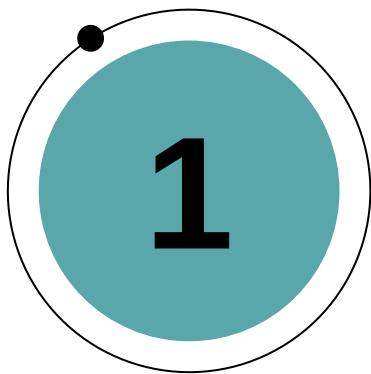


Registrars & ICANN: Perspectives on Accuracy

11 November 2024

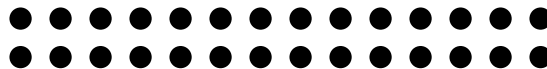
ICANN | RrSG

Registrar Stakeholder Group



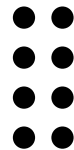
I C A N N | R r S G

Registrar Stakeholder Group

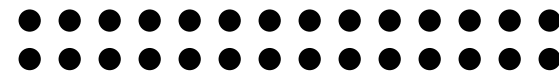


Welcome & Overview

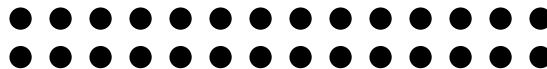
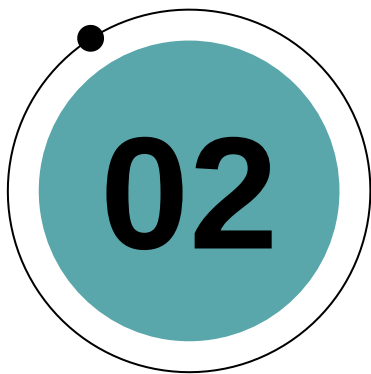
Ashley Heineman, GoDaddy, RrSG Chair



Meeting Agenda

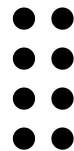


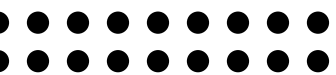
No.	Topic	Lead
1	Welcome & Overview (5 min)	Ashley Heineman, GoDaddy, RrSG Chair
2	Breakout Discussion on Accuracy Perspectives (35 min)	Sarah Wyld, Tucows, RrSG VC Policy
3	Summary of Breakout Discussion (20 min)	Ashley Heineman, GoDaddy, RrSG Chair



Breakout Discussions on Accuracy

Sarah Wyld, Tucows, RrSG VC Policy





Breakout Discussion

01

**Consider how your
group's allocated
perspective would
respond to the main
discussion questions
(10 mins)**



02

**Consider the
responses in light of
the additional
questions
(10 mins)**



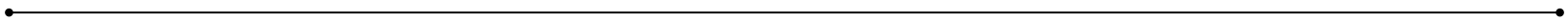
03

**Compare your
responses with those
provided
(10 mins)**



04

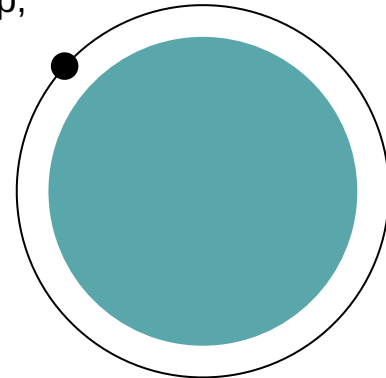
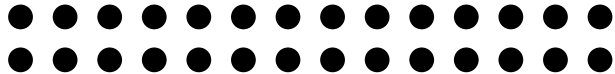
**Summarise your
discussion for group
feedback
(5 mins)**

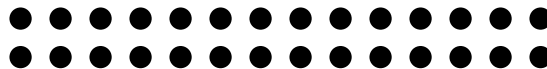
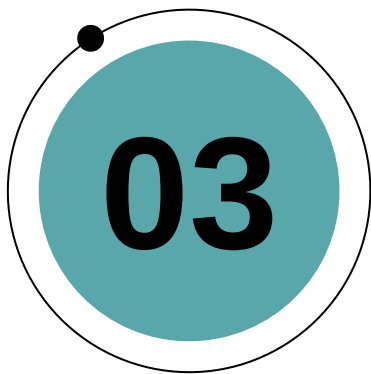




What does it mean for registration data to be accurate? What concrete effects have we seen from inaccurate data, how is it stopping legitimate things from happening? What processes should be in place to ensure data is accurate, and do those processes pose risks of their own?

