ICANN 69

VIRTUAL ANNUAL GENERAL

Thank You to our Sponsors!

WHOIS Changes Under GDPR: Impact to End-Users and Public Safety

ICANN69 Plenary Session

Wednesday, 21 October 2020
10:30-12:00 CEST

Opening Remarks

Jonathan Zuck (ALAC)
Moderator

Introductions

Participant	Perspective	Affiliation
Jonathan Zuck	Moderator	At-Large Advisory Committee (ALAC)
Laureen Kapin	Law Enforcement	Federal Trade Commission (US)
Gabriel Andrews	Law Enforcement	Federal Bureau of Investigation (US)
Greg Aaron	Cybersecurity Research	Interisle Consulting Group
Lyman Chapin	Cybersecurity Research	Interisle Consulting Group
Mark Svancarek	Corporate Fraud Prevention	Microsoft
Milton Mueller	Noncommercial Registrant	Noncommercial Stakeholder Group (NCSG)
Owen Smigelski	Contracted Parties	Registrar Stakeholder Group (RrSG)

Program

1.	Opening Remarks and Introductions	Jonathan Zuck	5 minutes
2.	Perspectives		
	a. Law Enforcement	Laureen Kapin and Gabriel Andrews	10 minutes
	b. Cybersecurity Research	Greg Aaron and Lyman Chapin	10 minutes
	c. Corporate Fraud Prevention	Mark Svancarek	10 minutes
	d. Noncommercial Registrant	Milton Mueller	10 minutes
	e. Contracted Parties	Owen Smigelski	10 minutes
3.	Discussion	All	30 minutes
4.	Closing Remarks	Jonathan Zuck	5 minutes

Law Enforcement

Lauren Kapin (FTC)
Gabriel Andrews (FBI)

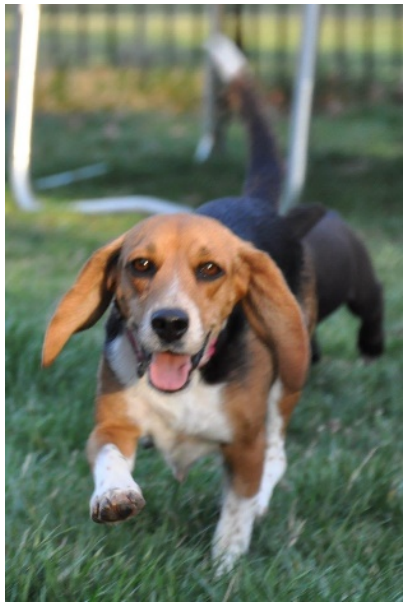
WHOIS Post-GDPR: Impact on the Public

Laureen Kapin

Counsel for International Consumer Protection,
U.S. Federal Trade Commission
Co-Chair, GAC Public Safety Working Group

How the Public Uses WHOIS

Complaint Types

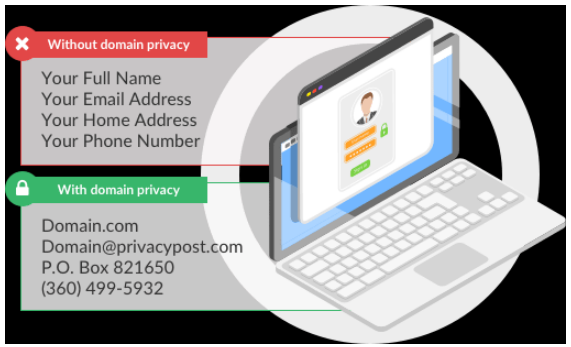


Complaint Types

Impact of GDPR on Law Enforcement Investigations

CCPA

Privacy/Proxy Services



Impact of GDPR on Law Enforcement Investigations

For Law Enforcement purposes, ideal DNS checks are Timely & Accurate.

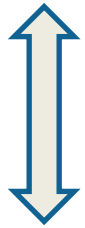
93.184.216.34

2606:2800:220:1:248:1893:25c8:1946

www.example.com

?

