful.

Having found that the Plaintiff had not consented to the processing of his personal data, the Court ought to have considered whether the Defendants' processing could be justified under any of the lawful bases recognised under Section 7(2) of the DPPA. This was not done and the judgment proceeded from the absence of consent to the conclusion that the Defendants had unlawfully processed the Plaintiff's personal data without considering the exceptions.

7.3 Legitimate Interests as a Lawful Basis

Regulation 10(2)(b) excludes a data subject's right to object to processing of personal data where the processing is subject to the data collector or controller's legitimate interest. Regulation 10(3) goes ahead to define legitimate interests as processing which the data subject would reasonably expect or where there is a compelling justification for the processing. Although legitimate interests are not expressly listed in Section 7(2) of the DPPA, Regulations 10(2)(b) and 10(3) effectively introduce them as a lawful basis for processing personal data.¹⁸

This position was also advanced by the Personal Data Protection Office (PDPO) in its decision in *AdLegal International Limited v WhatsApp LLC and another*¹⁹ where it held

17. Civil Suit No. 665 of 2021.

18. This brings about a tension on whether the Regulations can expand the lawful bases beyond what the Act contemplated. Despite the fact that Section 39 of the DPPA empowers the Minister to make regulations for matters required to be prescribed under the Act, this comment argues that enlarging a list of lawful bases which Parliament closed falls outside what the Minister is permitted to do; Regulation 36 raises a similar concern on the tensions between the Act and its Regulations. Section 25(1) of the DPPA permits a data subject to require cessation of processing "which causes or is likely to cause unwarranted substantial damage or distress". Regulation 36(1) permits a data subject to require cessation of processing which is "not compatible with the purpose for which the personal data was collected". In contrasting the two provisions, it appears that Regulation 36(1) effectively substitutes the DPPA's threshold of unwarranted substantial damage or distress with a different criterion based on purpose compatibility thereby raising inconsistency of the Regulations with the parent Act.

19. Complaint No. PDPO 086/2025 (Hereinafter "AdLegal International Limited v WhatsApp LLC and another").

that Regulation 10(2)(b) provides for "legitimate interests" as a lawful ground for collecting and processing data.²⁰

If legitimate interests were available as a lawful basis, the argument in the present facts would merit serious consideration. The Plaintiff himself averred that, due to his versatile digital media footprint and depth of content, he received several paid media requests to offer expert analysis and had synchronised his social media handles and website to broadcast the same content.²¹ These circumstances could have been relied upon by the Defendants to argue that the use of the Plaintiff's published commentary by media outlets was within the scope of processing that he could reasonably expect. The fact that some of those engagements were paid does not necessarily alter that expectation.

The difficulty with relying on legitimate interests in the present case arises from Regulation 10(4), which places the burden of establishing the legitimate interest on the data controller. The Defendants would have been required to lead evidence establishing the legitimate interest relied upon, the necessity of the processing and the balancing of that interest against the Plaintiff's rights and freedoms. However, upon failure to comply with the Court's directions requiring the filing of witness statements and trial bundles, Court invoked Order 17 Rule 4 of the Civil Procedure Rules²² and proceeded with the case *ex parte*. The Defendants therefore led no evidence on the matters necessary to establish a legitimate interest and could not have discharged the burden imposed by Regulation 10(4).

8. Quality of Information as the Proper Basis for Liability

Section 3(1)(e) of the DPPA provides for the principle of information quality as a binding obligation on every person or entity that collects, processes, holds or uses personal data. In like manner, Section 15(1) of the DPPA provides that a data collector, processor or controller "shall ensure that the data is complete, accurate, up-to-date and not misleading having regard to the purpose for its collection or processing".

Where journalists are involved in processing personal data, Paragraph 2 of Schedule 4 to the Press and Journalist Act²³ places a duty on them to avoid publishing inaccurate, misleading or distorted information and Paragraph 3 requires them to respect the constitutional right to privacy.

20. AdLegal International Limited v WhatsApp LLC and another, at paragraph 45.

21. Silver Kayondo v Monitor Publications and Others, page 2 of the Judgment.

22. SI 71-1.

23. Cap. 100

The relationship between the principle of accuracy and the requirement that personal data is not misleading was considered in the case of *Dale Vince v Associated Newspapers Limited*,²⁴ by the England and Wales Court of Appeal (Civil Division) where a newspaper published photographs of the appellant beneath a headline referring to a 'sex harassment' donor. Although the appellant appeared later on in the news story, he was not the sex harassment donor the article talked about. Vos MR did not determine whether the publication was inaccurate²⁵ but held that the obligation to avoid publishing misleading information extended beyond the accuracy obligation.²⁶ Since many readers do not proceed beyond the headline and accompanying images, they would understand the appellant to be the 'sex harassment donor' who was being referred to.²⁷ Having failed to take the care required of it to avoid publishing misleading information and images, the newspaper was held to have processed the appellant's personal data unfairly.

