

STRENGTHENING TRUST AND ACCOUNTABILITY IN THE RDRS THROUGH PRIVACY AND CYBERSECURITY SAFEGUARDS

I welcome the recommendation of the Standing Committee to continue the RDRS beyond its pilot phase and to begin introducing authentication for specific requestor groups, particularly law enforcement. From my perspective as a lawyer in Nigeria working at the intersection of cybersecurity and privacy, this step is critical. Authentication is not just a technical adjustment, it is a legal and trust safeguard. In Africa, where the Cybercrimes Act and new data protection laws such as Nigeria's Data Protection Act 2023 are increasingly being enforced, it is important that any disclosure of registrant data is verifiable, accountable, and auditable. Without this, the system risks either misuse or rejection by regulators and contracted parties who fear liability.

That said, I caution against an overly complex accreditation model that may prove costly and inaccessible for developing regions. A layered and phased approach, starting with the most sensitive use cases such as law enforcement, strikes the right balance. This would allow African governments and regulators to strengthen their response to DNS abuse and cybercrime while still respecting privacy and proportionality. My conclusion is that the RDRS should remain online and be improved in a pragmatic way, building on what works and adapting to diverse regional legal environments. Done properly, it can become a trusted bridge between cybersecurity needs and the protection of fundamental rights.

FOLARANMI UMORU,
Lawyer, End-user
Nigeria,