ICANN | RrSG

Registrar Stakeholder Group

RySG

gTLD Registries Stakeholder Group

Practical Insights on Data Disclosure from Contracted Parties

22 September 2020

Agenda

Time (UTC)	Topic	Discussion Leader
14:00 - 14:05	Welcome	Owen Smigelski, NameCheap, Inc.
14:05 - 14:20	Background - The Impact of GDPR	Alan Woods, Donuts Inc.
14:20 - 14:40	By the Numbers	Sarah Wyld, Tucows Inc.
14:40 - 15:00	Request and Response Process	Beth Bacon, PIR
15:00 - 15:30	Q&A	Owen Smigelski, NameCheap, Inc.

Background - Impact of GDPR:

Summary:

- History of data protection
- How data protection now applies to the DNS?
- Pre GDPR WHOIS
- Post GDPR - Temporary Specification and the task of the EPDP

Key Considerations:

- Why was Data Protection necessary?
- What is it ‘protecting’?
- When did it all begin?
- Why the DNS needed to change?
- What was our actual goal and was that achieved?

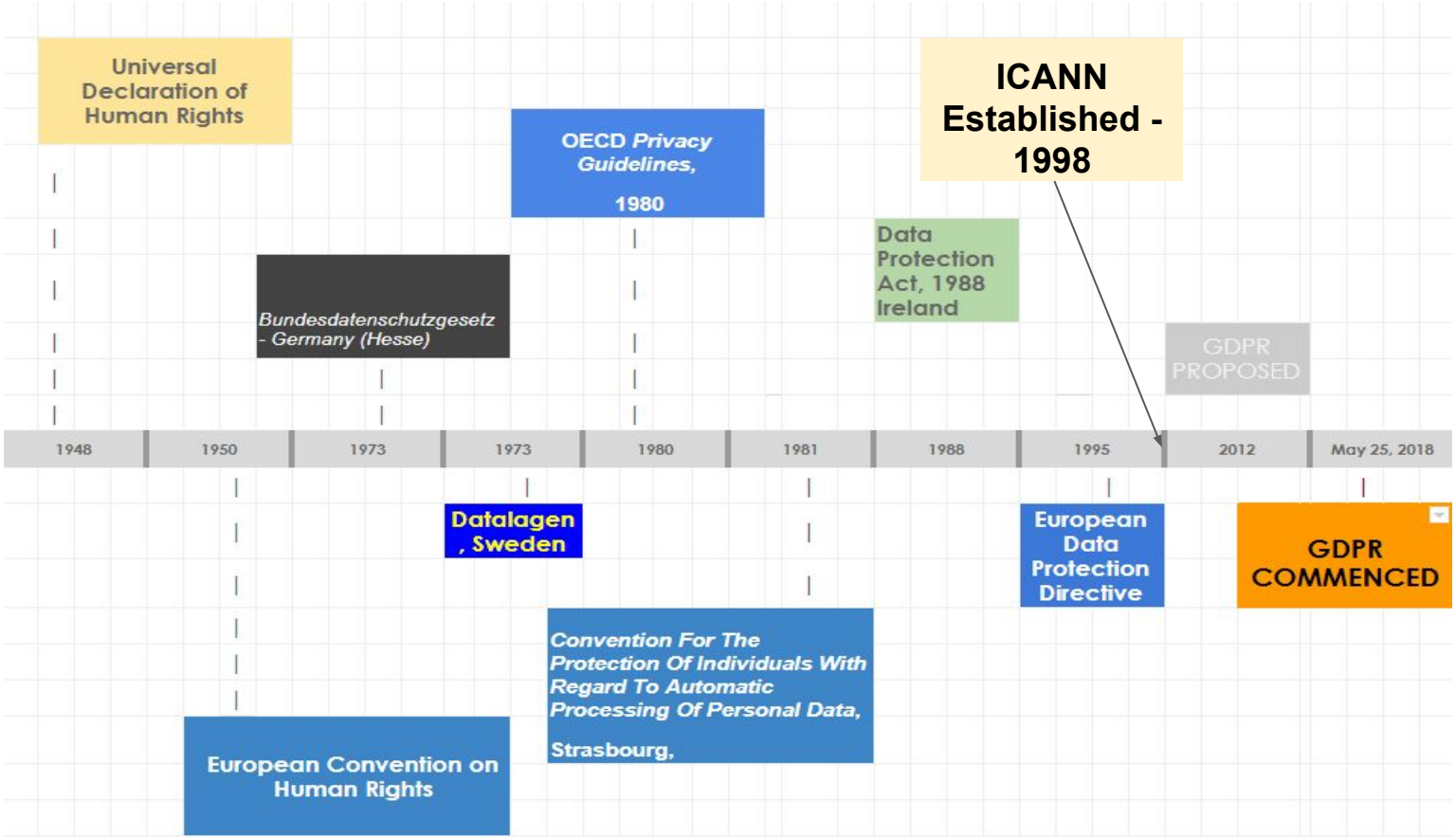
Data Protection - A very abridged history

