Non-Commercial Stakeholders Group (NCSG)
Position Paper on Data Accuracy

Executive Summary

Will obtaining and keeping a domain name soon require showing identity documents? That possibility exists as ICANN stakeholders discuss the concept of domain registration data “accuracy”.

Although some countries already require identity documentation for domain registration, the Non-Commercial Stakeholder Group (NCSG) maintains that ICANN should not follow this route, but instead ensure that “data accuracy”, in the context of domain registration, remains defined as contactability; i.e. the ability to reach a registrant via functional contact information. This paper reviews the rationale for avoiding the unnecessary dangers inherent in officially conflating “accuracy” with “identity”.

Accuracy, when limited to contactability, serves ICANN’s mission, since a fundamental requirement for managing the DNS is the ability for parties to communicate about domains, whether for technical, contractual or administrative purposes. This is fully met when verifiable domain registrant contact details are collected and regularly reviewed, ensuring that the registrant is aware of, and can respond to, legitimate inquiries or compliance issues, or other issues related to the domain name. By requiring registrants to disclose and verify their personal identity, ICANN’s becomes a global identity authority, which is neither its purpose nor within its legal capacity

Furthermore, expanding accuracy to include verification of identity carries significant and disproportionate human rights risks. For example, collecting and storing verified identity information would vastly increase the amount of sensitive data that registrars must store and maintain, raising the risk of breaches, surveillance, and misuse, whereas limiting registration data allows for anonymous or pseudonymous registration, providing vital privacy and security protections that are fundamental to exercising the freedom of opinion and expression.

Many stakeholders, including law enforcement and intellectual property interests, along with some ICANN contracted parties, have expressed concerns, arguing that verified identity data supports addressing challenges such as cybercrime, intellectual rights infringement and DNS abuse. The NCSG agrees that all of these issues present major challenges, but emphasize that either existing mechanisms exist to confront them or that collecting identifying data does little to mitigate the harm while only adding additional risk. In particular, the paper highlights how the implementation of the EU’s NIS2 Directive demonstrates how countries are already conflating accuracy with identification.

The NCSG believes there are ways that ICANN can promote accuracy without overreach, and maintains that defining “accuracy” as “contactability” ensures that ICANN fulfills its focused The NCSG calls on ICANN to reaffirm that contactability, not identification, is the correct and proportional standard for registration data accuracy and refrain from describing WHOIS or RDAP as a mechanism to “identify” the registrants

Introduction

“Give us your passport or you cannot register a domain name.” While there are several ccTLD registries that require this, including China and several EU countries, this is not a requirement you hear often from registrars. But if accuracy is misinterpreted, you might. And if you don’t have an ID, or cannot present it, or the registrar does not recognize it as valid (because maybe it’s in another language), then you won’t be allowed to register a domain name. And that will be bad for the Internet, for the end user and for trust in the Internet.

The dangers of collecting more data than is needed has been illustrated in many case studies. China’s Cybersecurity Law enacted in 2017 already requires real-name identity verification for domain name registration, and the government has added new requirements for all internet users to register via the National Online Authentication App using their national identification card and facial recognition. In a joint analysis[1], CHRD and ARTICLE 19 determined that the regulations give the Chinese government even greater opportunities to surveil and control online speech, expand censorship, and threaten reprisals against human rights defenders.[2] Another case that was recently revealed was the “First Wap” investigation in a collaborative exposé by Lighthouse Reports and partners exposing how a company called First Wap, run from Jakarta and Dubai by European executives, secretly sold and brokered surveillance technology to governments and intelligence clients worldwide, often evading export controls and sanctions.[3] The First Wap investigation illustrates how easily identification mechanisms can be weaponized once personal data becomes linkable across systems. Surveillance firms like First Wap operate by stitching together fragments of “accurate” data - from phone registries, telecom logs, and open online records - to identify and track individuals. Combine those with a disclosure system or a centralized triage system and requiring ID verification from registrar, it facilitates surveillance and can risk human rights. It can also be an impediment for Internet access and online presence.