10 seconds

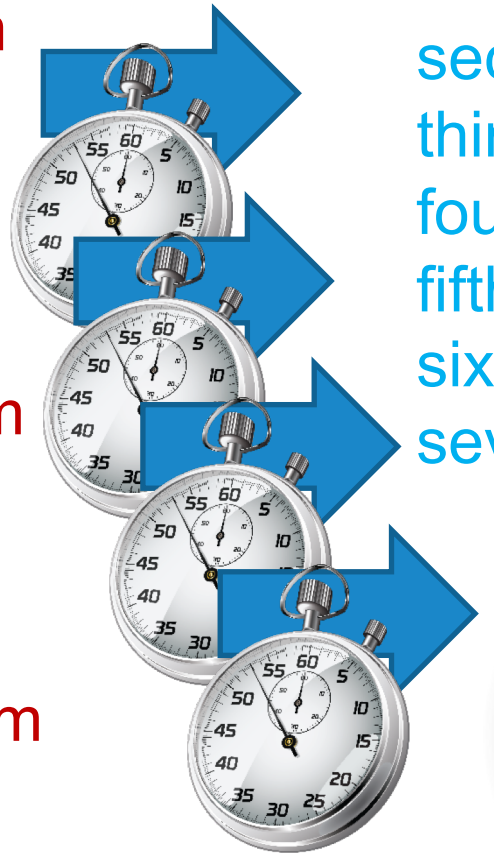


6 months

Impact of GDPR on Victim Notifications

ceo@exanple.com

exanple.com
secondexanple.com
thirdexanple.com
fourthexanple.com
fifthexanple.com
sixthexanple.com
seventhexanple.com
eigthexanple.com
ninthexanple.com
tenthexanple.com
eleventhexanple.com



secondexample.com
thirdexample.com
fourthexample.com
fifthexample.com
sixthexample.com
seve…

Cybersecurity Research

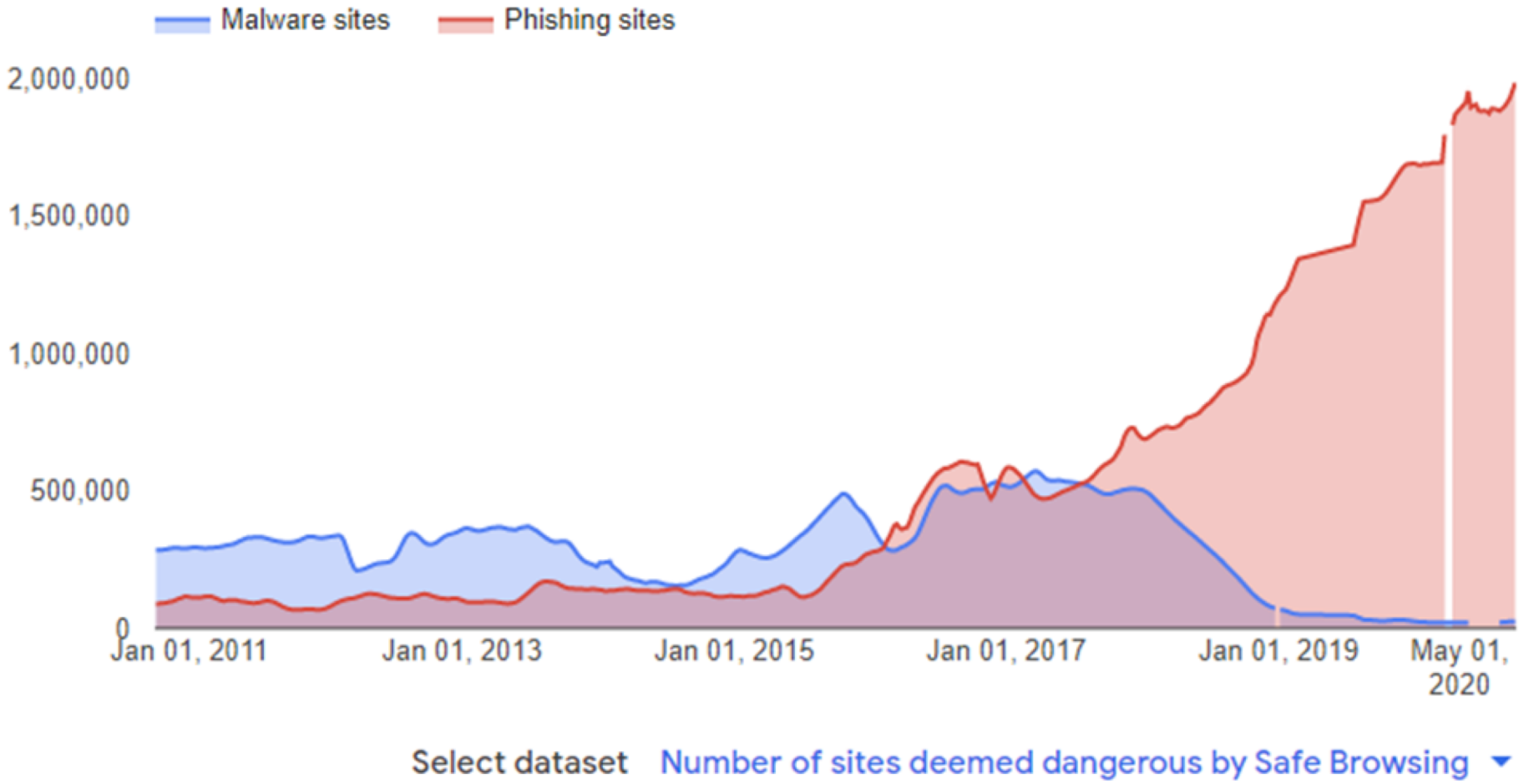
Greg Aaron and Lyman Chapin (Interisle Consulting Group)