- The roots of data protection are traced to the end of World War II.

- The concept of personal privacy was as a direct reaction to the use of personal information to specifically profile and target numerous groups by state and other actors.

> **No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.**

Article 12, Universal Declaration of Human Rights, 1948


Universal Declaration of Human Rights
OECD Privacy Guidelines, 1980
ICANN Established - 1998
Data Protection Act, 1988 Ireland
Bundesdatenschutzgesetz - Germany (Hesse)
GDPR PROPOSED
1948
1950
1973
1973
1980
1981
1988
1995
2012
May 25, 2018
Datalagen , Sweden
European Data Protection Directive
GDPR COMMENCED
Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, Strasbourg,
European Convention on Human Rights

Data Protection Principles

There are 7 principles that represent the basis of all European data protection laws and all should be read with the Data Subject as the intended beneficiary of the protection

- Lawfulness, **fairness** and **transparency**.
- **Purpose** limitation.
- Data minimisation.
- **Accuracy**.
- Storage limitation.
- **Integrity** and **confidentiality** (**security**)
- **Accountability**.

These core principles were asserted in 1980 in the OECD guidelines, and were the basis of the 1995 Data Protection Directive and remain the core concept of the GDPR today.

WHOIS - Pre GDPR

- No formally established purpose for data publication - **no transparency or minimization**
- Freely published personal data of all registrants - **no purpose limitation**
- Data scraping, repackaging and resale of registrant data. - **No access / storage limitations**
- Inability to limit the use of the publicly available data - **No use limitations , no purpose limitations and a very clear lack of data integrity and confidentiality**
- Inability to apply and complete data subject requests no accountability - **failure to vindicate the rights of the data subjects**

All these issues existed before the GDPR!

"WP29 wishes to stress that the unlimited publication of personal data of individual domain name holders raises serious concerns regarding the lawfulness of such practice under the current European Data Protection directive (95/46/EC)" (letter WP29 - ICANN - December 2017)

Temporary Specification

- Top down effort to apply the requirements of the GDPR. ICANN drafted the 'Temporary Specification' to permit the Contracted parties to modify the means of processing of data.
- Most notably, put a hold on the publication of data ('***going dark***') via WHOIS.
- Under GNSO / ICANN bylaws, the Expedited Policy Development Process (ePDP) was formed and tasked the community to affirming (with or without necessary changes), or reject the Temporary Specification within 12 months.
- Many saw this as an opportunity to finally bring the data processing at ICANN in line with legislative requirements, others took an alternative approach and sought to 'justify' the way things were or the '**Status Quo**'.

WHOIS 'going dark' - the term coined by those who had relied on 'open publication' of the WHOIS and who no longer had unlimited use of, or the ability to scrape and repackage registrant data, for their own undisclosed purposes, without limitations imposed by the controller..

Status Quo - a term created to describe the state that WHOIS was in prior to the temporary specification 'before WHOIS 'going dark'- the return to which (or as close as possible) was the stated goal for the outcome for the EPDP for many.