In the instant case, the Plaintiff's tweet stated that "*Lenders push values of their shareholders*". The Defendants took the original tweet, altered it and republished it stating that "*Lenders push value for their shareholders*," replacing the Plaintiff's original wording of "values" with "value" and "of" with "for". The Plaintiff's original tweet conveys a narrative that lenders push the beliefs, principles or interests of their shareholders while the version quoted by the Defendants conveys a financial proposition that lenders focus on increasing shareholder returns. The Defendants additionally attributed to the Plaintiff a statement, "*Uganda, as a donor-dependent country, may be left with little choice but to adhere*", which he averred that he never made.

Having regard to the purpose of processing, which was to report on the Plaintiff's expert commentary on the conduct of lenders and the World Bank-Uganda situation, the Defendants were required to ensure that the information attributed to the Plaintiff was accurate (in the sense that it faithfully reflected his words and views and not whether those views were objectively correct) and not misleading. The alteration of the first statement inaccurately recorded the words used by the Plaintiff and was misleading as to the meaning they conveyed. The attribution of the second statement inaccurately represented him as having expressed a view he denied making. In both instances, the Defendants failed to take the care required of them by Paragraph 2 of Schedule 4 to the Press and Journalist Act before publishing altered and invented words under the Plaintiff's name. The false attribution may also engage separate claims arising from false attribution in defamation.

24. [2026] EWCA Civ 899 (Hereinafter '*Dale Vince v Associated Newspapers Limited*').

25. *Dale Vince v Associated Newspapers Limited* at paragraph 13 and 70.

26. *Dale Vince v Associated Newspapers Limited* at paragraph 69.

27. *Dale Vince v Associated Newspapers Limited* at paragraphs 13 and 57.

From the above, this case presented a straightforward dispute on information quality. The Court's failure to consider the principle of accuracy and the requirement that personal data should not be misleading meant that it did not fully engage with the nature of the complaint before it, resulting in an incomplete analysis of the basis upon which liability could arise under the DPPA.

9. The Missing Journalistic Use Exception

This case exposes a critical gap in the statutory framework governing data protection and privacy in Uganda. Utilising personal information may be necessary for reporting news, live events and matters of national concern, consistent with the right to freedom of expression and obtaining consent before information is used might not be feasible in all circumstances. Kenya's Data Protection Act²⁸ expressly recognises this and its Section 30(1)(b)(viii) permits the processing of personal data, without the consent of the data subject, where the processing is necessary for journalistic purposes.²⁹ South Africa takes a broader exclusionary approach and its Section 7 excludes the applicability of the Protection of Personal Information Act³⁰ altogether from processing of personal data relating to journalistic, literary or artistic expressions.³¹

The DPPA provides no express basis or exemption for the processing of personal data for journalistic purposes. This may unduly constrain the exercise of the right to freedom of expression guaranteed under Article 29 of the Constitution more so where the processing is necessary to report on matters of legitimate public interest.³²

10. Jurisdiction of the High Court to hear Data Protection Claims

Another contention that implicitly arises from this dispute is whether the High Court has jurisdiction to hear a data protection claim in light of the fact that an operational statutory office, the PDPO, exists to handle such disputes. To resolve that contention, recourse should be sought from the provisions that provide for the respective jurisdictional powers of the PDPO and the High Court.

Article 27 of the Constitution provides for the foundational right to privacy protecting individuals, home or correspondence from unjustified intrusion and Section 31 provides that any data subject who believes that their rights under the DPPA have been infringed can make a complaint to the Authority (PDPO).

28. Cap. 411C.

29. Section 52 also excludes the applicability of the Kenya Data Protection Act to processing of personal data for journalistic purposes. However, the Office of the Data Protection Commissioner (ODPC), Guidance Notes on Processing for Journalistic Purpose, 2025 recognise the importance of accuracy in the processing of personal data for journalistic purposes as a key principle in preserving the privacy rights of data subjects. See, Office of the Data Protection Commissioner, "Guidance Notes on Processing for Journalistic Purpose, 2025", accessible via <https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-%E2%80%93-GUIDANCE-NOTES-for-Journalistic-Purpose.docx-.pdf> at pages 15, 30, 31 and 42.

30. Act No. 4 of 2013.

31. See also, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Article 85.

32. Collaboration on International ICT Policy for East and Southern Africa (CIPESA), *The Highs and Lows of Uganda's Data Protection and Privacy Act (2019)* at page 3.