- What problem is being solved?
- Does this consider costs?
- Is this necessary, proportionate, and limited?
- Does it reflect data subject rights? The experience of a normal registrant?
- Does this introduce vulnerabilities? What potential problems would come up, *e.g. risk of social engineering?*
- Is this the best way to address this problem or are there alternatives to consider?



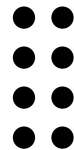


I C A N N | R r S G

Registrar Stakeholder Group

Summary of Breakout Discussions

Ashley Heineman, GoDaddy, RrSG Chair



Internet Service Provider (ISP) Perspective

What does it mean for registration data to be accurate?

- 'Reliable': meaning that they can be trusted and used without leading to errors, notably that the contact details can be used if necessary (eg emails be assumed to be delivered to the registrant) and Use of servers in the registration data does not lead to network or connection failed errors
- 'Up-to-date': meaning that changes of contact are made in a timely manner and Registrant can modify registration data at any stage

What concrete effects have we seen from inaccurate data, how is it stopping legitimate things from happening?

- "Delivery Status Notification (failed)" error messages received when emails are sent to whois Registrant Email, or calls not delivered to Registrant Phone or Fax.
- "connection failed" or "server not found" errors when registration server details are not accurate
- When dealing with cybersecurity issues, anything that stands in the way of identifying the source is a problem, including inaccurate domain name whois data – requests for such identification may be internal to ISPs or may be requested to ISPs by law enforcement agencies

What processes should be in place to ensure data is accurate? Do those processes pose risks of their own?

- Enforce RAA provisions on accuracy (eg 3.7.7.2, 3.7.8 etc) and more generally the RDDS Accuracy Program Specification
- Validate data at registration, check accuracy at registration renewal, with a risk of administrative overhead
- Conduct technical checks and consider coercive measure such as suspension, if necessary
- Consider stronger registrar/registry coordinated effort?
- Promote 'KYC (Know Your customer)' on every renewal

Business Perspective

What does it mean for registration data to be accurate?

- To be a precise representation of the contact details for the beneficial registrant of a domain name (e.g., not privacy / proxy data).
- Syntactical accuracy is not accuracy. Anyone can use any working email address and phone number. That doesn't necessarily mean it's the real registrant behind it.

What concrete effects have we seen from inaccurate data? How is it stopping legitimate things from happening?

- It's not that it's necessarily stopping legitimate things from happening. It's that it helps illegitimate things continue to happen (e.g., hiding behind inaccurate data – sometimes hundreds of names at once – to launch a phishing attack).
- The more anonymous a registrant can be, the more room there is to operate in the dark. If no one can find you, you can phish, distribute malware, steal intellectual property, install botnets, etc. And you can do it at scale. Accurate and available data prevents wild goose chases.
- Inaccurate data hinders legitimate investigations and research and often involves identity theft and innocent parties.

What processes should be in place to ensure data is accurate? Do those processes pose risks of their own?

- A reasonable verification procedure can be employed, like those a) already in use in EU ccTLDs, and b) presented during the ALAC's outreach on accuracy at ICANN79 in San Juan.
 - This will marginally increase registration costs, but will help reduce the hundreds of millions in impact DNS abuse has on businesses and consumers.
- The risk-based verification idea posed by the Article 28 Coordination Group is a good start.



Security Perspective

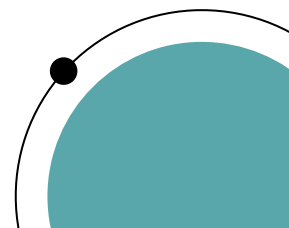
What does it mean for registration data to be accurate?