WHOIS - Post GDPR / Post ePDP

- Established and explained the basic legal purposes for the collection of registration data and considered ‘necessity’ and ‘minimization’ i.e. what was the least amount of data necessary to achieve the purposes as stated. ***[ePDP phase 1 - Rec 1]***
- Ceased the publication of personal data in WHOIS (and RDAP) ***[ePDP phase 1 -Rec 5]***
- Prevented widespread mass data scraping, repackaging and resale of registrant data.
    - Note the US courts recently affirmed that such data scraping and repackaging was contrary to the terms of and conditions (i.e. purpose) of WHOIS (See.NZ case). Replicated across the majority of operators.
- Established a means by which requests for disclosure may be legally processed ***[ePDP phase 1-Rec 3, Re 18 and ePDP Phase II].***
    - Emphasis placed on due process. Involved parties must ensuring proper consideration of rights of the data subject.This recognizes that ‘disclosure’ is only possible where requesters establish necessity. The Controller must measure that necessity against the rights of the data subject..

Takeaways

- **The GDPR was not new** - the law changed very little in substance but the community finally took note, as it hugely increased liability and had massive implications for enforcement.
- **WHOIS never went 'Dark'** - if anything it came into the light for the first time ever.
- The **'Status Quo'** is a poor goal and should never have been considered a 'target outcome'. It represented a state of being where laws regarding the privacy rights of registrants were routinely ignored.
- **Data Protection / GDPR / CCPA confers rights to Data Subjects -** it does NOT provide a right to any 3rd party to access that data, nor does it create any obligation to disclose that data to them.

The ICANN Community, have gone to huge lengths support the legal disclosure of data, to enable disclosure to those persons and entities who present a valid legal basis and a sound purpose for such disclosure, with due regard to both necessity and data minimization.

By The Numbers

Summary:

- Rates of requests and responses
- Rates of disclosures and denials
- Categories of requestors
- Rate of unique vs. repeat requestors

Key Considerations:

- When requests are approved, what data is disclosed?
- Are requestors satisfied with responses?
- How long is the typical processing time?
- What do these numbers tell us about the effect of public data availability on abuse rates?

Request Rates

Summary:

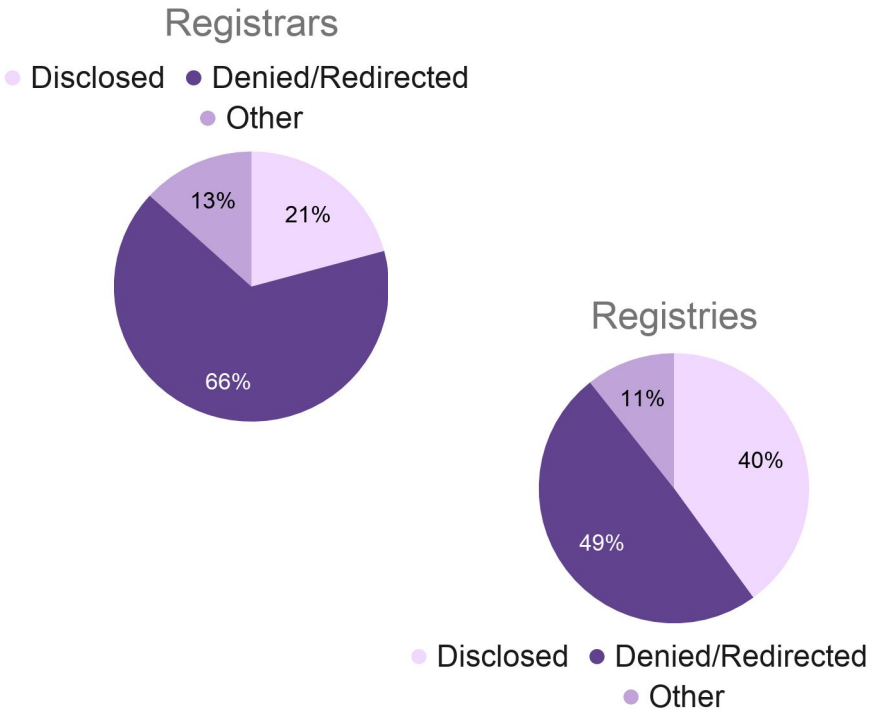
- Registrars reported as few as 30 and as many as 3400 requests*
- Registries reported as few as 80 and as many as 300 requests*
- All responders found an increase in request rates from 2018 to 2019, then level off for 2020 so far