Phishing Landscape 2020

http://www.interisle.net/PhishingLandscape2020.html

- 298,012 phishing URLs, on 99,412 domain names
- Phishing is highly concentrated at certain domain registrars, hosting providers, TLDs.
- Most domains used for phishing are used with 14 days of creation.
- Phishing is a bigger problem than is reported. We can establish a floor. We don't know the ceiling.
- Detection and blocklisting of phishing domain is impacted by several factors. Lack of WHOIS data is one of those factors.

Is phishing going up or down?



Source: Google Safe Browsing Transparency Report
https://transparencyreport.google.com/safe-browsing/overview

Fighting Phishing: Need WHOIS for:

Need public, non-sensitive data:

- Registrar
- domain creation date

***Problem*: rate-limiting**

- Prevents WHOIS users from getting even the basic, non-sensitive data
- See SAC101

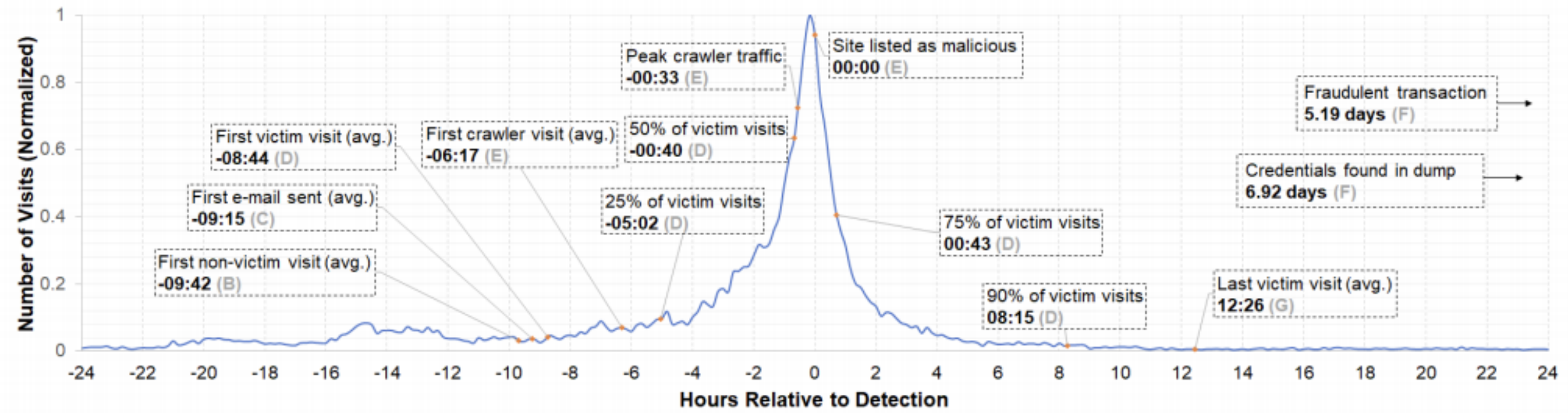
Need to evaluate registrant

- Is the registrant an innocent party, or a phisher?
- Bogus contact data is a sign of bad faith

***Problem:* most contact data now usually redacted, as allowed by ICANN policy**

Phishing attacks last ~17 hours

By the time they are detected, most of the victimization has already taken place.



