Access to Domain Name Registrant Private Data: Authentication, Authorization & Human Rights Impact Assessment

The Core Problem

Misdirected Requests

LEAs submit broad requests to entities that don't hold the data — registries vs registrars vs resellers vs hosts.

Jurisdictional Fragmentation

One case can span victim, registrar, and reseller across 3+ countries — each under different legal regimes.

Human Rights at Risk

Basic subscriber data — name, email, address — can trigger investigations, deportation, or persecution.

Authentication ≠ Authorization

AUTHENTICATION

Who is making this request? Do they have jurisdiction?

- Verify officer identity via official government domain email
- Independent callback to publicly listed agency phone
- Cross-check digital signatures and message headers
- Portal-based verification (Kodex, Google LERS)
- Zero-trust: never click embedded links; always validate out-of-band
- ⚠ **Even verified identity ≠ legitimate request**

AUTHORIZATION

Is the legally valid? Does it ?

- Subpoena → basic subscriber info (US, lowest threshold)
- Court order → metadata, IP logs, timestamps
- Search warrant → content data (highest threshold)
- GDPR balancing test → proportionality review (EU)
- MLAT / CLOUD Act / EIO for cross-border requests
- Human rights assessment required before any disclosure

Both gates must be passed — independently

Human Rights at Risk

Privacy (ICCPR Art. 17)

Subscriber data — name, email, address — enables profiling, surveillance, and targeted persecution without judicial review.

Free Expression (ICCPR Art. 19)

Unmasking the person behind a domain or social account can silence dissent, journalism, and whistleblowing globally.

Free Association (ICCPR Art. 22)

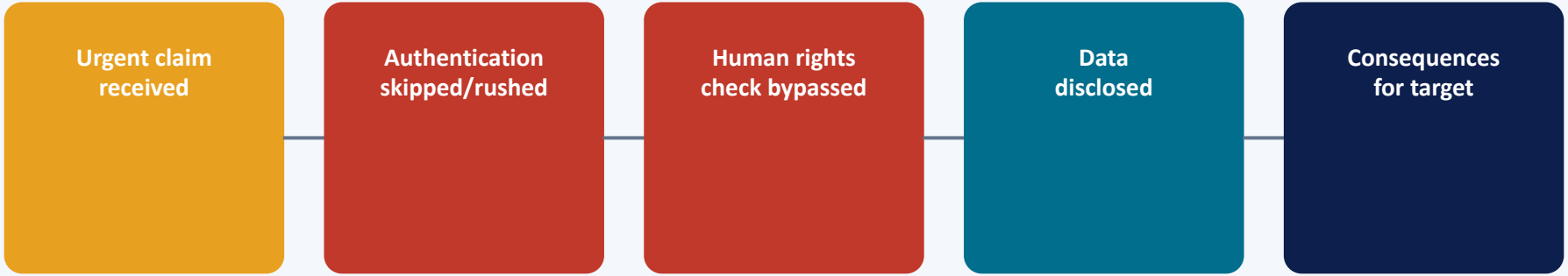
Registration data reveals organizational affiliations. Disclosure maps networks of activists, minorities, and opposition groups.

Life & Security (ICCPR Art. 6/9)

Data disclosed to jurisdictions using the death penalty or where torture is practiced can have irreversible, fatal consequences.

"Basic" subscriber data is not low-risk — it is the key to an individual's entire digital life.

Emergency / Urgent Requests — Specific Risks



⚠ **Known exploit:** In 2024–2025, a cybercrime group created a fraudulent account inside Google LERS by impersonating a government entity. The 2021 hacks obtained real user data from Apple, Meta, and Discord using forged emergency requests. Centralization creates high-value targets.

Human Rights Framework — Legitimacy, Necessity & Proportionality

Based on ICANN Bylaws Art. 1.2(b)(viii), CCWG-WS2 Framework of Interpretation (FOI-HR, 2019) & ICANN 81 HRIA Guidelines

1 Legitimacy

Does a valid legal basis exist?

The interference must pursue a legitimate aim recognised under international human rights law, specified in law and serving a genuine public interest.

- Grounded in a specific statute or court order?
- Legitimate aim under ICCPR / ECHR?
- Requesting authority legally empowered to demand this data?
- Could this request suppress political speech or dissent?

2 Necessity

Is this the least intrusive means?

The measure must be strictly necessary in a democratic society — the least intrusive means. Infrastructure data must be a last resort, not a first call.

- Alternative methods exhausted (OSINT, financial records, platform)?
- Domain registration data actually required for this investigation?
- Is this the correct layer (registry / registrar / reseller / host)?
- Would a narrower request achieve the same goal?

3 Proportionality

Does the harm outweigh the benefit?

Even a necessary measure must be proportionate — the investigative benefit must not be outweighed by harm to individual rights. Enhanced scrutiny for vulnerable targets.