*May 2018-Aug 2020

Key Takeaways:

- Overall <1% of total domains under management are subject to disclosure requests
- Rates vary significantly due to different redaction rules and when redaction was applied (later = fewer requests)

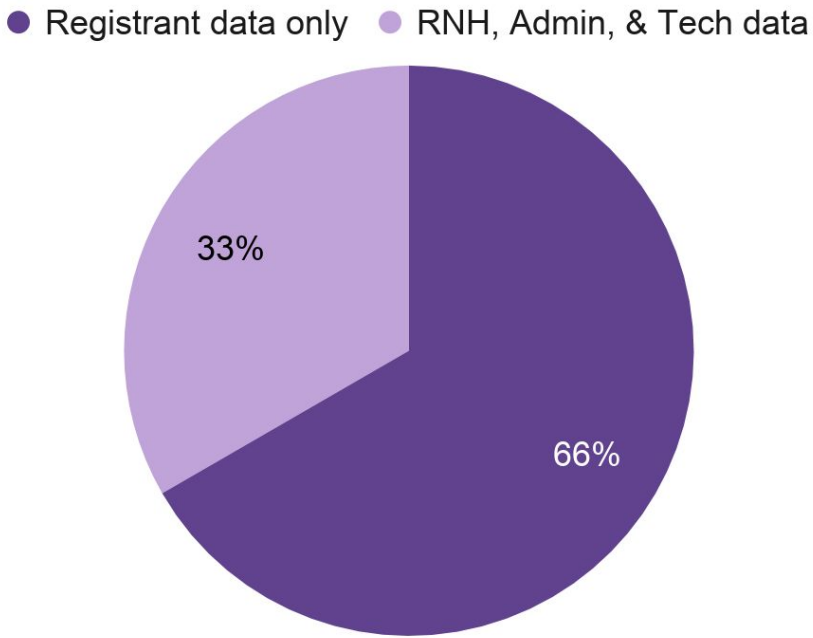
Outcome Rates



Key Takeaways:

- "Denied or redirected"
  - Directed to another party (e.g. registry to registrar)
  - Lawful basis not demonstrated
- "Other"
  - Partial data disclosed
  - P/P service
  - Incomplete request
  - Data not redacted
  - Domain not registered/not with that provider

What Data is Provided?



Key Takeaways:

- When data is not disclosed, standard practice is to provide the rationale and suggested next steps
- When Privacy/Proxy services are enabled, standard practice is not to reveal the underlying data, but to give the P/P service contact method
- Security methods for data disclosure vary among contracted parties

Appeals

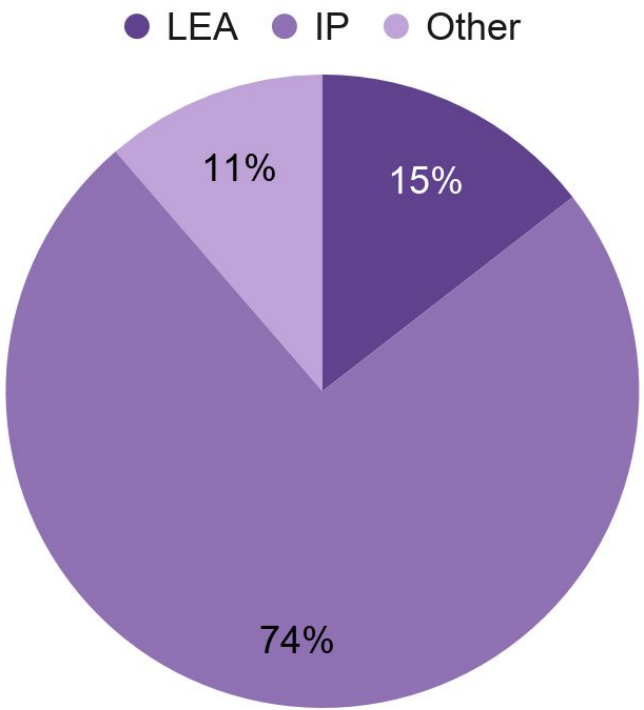
Summary:

