

Access is not Consent: Lessons from DPLAN v. Truecaller

October 2026

Introduction

The case of ***Incorporated Trustees of the Data Privacy Lawyers Association (DPLAN) v. Truecaller International LLP ("DPLAN v. Truecaller")*** raises important questions about consent and accountability in data protection. The applicants challenged Truecaller's collection, processing and display of telephone numbers and associated identities belonging to non-users who had not consented to such processing. In considering the dispute under ***Section 37*** of the Constitution of the Federal Republic of Nigeria 1999 **(the "CFRN")** and the Nigeria Data Protection Act 2023 **(the "NDPA")**, the Court rejected the proposition that one user's consent extends automatically to others whose data appears in their contact list. However, it dismissed the application for failure to establish a breach of fundamental rights through cogent and credible evidence. This article examines the Court's reasoning on consent, data controller accountability, the burden of proof and Truecaller's public safety justification, alongside the implications for organisations processing third-party personal data.

Background of the Case

The applicants **(an association of privacy lawyers)** challenged Truecaller's processing and display of personal information belonging to individuals who were not users of its application. Specifically, they complained that the telephone numbers and associated identities of the second and third applicants appeared on the platform despite their alleged lack of consent which infringed their constitutional right to privacy under ***Section 37 CFRN*** and contravened the NDPA. They argued that the publication of their information deprived them of control over their personal data and exposed them to risks including identity theft, misuse of their information and unwanted intrusion.

On the other hand, Truecaller maintained that it was an Indian entity without an office, server or infrastructure in Nigeria and characterised its application primarily as a dialer. According to Truecaller, contact information reached its platform when a user voluntarily activated the optional "Enhanced Search" feature and confirmed the authority to share the user's contacts. It argued that those users were responsible for obtaining the necessary

consent. Further, Truecaller relied on public safety and legitimate interests to justify its processing by stating that its "Public Safety Function" helped users identify spam calls, fraudulent calls and other intrusive communications. Truecaller further contended that the second applicant's telephone number was already available on Instagram, while the third applicant's number was a business line. It challenged the applicants' failure to identify the non-user members whose rights were allegedly infringed and argued that no sufficient harm had been established.

The dispute therefore required the Court to consider whether user consent justified the processing of third-party contact information, who bore responsibility for that processing, and what evidence was necessary to establish a violation of the constitutional right to privacy.

The Decision of the Court

The Court recognised that the constitutional right to privacy under ***Section 37 CFRN*** encompasses data protection, while acknowledging that the right is subject to the exceptions under ***Section 45 CFRN***, including those relating to public safety, public order, public health and the rights and freedoms of others. Although it accepted the importance of protecting users from spam calls, fraudulent communications and similar risks, it emphasised that reliance on public safety does not dispense with the requirement to establish a lawful basis for processing personal data under the NDPA.

Furthermore, the Court rejected the argument that a user's agreement to upload contact information automatically constitutes consent from the individuals whose details appear in the address book. It found no basis for assuming that users possess implied authority to consent on behalf of those individuals. The Court also rejected Truecaller's attempt to transfer responsibility for the processing to its users, focusing instead on the platform's control over the purposes and subsequent use of the uploaded information.

Despite these findings, the Court dismissed the application because the applicants had failed to establish the alleged fundamental-rights violation through cogent, credible and convincing evidence. It also reasoned that the public safety function involved searching for a name using a telephone number already known to the searching user, and that the alleged misappropriation of personal information, without economic harm or another established injury, did not amount to damage or injury. The judgment thus distinguished between the legal requirements governing personal data processing and the applicants' failure to establish an entitlement to the reliefs sought.

Analysis of the Decision

Consent is Personal

Section 65 of the NDPA defines consent as a freely given, specific, informed and unambiguous indication of a data subject's wishes, including consent given by a person authorized to act on another individual's behalf. This qualification does not confer general authority on individuals to consent to the processing of other people's personal data. The person giving consent must possess the requisite authority to act for the affected

individual. Truecaller's argument appeared to assume that users who upload their address books possess authority to share the personal information of everyone listed in them. The Court rejected that assumption, establishing that possession of another person's telephone number does not, without more, confer authority to consent to its subsequent processing and disclosure. For platforms that depend on user-contributed information, the practical difficulty of obtaining consent from every affected individual does not itself establish a lawful basis for processing their data.

Accountability cannot be outsourced

Truecaller argued that users voluntarily activated contact sharing and should therefore bear responsibility for the information uploaded. The Court rejected this position by focusing on the platform's role in determining how the information was used rather than accepting the allocation of responsibility advanced by Truecaller. Hence, it held that Truecaller acts as a controller in relation to its users and as a processor regarding the data transferred to its servers, and it applied the duty of care and accountability under the law.

This is consistent with the General Data Protection Regulation (GDPR) under which a platform that designs the processing architecture and derives its own commercial purpose from user-contributed data will typically be treated as a controller, or at minimum a joint controller rather than a mere processor regardless of how its terms of service characterizes the relationship.

The Burden of Proof

Section 26(1) of the NDPA places the burden of demonstrating consent on a controller that relies on consent as its lawful basis. This requirement recognize that the controller ordinarily holds the records needed to establish whether valid consent was obtained. However, the court in applying the case ***Oando Plc v Farmatic Biogas West Africa Ltd & Anor***, dismissed the application by holding that a fundamental rights applicant must prove a real and factual breach by cogent and credible evidence. It reasoned that the public safety function works on a number-for-name search, so the searching user must already have the number. It also observed that misappropriation of personal information, without economic harm or other injury, is "neither damage nor injury."