On the other hand, Article 50 provides an individual who believes that their rights have been infringed a right to apply for redress in any court of competent jurisdiction and Article 139 gives the High Court unlimited original jurisdiction. This means that the High Court can hear any matter regardless of its value, subject matter or where the cause of action arose in Uganda. In recognition of this, Section 33 allows an aggrieved data subject who has suffered damage to apply to a court of competent jurisdiction to seek compensation³³ which may be the High Court depending on the circumstances.

However, the High Court's jurisdiction is both unlimited and limited. Article 139 itself expressly provides that the High Court's jurisdiction is 'subject to the provisions of the Constitution'. Accordingly, any limitation on the High Court's jurisdiction must find its basis in the Constitution itself.

The Supreme Court clarified the scope of the High Court's unlimited original jurisdiction under Article 139 in the case of *Uganda Revenue Authority v Rabbo Enterprises (U) Ltd & Anor.*³⁴ The Supreme Court held that although Article 139 confers unlimited original jurisdiction on the High Court, that jurisdiction is subject to other provisions of the Constitution.³⁵ This means that any limitation, variation or modification of the High Court's unlimited original jurisdiction must find its basis in an express provision of the Constitution itself.³⁶ Accordingly, in the *URA v Rabbo* case, since the matter involved a determination of a tax dispute, the Supreme Court qualified the High Court's unlimited original jurisdiction in that regard to Article 152(3) of the Constitution which expressly establishes a specialised body for the determination of tax disputes.³⁷ On that basis, the Supreme Court held that the Tax Appeals Tribunal was the court of first instance supposed to resolve tax disputes.

The Supreme Court further buttressed its reasoning in the statutory framing of the Tax Appeals Tribunal Act³⁸ Section 27 of which provides for appeals from the Tax Appeals Tribunal to the High Court. The Court interpreted this appellate structure as demonstrating Parliament's intention that tax disputes be determined by the Tribunal in the first instance before reaching the High Court.

In light of the *URA v Rabbo* case, the *Kayondo* case is distinguishable. Unlike tax disputes, the Constitution contains no equivalent of Article 152(3) in relation to the right to privacy under Article 27 limiting the High Court's jurisdiction or requiring privacy disputes to first be filed before the PDPO. Therefore, while the PDPO is the

33. DPPA

34. Civil Appeal 12 of 2004, Judgment of Professor Lillian Tibatemwa-Ekirikubinza. (Hereinafter referred to as "*URA v Rabbo*").

35. *URA v Rabbo*, page 10.

36. *Habre International Co. Limited v Kassam & Others*, Civil Appeal 4 of 1999, Judgment of Karokora, JSC at page 3.

37. *URA v Rabbo*, page 10.

38. Now Cap. 341.

statutory office established to administer and enforce the DPPA, the High Court is not precluded from entertaining privacy claims at first instance.

11. Conclusion

The Defendants published misleading and inaccurate statements while attaching the Plaintiff's name, nationality and profession to them. That was the wrong they committed and the Court's reasoning would have been more coherent had it grounded liability in the Defendants' failure to comply with the obligation under Sections 3(1)(e) and 15 of the DPPA to ensure that personal data was accurate and not misleading rather than in the absence of consent as the lawful basis for processing personal data.

12. Recommendations

12.1 Media Actors Must Take Care When Publishing Information

Media actors are primarily engaged in the business of collecting, creating and disseminating information. As discussed above, the DPPA puts in place obligations to ensure that all information processed about identifiable individuals be accurate, up-to-date and not misleading. While this obligation does not suggest that errors in journalism can never occur,³⁹ it requires media actors to adopt comprehensive editorial review processes such as fact checking, source verification, proof reading and where appropriate, legal review before publication to avoid inaccuracies. Where inaccuracies arise, Regulation 30 gives data controllers and collectors a period of thirty (30) days within which to act on legitimate rectification requests from data subjects, failing which a complaint may be made to the PDPO.⁴⁰ Media houses and journalists should therefore ensure that their practices protect accuracy of information both at the point of publication and where individuals raise legitimate concerns about continued dissemination of inaccurate information, rectifications are effected.⁴¹

12.2 Utilisation of Judicial Referral Mechanisms to Access the PDPO's Specialised Data Protection Expertise

Section 26 of the Judicature Act⁴² gives the High Court power to refer any question arising in a civil cause or matter to an official or special referee for inquiry and report. This comment recommends greater utilisation of this referral mechanism where proceedings before the courts of general jurisdiction raise questions falling within

39. See *Dale Vince v. Associated Newspapers Limited*, [2026] EWCA Civ 899 at paragraph 58.

40. Data Protection and Privacy Regulations, 2021.

41. In this specific case, the Defendants duly rectified the inaccuracies in the article by dealing away with the Plaintiff's comments altogether in the online article. See Deogratius Wamala, 'Inside Uganda's Talks with the World Bank' Daily Monitor (16 September 2023) <https://www.monitor.co.ug/uganda/news/national/inside-uganda-s-talks-with-the-world-bank-4370382> accessed 29 August 2026. However, other sites such as Africa Press that had republished the original article from the Defendants still carry the unrectified version, see Deogratius Wamala, 'Inside Uganda's Talks with the World Bank' Africa-Press (16 September 2023) <https://www.africa-press.net/uganda/all-news/inside-ugandas-talks-with-the-world-bank> (unrectified as at 29 August 2026).