- The Data provided is sufficient to carry out the purpose it was provided (i.e. to contact the registrant) - For us the main reason for contact is the notification of compromised hosts/sites

What concrete effects have we seen from inaccurate data, how is it stopping legitimate things from happening?

- Registrant data is not readily used in our day-to-day abuse management process, barring its use for escalations to registrants, on behalf of our registrar clients
- Registrant data is generally not part of our review process, as there are far more reliable and useful indicators of abuse
- To add a stricter accuracy requirement would be unlikely to have a marked impact on the work we already do.

What processes should be in place to ensure data is accurate? Do those processes pose risks of their own?

- The use of the data is to ensure contact with the registrant. Current verification procedures achieve this level of accuracy.
 - An improvement could be on ensuring that email AND at least 1 other contact should be subject to the current verification procedures (email AND Phone, or email AND address), to ensure contingency, should one of the means to communicate fails.
 - This would ensure better escalations, and help decrease potential TTL of abuse where a form of compromise of the infrastructure attached to the domain, has been identified.
- 



Law Enforcement Perspective

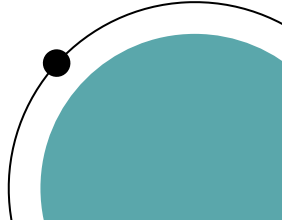
What does it mean for registration data to be accurate?

- Reflects the true details of the end beneficiary of a domain's registration.
- Clearly distinguishes all entities involved (e.g., resellers, proxies).
- Uniquely identifies entities with sufficient information (e.g., ID number, physical address).

What concrete effects have we seen from inaccurate data, how is it stopping legitimate things from happening?

- Delays or misroutes communication for public safety officials.
- May reveal sensitive investigation information to unrelated individuals.
- Hinders investigations into illegal activities (e.g., online CSAM dissemination).

What processes should be in place to ensure data is accurate? Do those processes pose risks of their own?

- Clearly distinguish roles of entities in registration data.
 - Conduct periodic reviews to match reality.
 - Use KYC practices for high-risk registrations.
 - Require live photographs of ID documents for verification.
- 

Registrant Perspective

What does it mean for registration data to be accurate?

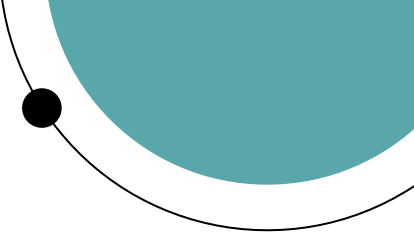
- Defined based on applicable laws and policies, with ICANN policies taking into account that country laws differ
- Takes into consideration that mistakes happen in formatting and inserting the data
- Does not require authentication and identification of the domain name registrant, per ICANN rules
- Is only for the domain name lifecycle: for registrations, its technical administration, and its renewal (or transfer).
- Should be limited to the ICANN purposes of processing WHOIS data, to facilitate “contactability” of the registrant by the registrar. It is not about identification or authentication of the registrant.

What concrete effects have we seen from inaccurate data, how is it stopping legitimate things from happening?

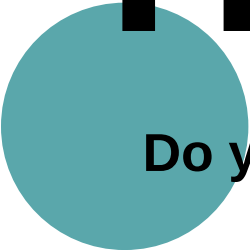
- Counter to stopping things, use of pseudonyms has been essential to sharing ideas that pursue fundamental societal and human rights in places where use of their real name may result in prosecution, persecution, and threats to their or their family/friend's lives. Pseudonyms are protected by law in many countries

What processes should be in place to ensure data is accurate? Do those processes pose risks of their own?

- Should use existing processes. Having more in place *creates risks*:
 - Unfair suspension of the domain name and loss of key websites
 - Furthering the digital divide by penalising those who do not have a working phone number or email address or have cell connectivity issues
 - Simple mistyping becoming a fatal error to a domain name and its associated websites, emails and listservs
 - High resource costs for registrars leading to operation issues for smaller registrars and increased domain costs
 - Conflict with data protection laws



Thanks!



Do you have any questions?

secretariat@icannregistrars.org

www.rrsg.org