This case shows clearly what happens when too much data is collected and becomes available. When governments or regulators insist on high “accuracy” in domain registration data, they often conflate accuracy with verified identity. **What begins as a cybersecurity or accountability measure can evolve into a surveillance tool**, enabling states or intermediaries to unmask speakers, monitor dissidents, or suppress legitimate online expression. The First Wap story is a reminder that identification can create the very conditions for abuse that ICANN and other Internet governance organizations are meant to overcome.

The Non-Commercial Stakeholder Group (NCSG) maintains that “data accuracy” in the context of domain registration must be defined strictly as **contactability**; i.e. the ability to reach a registrant via functional contact information.

This paper examines the concept of contactability and explores how efforts to expand the definition of accuracy beyond contactability not only risks exceeding ICANN’s technical coordination mandate to ensure the stable and secure operation of the Domain Name System (DNS), but also would endanger privacy, freedom of expression, and the safety of Internet users worldwide.

[1] https://www.nchrd.org/wp-content/uploads/2025/02/internetID_full-analysis-new.pdf

[2] ARTICLE 19, “China: New Internet ID System a threat to online expression” (2025).

[3] See the report on this issue at this link: https://www.lighthousereports.com/investigation/surveillance-secrets/

Accuracy as Contactability Serves ICANN's Mission

The core operational requirement for the DNS is that registrars and registries can communicate effectively with registrants regarding their domains, whether it be for technical, contractual, or administrative purposes.

This requirement is fully met when:

- The contact information provided (e.g., email or phone) is functional and regularly monitored to ensure the registrant can be reached;
- The registrant can respond to legitimate inquiries or compliance issues, or technical issues related to the domain name; and
- The registrar maintains processes for validating the operability of contact data.

By requiring registrants to disclose and verify their personal identity, ICANN's role becomes that of a **global identity authority**, which is neither its purpose nor within its legal capacity.[4]

The Many Risks of Expanding Accuracy to Mean Identification

Expanding accuracy to include verification of identity carries significant and disproportionate human rights risks:

- **Privacy and Data Protection:** Collecting verified identity information would vastly increase the amount of sensitive data registrars hold, raising the risk of breaches, surveillance, and misuse.[5]
- **Freedom of Expression:** Anonymous or pseudonymous registration provides vital privacy and security protections that are fundamental to exercising the freedom of opinion and expression,[6] particularly for journalists, activists, and individuals working under repressive regimes.[7]
- **Safety and Security:** Publicly or even administratively stored identity data can lead to harassment, targeting, or physical danger for vulnerable registrants.[8]

These risks are not hypothetical but are well documented in human rights reports and past incidents of data misuse within the DNS ecosystem.

Addressing Common Concerns

a. **Law Enforcement and Public Safety**
Law enforcement agencies often argue that access to verified identity data would help trace cybercriminals and prevent online abuse. While these goals are legitimate, broad identity collection at the point of registration has not been shown to be either necessary or effective.

[4] ICANN Bylaws, Art. 1, Sec. 1.1(a) indicates that "ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide...".

[5] Data Breaches of registrars and registries have occurred (example: en.wikipedia.org/wiki/2021_Epik_data_breach).

[6] ARTICLE 19, Privacy and surveillance.

[7] UN Special Rapporteur on Freedom of Expression, "Encryption, Anonymity and the Human Rights Framework," A/HRC/29/32 (2015).

[8] ARTICLE 19, "Whois and Privacy," Policy Brief (2018).

- **Existing mechanisms work:** Law enforcement already uses established channels, such as **mutual legal assistance treaties (MLATs)** and **registrar disclosure processes**, to request registrant data in specific investigations.
- **Overcollection risks misuse:** Registrar or registry data breaches can have a more profound effect on registrants when stolen information goes beyond contactability. These risks become compounded when the countries where the registrar or registry are located have not yet implemented robust data protection laws.
- **Proportionality principle:** The **Court of Justice of the EU** has ruled that indiscriminate data retention violates fundamental rights.[9] This reasoning is equally applicable to pre-emptive collection of identity data.

The NCSG agrees that law enforcement needs timely cooperation, and that ICANN can facilitate legitimate access while maintaining due process and transparency *without redefining accuracy as anything more than contactability.*

b. Intellectual Property Interests

Intellectual Property Rights holders often raise concerns that anonymity enables infringement or phishing. Yet history shows that compulsory identity disclosure doesn't stop abuse, and sometimes enables it.