If the controller bears the burden of proving consent, once the processing of an applicant's personal data is established, it should fall to the controller to demonstrate that consent was obtained rather than require the applicants to prove its absence through evidence of harm. The Court's observation on injury also sits uneasily with the definition of a personal data breach under ***section 65 NDPA***, which focuses on unauthorised access to or disclosure of personal data without requiring proof of economic loss. It is also difficult to reconcile with the Court of Appeal's decision in ***Emerging Markets Telecommunication Services Ltd v. Eneye*** that unsolicited messages alone constituted a breach of ***Section 37 of the CFRN***. Whether proof of harm is a prerequisite to obtaining a declaration that processing lacks a lawful basis therefore remains unresolved by this judgment.

Public Safety as a Lawful Basis

Truecaller's reliance on public safety raises an important question about the relationship between legitimate objectives and the legal requirements governing personal data processing. The Court acknowledged the public interest in protecting users from spam calls, fraud and intrusive communications, but the legitimacy of that objective does not establish that the processing undertaken to achieve it is lawful.

Section 45 CFRN identifies circumstances in which laws may restrict certain fundamental rights. It does not independently authorize every private organisation to process personal data without satisfying the NDPA. Under ***Section 25 NDPA***, a controller must establish an applicable lawful basis, which might include consent, a task carried out in the public interest or legitimate interests, subject to the relevant statutory conditions.

Where a controller relies on legitimate interests, the law requires consideration of whether those interests override the data subject's fundamental rights and freedoms. The assessment should address the processing purpose, its necessity, the reasonable expectations of affected individuals and the availability of less intrusive alternatives. A platform's usefulness in identifying suspicious telephone numbers, for instance, does not automatically establish the necessity of displaying information about individuals who have never used the service. Although the Court rejected the proposition that public safety eliminates the need for a lawful basis, it did not clearly identify the precise basis supporting the processing of non-users' information or explain fully how the relevant statutory conditions were satisfied.

Conclusion

This decision distinguishes access to personal data from lawful authority to process it. The Court rejected the proposition that a user's consent to upload contact information automatically constitutes consent from the individuals identified in the address book. It also rejected Truecaller's attempt to transfer responsibility to its users and reaffirmed the need for a lawful basis under the NDPA.

Nonetheless, the Court dismissed the application because the applicants failed to establish the alleged fundamental-rights violation through cogent and credible evidence. Its treatment of the evidential burden, the controller's statutory obligation to prove consent and the role of harm leaves important questions unresolved. The decision offers useful guidance on consent and accountability, but its reasoning on evidence and injury limits the extent to which it settles the relationship between unlawful processing, constitutional privacy rights and the remedies available to affected individuals.

You may reach out to our team at: info@wtsblackwoodstone.com for further guidance and support.

Authors



Merry Ikatari
Merry@wtsblackwoodstone.com



Daniel Okpalifo
Daniel@wtsblackwoodstone.com

About WTS Blackwoodstone

WTS Blackwoodstone is an international business law firm that provides innovative business solutions for clients with diverse needs. The Firm's core practice areas include Corporate and Commercial law, Tax Advisory & Compliance and Transactional Services to resident and non-resident companies doing business in Nigeria. Our practice is based in Lagos and Abuja and is strategically placed to offer hands on legal services to our clients in the major economic hubs of Nigeria and the rest of Africa.

Our clients include locally headquartered multinationals, medium and small local and international clients, family-owned businesses, government agencies and high net worth individuals.

WTS Blackwoodstone is the Nigerian network partner of WTS Global. With representation in over 100 countries, WTS Global has grown to a leadership position as a global tax practice offering the full range of tax services and aspires to become the preeminent non-audit tax practice worldwide. WTS Global embodies the core values which we as a firm base our daily actions upon – innovation, excellence, reliability, and a global mindset – thereby further strengthening our firm's offering to multi-national clients.

About WTS Global

With representation in over 100 countries, WTS Global has already grown to a leadership position as a global tax practice offering the full range of tax services and aspires to become the preeminent non-audit tax practice worldwide. WTS Global deliberately refrains from conducting annual audits in order to avoid any conflicts of interest and to be the long-term trusted advisor for its international clients. Clients of WTS Global include multinational companies, international m.id-size companies as well as private clients and family offices.

The member firms of WTS Global are carefully selected through stringent quality reviews. They are strong local players in their home market who are united by the ambition of building a truly global practice that develops the tax leaders of the future and anticipates the new digital tax world.

WTS Global effectively combines senior tax expertise from different cultures and backgrounds and offers world-class skills in advisory, in-house, regulatory and digital, coupled with the ability to think like experienced businesspeople in a constantly changing world.

For more information please see: wts.com

Imprint
WTS Blackwoodstone
Unit 12, No 8 Office Apartments, Plot 8, Rasheed Alaba Williams, Lekki,
Lagos
Nigeria
T: +234 9033 501 613 www.wtsblackwoodstone.com |
info@wtsblackwoodstone.com

*[**Disclaimer**: The above information is intended to provide general guidance with respect to the subject matter. This general guidance should not be relied on as a basis for undertaking any transaction or business decision, but rather the advice of a qualified consultant should be obtained based on a taxpayer's individual circumstances. Although our articles are carefully reviewed, we accept no responsibility in the event of any inaccuracy or omission. For further information please refer to the author.*

wts global