

Digital Accountability Doesn't Need Identification

NonCommercial Stakeholder Group position on Data Accuracy

Non-Commercial Stakeholder Group position on Data Accuracy

Introduction

When "Accuracy" Becomes "Identification"

- "Give us your passport or you cannot register a domain name."
- Expanding accuracy beyond *contactability* risks excluding users and undermining trust.
- Over-collection of data → surveillance and censorship risks.

Case Studies of Overreach

China's Cybersecurity Law (2017): real-name registration + facial recognition → expanded state surveillance.

First Wap Investigation: linkage of "accurate" data across systems enabled tracking and repression.

Discord Incident (2025): 70,000 users' government ID photos exposed after third-party vendor breach during age-verification checks. Highlights risks of outsourcing identity verification—meant to ensure accountability, but endangering privacy when vendors lack strong safeguards.

Identification mechanisms can be weaponized once data becomes linkable.

Non-Commercial Stakeholder Group position on Data Accuracy

NCSG's Core Position

Accuracy = Contactability

- Registrants must be reachable, not identifiable.
- ICANN's mission: ensure operability, not regulate identity.
- Identity checks risk turning ICANN into a global ID authority.

Non-Commercial Stakeholder Group position on Data Accuracy

What Contactability Entails

Functional Contact Information

- Email works and monitored by the user.
- Registrant responds to legitimate issues.
- Registrar validates contact channel functionality.

Non-Commercial Stakeholder Group position on Data Accuracy

Risks of Expanding Accuracy

Why Identification Is Dangerous

- **Privacy:** More data → more breaches.
- **Expression:** Anonymity protects activists and journalists.
- **Safety:** Stored IDs lead to targeting.
- **Access:** Many people lack government IDs.

Non-Commercial Stakeholder Group position on Data Accuracy

Addressing Common Concerns Law Enforcement & Public Safety

- Existing MLAT and disclosure channels are sufficient.
- Overcollection increases breach risk.
- EU courts reject indiscriminate data retention – proportionality matters.

Non-Commercial Stakeholder Group position on Data Accuracy

Addressing Common Concerns (2)

Intellectual Property Interests

- Abuse persists despite ID requirements.
- Fraudsters use fake or stolen IDs.
- Tools like URS and abuse contacts already work.
- Over-broad IP enforcement risks overblocking.

Non-Commercial Stakeholder Group position on Data Accuracy

NIS2 and "Identification Creep"

A Warning from Europe

- Article 28 → "accurate and complete" interpreted as ID checks.
- Creates de facto ID regimes via eID systems.
- Chills anonymity and concentrates personal data.

Non-Commercial Stakeholder Group position on Data Accuracy

Rights-Respecting Accuracy

1. Define accuracy strictly as functional contactability.
2. Support registrar-level email validation.
3. Maintain due-process-based data access.
4. Apply privacy-by-design and minimization.

Non-Commercial Stakeholder Group position on Data Accuracy

Final Message

Contactability, Not Identification

- Protect DNS stability *and* human rights.
- Uphold ICANN's mission limits.
- Reaffirm that WHOIS/RDAP ≠ global ID system.