- Scope of data limited to minimum necessary?
- Target a journalist, activist, dissident, or minority?
- Requesting jurisdiction apply death penalty or practise torture?
- Could disclosure map associations or expression beyond stated purpose?

Transparency & Accountability

- Notify registrant? (default: yes, unless court-ordered gag)
- Will this request appear in transparency reporting?
- Gag order judicially authorised? (informal secrecy insufficient)
- Is an audit trail maintained for accountability?

ICANN FOI-HR: No Core Value takes automatic priority. Balancing must be case-by-case, on the basis of proportionality, without automatically favouring any single value. The result must not cause ICANN or contracted parties to violate any Commitment. (Bylaws §1.2(c); FOI-HR 2019)

ICANN-Level Considerations & Gaps

Current Gaps

- No mandatory HRIA standard for accredited registrars
- Thin vs thick registry model creates uneven data exposure
- UN Cybercrime Convention (signed Dec 2024) has not yet been ratified — impact on registrars depends entirely on domestic implementation
- EU E-Evidence Regulation prioritizes speed over rights balancing; removes robust per-case assessment incentives
- No cross-transparency reporting standard
- No Authentication mechanism

What is Being Done and Can be Done

- Mandate minimum HRIA standards in Registrar Accreditation Agreements (RAA)
- Create an authentication mechanism
- Standardize LEA request formats and necessity statements across all accredited registrars
- Develop data-mapping guide: which layer holds which data (registry / registrar / reseller / host)

Risk Reduction — Who Does What

Actor	Authentication Risk	Authorization Risk	Human Rights Mitigation
ICANN	Central LEA verification mechanism	RAA doesn't require legal threshold compliance checks	**Embed HRIA standards in RAA; transparency reporting at some level**
Registry	Minimal LEA-facing systems; relies on ICANN WHOIS for redirect	Thin model limits exposure; must not disclose beyond what is held	**Publish transparency reports; adopt thin model to minimize data**
Registrar	Sniff test + callback; zero-trust approach critical	Must match legal instrument to data tier (subpoena/order/warrant)	**HRIA, notify registrant; refuse requests from human rights violating jurisdictions**

The Fundamental Tension

Law Enforcement View

"Demanding a court order for basic information and citing vague statutory timelines feels like obstruction. In time-sensitive cases, these delays mean lost evidence or a disappearing suspect."

Registrar and Civil Society View

"Legal process is not an inconvenience — it is the boundary that prevents misuse of power and shields innocent users from fraud, harassment, and political abuse."

There is no single global rulebook — only overlapping systems with incompatible assumptions.

Ad-hoc interactions and unaccountable direct disclosure serve neither public safety nor human rights. Standards should make both possible.

Authentication form — proving who is asking

Self-declared identity + independent verifiability. The RDRS performs none of this — the registrar must do it all.

Officer identity

- Full legal name
- Badge / credential number
- Title, rank, department
- Official government-domain email
- Direct callback phone number

Agency identity

- Full agency name + country
- Agency type (criminal justice / admin / regulatory)
- Official agency website for cross-check

Legislative mandate

- Statute authorising access to private data
- Does mandate cover domain registration data?
- Judicial oversight required, or administrative only?

Cross-border mechanism

- Domestic or foreign request?
- If foreign: MLAT / CLOUD Act / EIO / INTERPOL
- Central authority notification confirmed?

Verification & anti-spoofing

- Email domain matches official agency domain
- Message header inspection — no spoofing
- Independent callback to public agency number
- Portal verification (Kodex / LERS) if available
- Zero-trust: never click embedded links

⚠ *Authentication confirms WHO is asking and if they have a mandate — it does NOT confirm the request is lawful or proportionate. Authorization is a separate gate.*

Authorization form — evaluating whether to disclose

Legal instrument + data scoping + human rights assessment + disclosure decision

1 Legal instrument

- Subpoena — subscriber info only
- Court order — metadata / IP logs
- Search warrant — content data
- Prosecutor order / EIO / MLAT
- Emergency — imminent threat only

2 Data scoping

- Exact domain name(s)
- Specific data elements sought
- Date range / timeframe
- Registrar actually holds this?
- Narrow to minimum necessary

3 Necessity statement

- What alternatives were tried?
- Why is infra data needed?
- Why this layer?
- Identifier ↔ alleged offence link

4 Purpose limitation

- Stated purpose only
- No secondary use
- No onward transfer
- Retention / deletion commitment

Human rights impact assessment (HRIA)

- Jurisdiction risk — death penalty / torture / persecution?
- Proportionality — scope narrowed to minimum necessary?
- Registrant profile — journalist, activist, dissident, minority?
- Necessity — alternative investigative methods exhausted?

Disclosure decision

- Approve — full or partial data
- Deny — with written reasons
- Narrow — reduce scope & re-evaluate
- Notify registrant unless gag order

Authorization is always the registrar's sole discretion — even a perfect legal instrument does not compel disclosure. The HRIA can and should result in refusal even when all