- Most respondents to our survey have received no appeals
- Registrars with appeals reported volume between 0.1% and 5% (of total requests)
- Registries reported 0% appeal volume

Key Takeaways:

- Appeals often relate to requests that came in via the wrong channel or where other mechanisms are more appropriate; educational outreach will help with this
- Appeals re denials due to lack of legal basis were resolved through discussion with Legal team and no disclosure

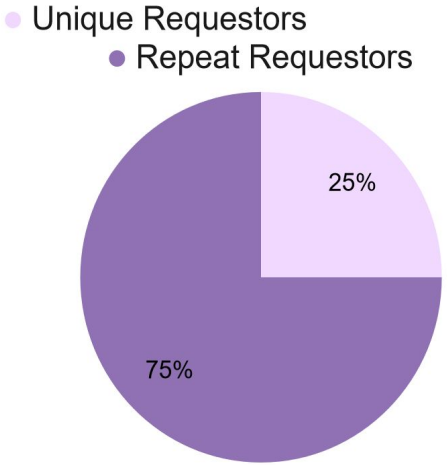
Requests by Requestor Type

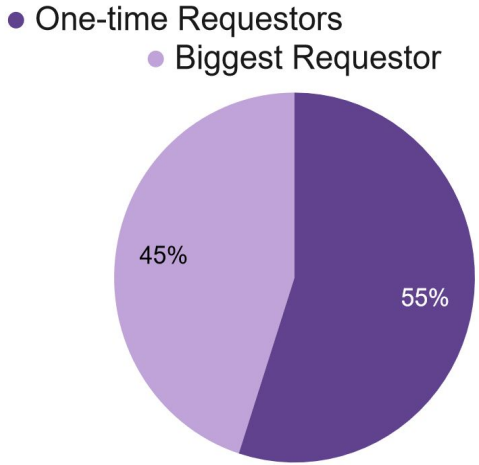


Key Takeaways:

- Majority of requests are related to IP
- “Other” includes:
  - security research
  - requests to contact domain owner
  - requests with no domain included
  - requests for domains not with that registry/registrar

Unique vs Repeat Requestors





Key Takeaways:

- Typical ratio of 1 requestor for every 4 requests
- One specific requestor is the source of 45% of requests, a significant portion of the total request volume

Average Response Time (Days)

Key Takeaways:

- Typical response time is < 3 days
- Registry response is time slightly faster (⅓ of a day less)
  - Registries send most requests to registrar instead of disclosing data directly, so the process is faster

Insights

Benefits to Redacting Data

- Publicly-available data was a major attack vector
  - Without this info, social engineering & similar methods are more difficult
- Abuse stats show significant decline following redaction of data, suggesting this data was being used for abuse purposes

Other Considerations re Abuse

- A single domain could have any number of subdomains being used for abuse
  - Working with the hosting provider is often necessary
- Enhanced CP & ICANN tracking for COVID-19 abuse indicated no increase

Request and Response Process

- **Requestor**
  - Data Subjects
  - Law Enforcement
  - Third-Party
- **Legal Basis**
  - For the disclosure
- **Jurisdiction**
  - Requestor
  - Controller
- **Type of Request**
  - Domain name is infringing third-party rights
  - Content is infringing third-party rights
  - Content or service is unlawful
  - DNS Security

Required Information for Requests

There are requirements outlined in the EPDP Phase 2 Final Report as well as best practices outlined in the Registrar and Registry Minimum Required Information for WHOIS Data Requests.

Required Information:

- Domain name
- Identification of and information about the Requestor
- Legal rights of the Requestor and legitimate interest or other lawful basis and/or justification for the request (purpose)
- Affirmation that the request is being made in good faith and that data received will be processed lawfully and only in accordance with the purpose specified
- A list of data elements requested and why the are necessary for the purpose of the request
- Request type

Request Review Process

ICANN | RrSG

Registrar Stakeholder Group

RySG

gTLD Registries Stakeholder Group

Q & A