A. Oest, P. Zhang, B. Wardman, E. Nunes, et al: "Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale." Proceedings of the 29th USENIX Security Symposium, August 12–14, 2020. https://www.usenix.org/system/files/sec20-oest-sunrise.pdf

About 60% of domains used in phishing attacks are registered by the phishers

We found **60,935** maliciously registered phishing domains, newly used in a three-month period.

The COMAR project from SIDN (.NL) and AFNIC (.FR) estimated it's 57%.

Maroofi, M. Korczynski, C. Hesselman, B. Ampeau, A. Dud, "COMAR: Classification of Compromised versus Maliciously Registered Domains." 2020 IEEE European Symposium on Security and Privacy (EuroS&P). http://mkorczynski.com/COMAR_2020_IEEEEuroSP.pdf and https://comar-project.univ-grenoble-alpes.fr/

Conclusions

The registrars and registry operators have the contact data. They must use it better, to suspend those malicious registrations.

EPDP says registries and registrars can fulfill cybersecurity data requests in five (5) days. (And then within *ten* days.) *That timeline will be ineffective for dealing with cybercrime.*

Phishing is an excellent candidate for automation in SSAD, for quick turn-around.

http://www.interisle.net/PhishingLandscape2020.html

Corporate Fraud Prevention

Mark Svancarek (Microsoft)

Noncommercial Registrant

Milton Mueller (NCSG)

Registrants have an interest in and a legal right to redacted PII

- Criminals and abusers can misuse open PII
- Not a good idea to make your email and physical address available randomly to anyone and everyone on the Internet
- Name of registrant, country and state still there
- New, efficient methods to disclose redacted data (SSAD)

No discernable impact on cybersecurity

	May 2008	Dec 2015	May 2018	Oct 2020	17 months before GDPR	17 months after GDPR
Malware	241,761	408,339	335,361	24,667	-18%	-93%
Phishing	54,760	268,086	771,319	2,010,143	188%	161%

Source: Google Transparency Report, Google Safe Browsing: "Number of dangerous sites"

The SSAD

- Centralized and standardized method for disclosure requests
- Compliant with GDPR

Contracted Parties

Owen Smigelski (RrSG)

Practical Insights on Data Disclosure from Contracted Parties

22 September 2020

RySG gTLD Registries Stakeholder Group

ICANN | RrSG Registrar Stakeholder Group

Presentation and recordings on GNSO Calendar

https://gnso.icann.org/en/group-activities/calendar

Data Protection – over 70 years of 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 honor 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***

- World's first national data protection law: Sweden (1973), with dozens more laws/treaties in Europe before creation of ICANN (1998)

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 minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Pre-GDPR, unrestricted access to registration data via WHOIS violated many of these principles.

Overview

- **The GDPR was not new** – did not change much substantively but did increase liability
- **WHOIS never went 'Dark'** – it now complies with the law
- **WHOIS data is not the best route to stop abuse** – report it to contracted parties and hosting providers. Reports and presentations do nothing to fix the problem.
- **Data Protection / GDPR / CCPA confers rights to Data Subjects -** it does NOT provide a right to any third party to access that data, nor does it create any obligation to disclose that data to them.
- **Unredacted WHOIS data provided attack vectors** for domain hijacking, spam, phishing, etc.
- Per ICANN data, **overall abuse using domain names is decreasing**, and there was no increase in abuse levels during COVID-19 pandemic

Required Information for Requests

There are requirements outlined in the EPDP Phase 2 Final Report as well as best practices detailed in the Registrar and Registry Minimum Required Information for WHOIS Data Requests (available at www.rrsg.org/whois)

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 Rates

Summary:

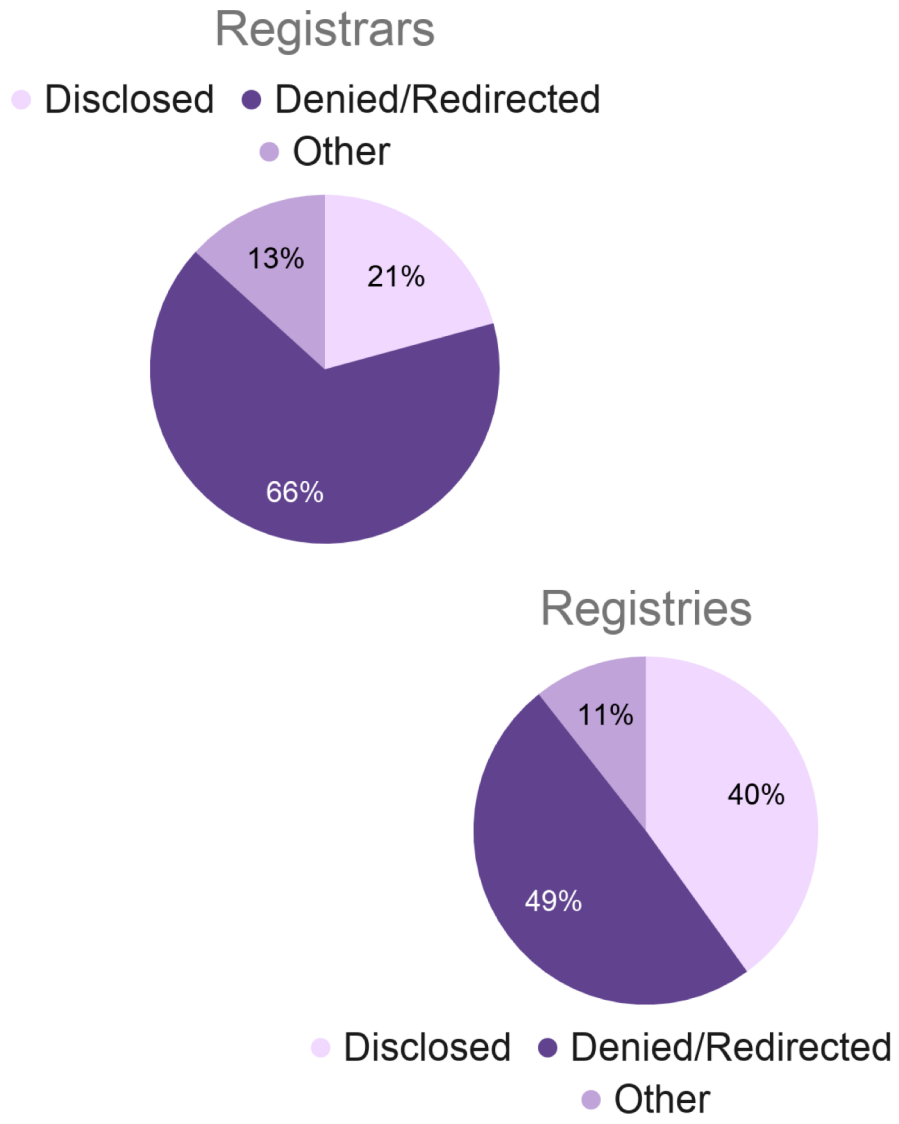
- Registrars reported as few as 30 and as many as 3400 requests*
- Registries reported as few as 80 and as many as 300 requests*
- All responders found an increase in request rates from 2018 to 2019, then level off for 2020 so far

*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)
- More metrics will be available with SSAD