42. Cap. 16.

the specialised expertise of another court, tribunal or statutory office. Such mechanisms will allow the High Court to benefit from the expertise of persons who deal with the subject matter on a day-to-day basis and may therefore be better placed to interrogate specialised questions than a generalist court dealing with a wide range of matters. In the instant case, where the dispute raised questions concerning the application of the DPPA, the Court could have sought the views of the PDPO on the data protection issues arising from the facts to aid its determination.⁴³

12.3 Inclusion of a Journalistic Lawful Basis for Processing Personal Data

Section 7 of the DPPA should be amended to expressly include a lawful basis for processing of personal data for journalistic purposes subject to a public interest test and other obligations arising under the DPPA and its regulations.

12.4 Elevation of Legitimate Interests from the Regulations to the Act

Legitimate interests should be elevated from Regulation 10 and expressly recognised under Section 7(2) of the DPPA as an independent lawful basis for processing personal data. This would address the current legislative tension arising from reliance on subsidiary legislation to establish a lawful ground not expressly provided for in the primary legislation.

43. This recommendation applies in equal measure for other disputes in employment, public procurement and disposal of assets, intellectual property which have statutory tribunals, courts and offices that can handle their resolution.

13. References

Constitution

Constitution of the Republic of Uganda, 1995 (as amended)

Legislation

Data Protection and Privacy Act, Cap. 97

Judicature Act, Cap. 16

Press and Journalist Act, Cap. 100

Civil Procedure Rules, SI 71-1

Data Protection and Privacy Regulations, 2021

Data Protection Act, Cap. 411C (Kenya)

Protection of Personal Information Act No. 4 of 2013 (South Africa)

Case Law

Habre International Co. Limited v Kassam & Others, Civil Appeal 4 of 1999

Uganda Revenue Authority v Rabbo Enterprises (U) Ltd & Anor, Civil Appeal 12 of 2004.

Nalubega Shadia v Stabex International Limited, Civil Suit No. 665 of 2021.

AdLegal International Limited v WhatsApp LLC and another, Complaint No. PDPO 086/2025

Dale Vince v. Associated Newspapers Limited, [2026] EWCA Civ 899

Svensson v Retriever Sverige AB, Case C 466/12

Hansard

Hansard of the 10th Parliament of Uganda, 5th December 2018, accessible via <https://cmis.parliament.go.ug/cmis/views/a78d1132-7688-45f0-8d11-327688f5f054%253B1.0>.

Guidance Note

Office of the Data Protection Commissioner, "Guidance Notes on Processing for Journalistic Purpose, 2025" (Kenya)

Articles

Collaboration on International ICT Policy for East and Southern Africa (CIPESA), *The Highs and Lows of Uganda's Data Protection and Privacy Act (2019)*

Deogratius Wamala, 'Inside Uganda's Talks with the World Bank' Africa-Press (16 September 2023)

<https://www.africa-press.net/uganda/all-news/inside-ugandas-talks-with-the-world-bank>

Deogratius Wamala, 'Inside Uganda's Talks with the World Bank' Daily Monitor (16 September 2023)

<https://www.monitor.co.ug/uganda/news/national/inside-uganda-s-talks-with-the-world-bank-4370382>

Facebook, 'Basic Privacy Settings and Tools' Facebook Help Centre,

<https://www.facebook.com/help/1297502253597210>

LinkedIn, 'Manage your account and privacy settings' LinkedIn Help,

<https://www.linkedin.com/help/linkedin/answer/a1337839/managing-your-account-privacy-settings?lang=en>

X, 'About public and protected Posts' X Help,

<https://help.x.com/en/safety-and-security/public-and-protected-posts>

Tweet/X

Silver Kayondo, 'World Bank-Uganda' X post (10 August 2023),

<https://x.com/silverkayondo/status/1689514927440941056>



DPO
PRIVACY CENTRE
EAST AFRICA



Interested in receiving similar
publications direct to your inbox?

Subscribe to our Substack

substack.com/@privacycentreea 

Want to contribute an article or have an
idea for collaboration?

Contact Us:

info@dpoprivacycentre.com 