- **Abuse uses false identities:** Fraudulent domain registrations routinely use fake or stolen identity data. However, data that links the availability of detailed registrant identity to lower DNS abuse levels is lacking.
- **Effective alternatives exist:** The **Registrar Abuse Contact** and **Uniform Rapid Suspension (URS)** mechanisms provide quick remedies for IP-related harm without requiring identity disclosure.[10]
- **Chilling legitimate speech:** Examples exist of how overbroad IP or content enforcement, when applied at the DNS level, can easily suppress legitimate expression, and supports NCSG's argument that identity-based DNS control or verification increases the risk of collateral harm.[11]

The NCSG believes that accountability and enforcement can be achieved through validated contact channels, not mandatory identity exposure.

c. Contracted Parties (Registrars and Registries)

Registrars and registries already hold transactional data sufficient for compliance with national financial and anti-fraud laws. Requiring them to collect and store identity data for ICANN purposes would be duplicative, costly, and legally risky. Moreover, some are also against requiring domain name registrants showing ID.[12]

- **Regulatory conflicts:** Under the **2013 Registrar Accreditation Agreement (RAA)**, registrars in **Germany, Norway, and Canada** faced conflicts between WHOIS requirements and national data protection laws, documented in ICANN's correspondence with data protection authorities in those jurisdictions.[13]
- **Data breach risk:** As noted previously, the potential for data breaches demonstrate that expanding the scope of stored personal data increases systemic vulnerability.

[9] See as one example *Digital Rights Ireland Ltd v. Minister for Communications* (Joined Cases C-293/12 and C-594/12); *Tele2 Sverige AB v. Post- och telestyrelsen* (C-203/15).

[10] ICANN, "Uniform Rapid Suspension System (URS) Overview," Policy Briefing (2019).

[11] See https://cdt.org/insights/an-object-lesson-in-overblocking.

[12] See Tucows blog: why requiring registrants to show ID is a bad idea?
https://opensrs.com/blog/requiring-registrants-to-show-id-is-a-bad-idea/

[13] Article 29 Working Party Letter to ICANN on WHOIS, 26 November 2003; follow-up correspondence with European DPAs (2013–2015).

- **Proportional compliance:** Payment and billing records already provide traceability under Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations where applicable.[14]

It is the NCSG's position that registrars already maintain sufficient information to meet operational and legal obligations. ICANN should not impose redundant or conflicting identity verification duties.

Accuracy as legal obligation can be interpreted as a requirement for identification

The implementation of the EU's NIS2 Directive demonstrates how "accuracy" can become conflated with "identification".

While NIS2 does not explicitly mandate registrants to provide government-issued IDs, its Article 28 requires registrars and registries to collect, verify, and maintain "accurate and complete" data sufficient to identify domain holders. This verification duty has led several national authorities and registrars to interpret accuracy as necessitating identity verification through ID checks or eID systems. In practice, what begins as a technical obligation to ensure reliable contact data evolves into a de facto identity regime, where individuals are required to reveal personal information far beyond what is necessary for DNS coordination. This conflation of accuracy with identification not only chills anonymous or pseudonymous online activity but also introduces privacy and human rights risks by creating a centralized identity layer within the Internet's naming infrastructure. We cannot allow for ICANN policies to be interpreted that way.

A Balanced, Rights-Respecting Path Forward

ICANN can advance both accuracy and accountability without overreach by:

- Defining accuracy strictly as functional contactability;
- Supporting registrar-level validation of contact methods (e.g., email confirmation);
- Maintaining clear processes for responding to verified lawful data requests; and
- Upholding data minimization and privacy-by-design principles consistent with global norms.

Defining "accuracy" as "contactability" ensures that ICANN fulfills its focused technical mission while respecting the human rights commitments embedded in its Bylaws. Expanding accuracy to mean identification would neither enhance DNS stability nor deter abuse, but it risks a compromise to privacy, safety, and trust.

We call on ICANN to reaffirm that **contactability, not identification**, is the correct and proportional standard for registration data accuracy and refrain from describing WHOIS or RDAP as a mechanism to "identify" the registrants.

[14] Financial Action Task Force (FATF) Recommendations, "Customer Due Diligence and Record Keeping," (2012, updated 2020)