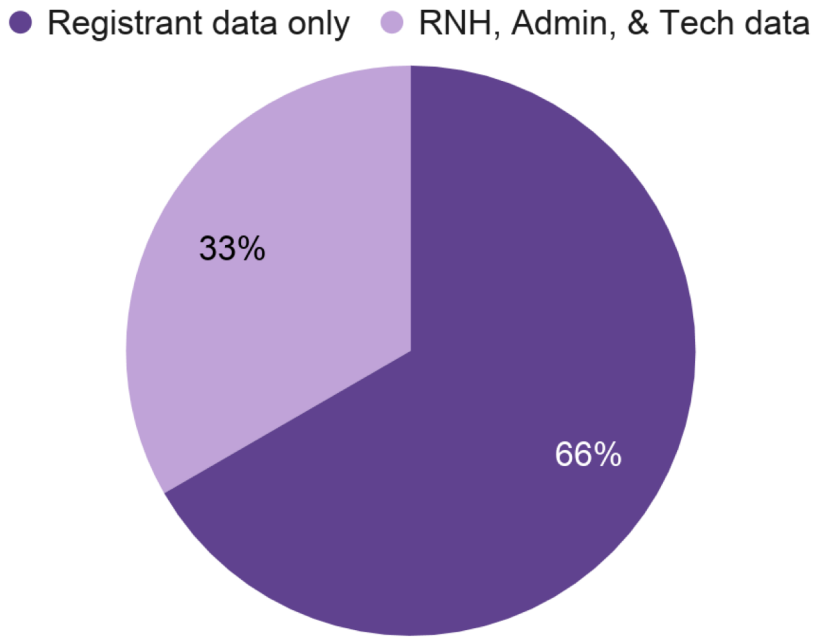
Outcome Rates



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

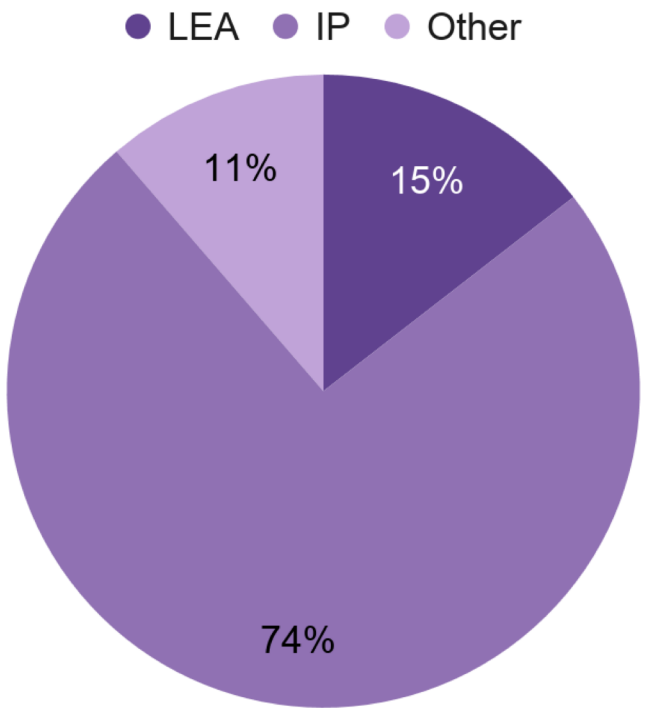
Summary:

- Most respondents to the 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

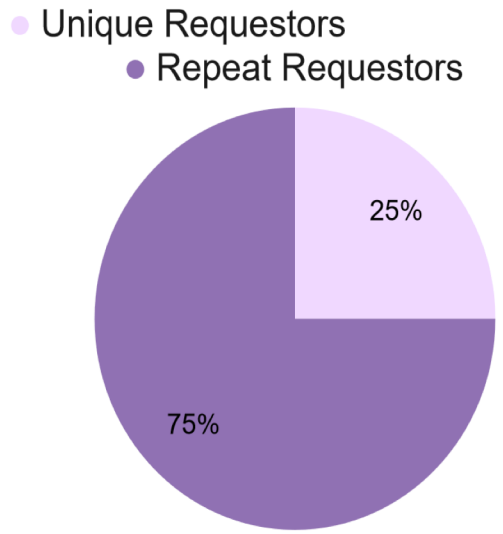
Requests by Requestor Type

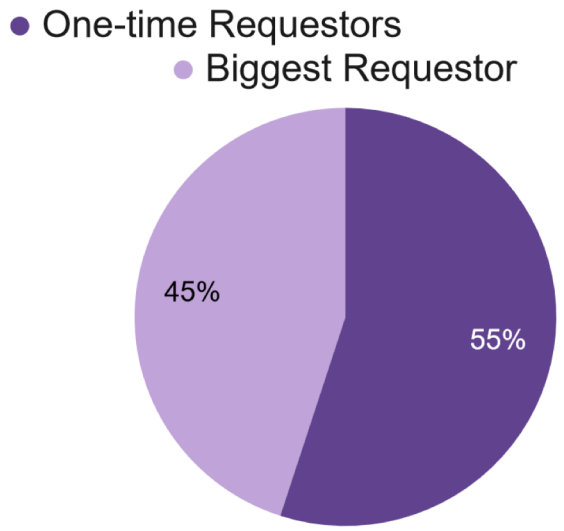


Key Takeaways:

- 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

Discussion

Jonathan Zuck (ALAC)
Moderator

Closing Remarks

Jonathan Zuck (ALAC)
Moderator

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann