

GROUP ONE

Steve Crocker



# Welcome to the Webinar

6 February 2025

Steve Crocker,  
[info@edgemoorresearch.org](mailto:info@edgemoorresearch.org)

Edgemoor Research Institute





# Goals for this Webinar



1. What the stakeholders need/desire.
2. Criteria for measuring effectiveness and efficiency.

Requestors, Data Holders, Governments, and Privacy Advocates will likely each have their own criteria

2<sup>nd</sup> webinar will use results from this webinar plus ideas we've been working on.

Rod Rasmussen

# Cybersecurity Perspective

- Real-time Access a.k.a. Incident Response
  - Help determine real vs. malicious
  - Contact responsible parties for compromised services tied to domain
  - Linking of evidence/exposure of clues for current incident
- Analysis
  - Identifying patterns of abuse
  - Building fact-based reputation scores
  - Linking of data elements: evidence/clues for campaigns and threat actors
- Cybersecurity community members are trusted entities
  - Routinely closely-hold highly sensitive data under strict guidelines/agreements

**Gabriel Andrews**

# Why do Public Safety Agencies care about Domain Name Data?

**Investigations**

Contacting Victims

**E.g., if a domain is used in phishing...**



Was that domain registered by the bad guy?

Which legit business did the bad guy talk to?

The registrar? A proxy? A reseller?

Where?

I.e., which LEA has jurisdiction there?



# Why do Public Safety Agencies care about Domain Name Data?


Investigations

**Contacting Victims**



**E.g., if the domain the bad guy used in phishing was...**

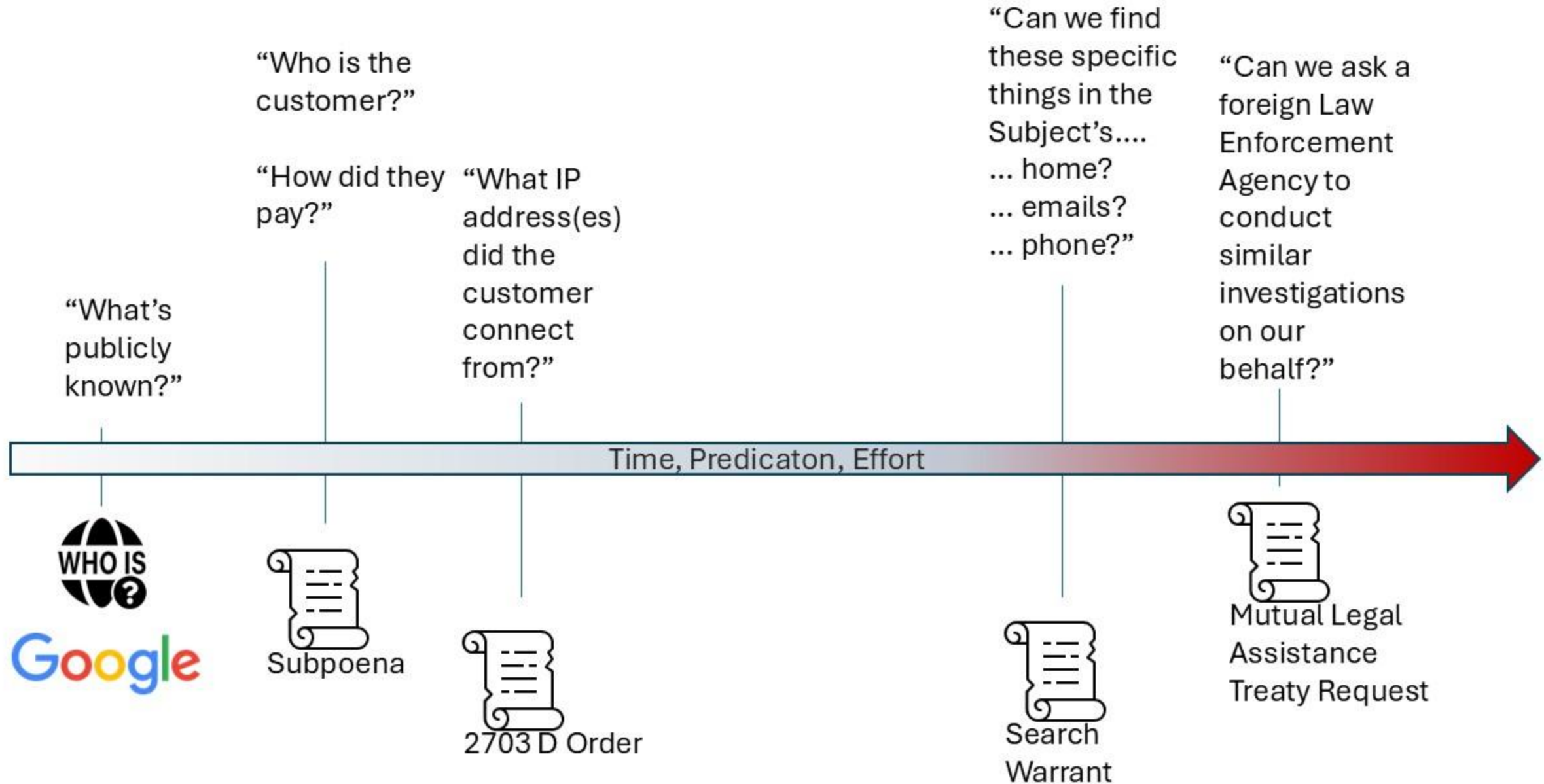
innocentvictim.com 

then WHOIS innocentvictim.com, 

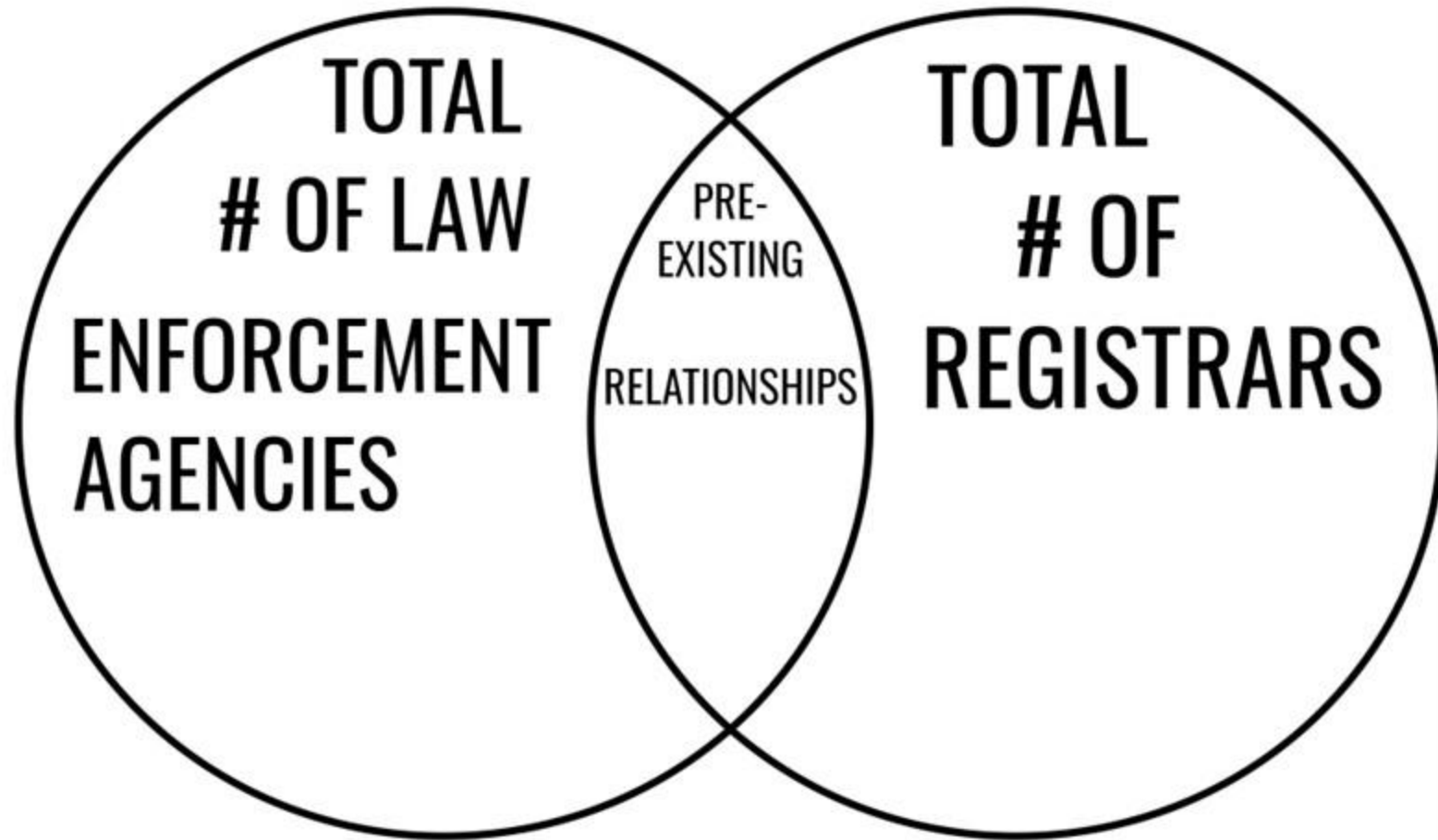
where are they? What's their phone #?

**Can we notify them in time to prevent harm?**

# Tools like WHOIS are foundational. LE tools build upon them.



**Ad hoc relationships are the status quo.  
We can do better.**



**Ignas Anfalovas**

# Challenges faced by IPXO



## IPXO: IP Solutions platform

- We use IP WHOIS to read and update the attributes of IP range

## Challenges we face:

- Different WHOIS data structures across RIRs and NIRs
- Each WHOIS automation that we do needs to be adapted to different RIRs and NIRs

## Our interest here:

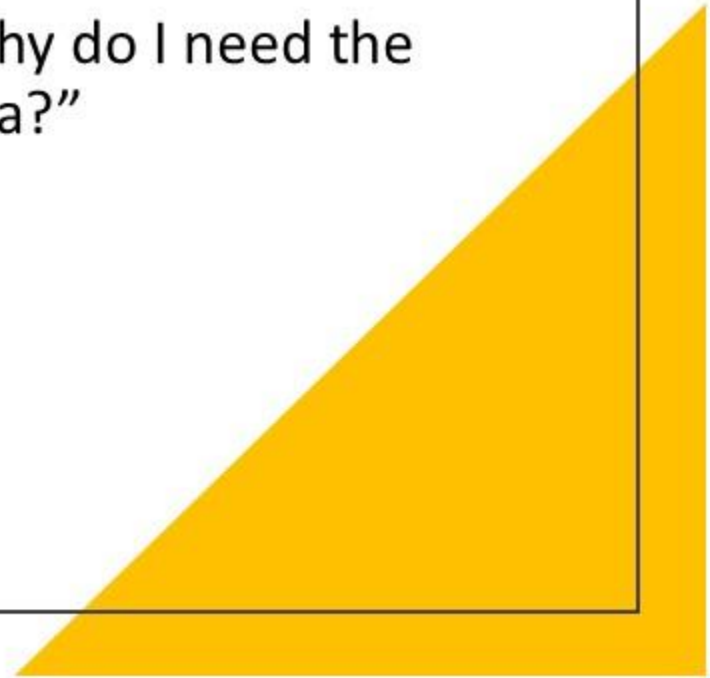
- To have a RIR and NIR data structure unifying framework

**John McElwaine**


Whose data  
is it  
anyway?

or


“Why do I need the  
data?”







Why do I  
need access  
to Domain  
Name  
Registration  
Data?



Investigation and Remediation of *civil*  
legal issues, such as:

- Trademark infringement or impersonation of brands;
- Copyright infringement or theft of authorship;
- Domain name acquisitions;
- Due diligence related to the acquisition of business with an online presence;
- Determining the date that a website or content on a website launched.



**Jothan Frakes**

# Inconvenient Difference in Perspective

## **Requestor** (LEA/Researcher/Spammer/IP)

- Are relitigating MSM-vetted matters (and thus eroding MSM) with repeat requests for same thing
- Assume access is, was and should always be free like before balancing tests needed
- Varying Purpose (good/evil)
- Zero relationship/agency w Registrant
- Volume/Result focused action
- Zero consequence for false positive effect on registrant (“acceptable losses”)
- Low/no accountability for privacy violation
- Often build for-profit services upon the data and sell it to 3<sup>rd</sup> parties
- Automated cease-and-desist notices or predictive algorithms to determine intent of registration

## **Holder** (Reseller/Registrar/Registry)

- Shared dissatisfaction, but instead, are following MSM in good faith
- Pay for Servers, Bandwidth, legal balance review and other cost burdens to meet SLAs
- Specific Purpose (Domain Registration)
- Direct (Customer) relationship
- Action must be elegant
- “Friendly Fire” disruption can harm commercial relationship with good customers
- Directly accountable w/ privacy regulation
- Often have abuse/legal burdened with overload when those these services are inelegant or ‘predictive’ irresponsibly

**Christine Runnegar**

# DNS AND PRIVACY

minimize collection

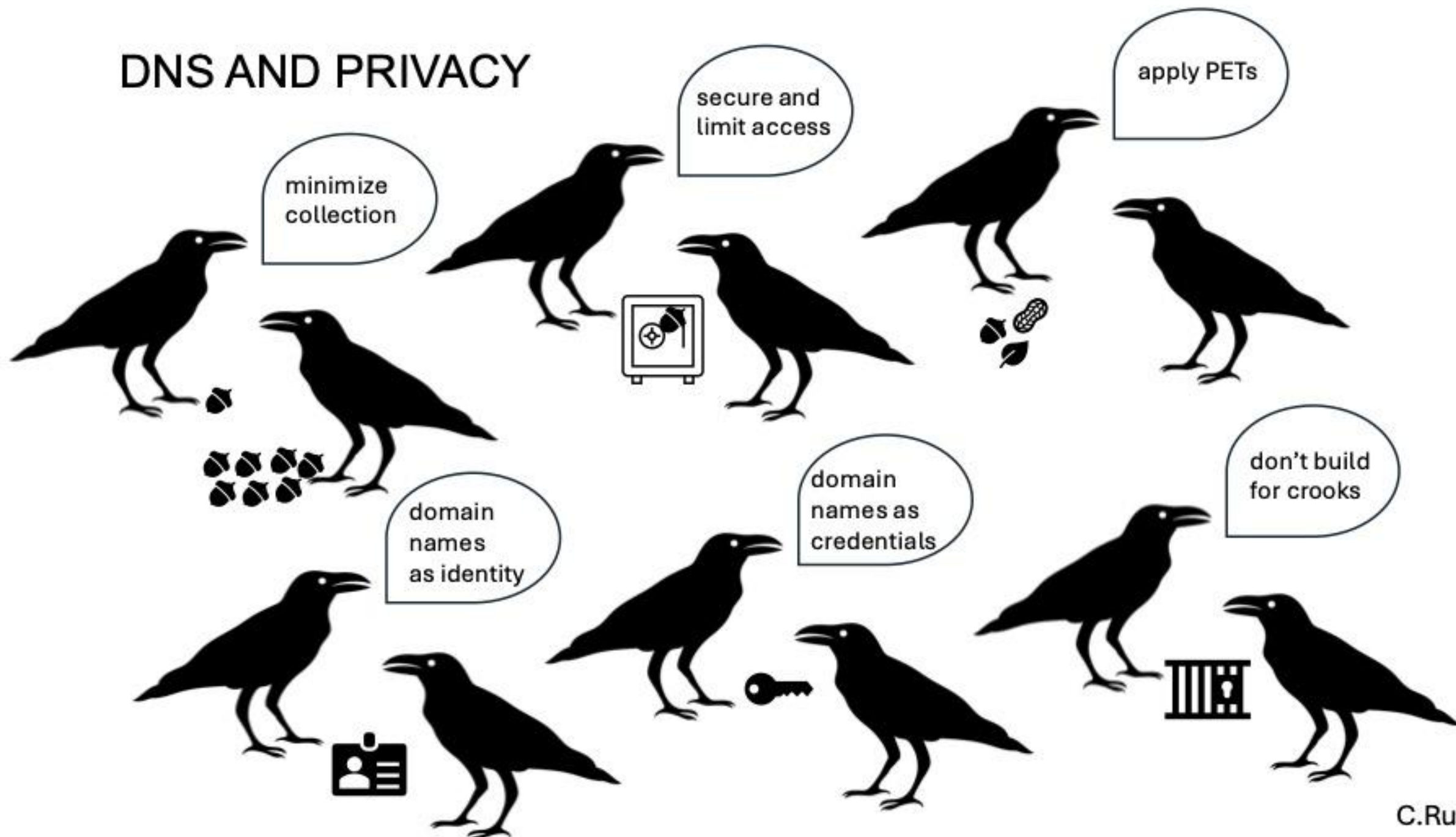
secure and limit access

apply PETs

domain names as identity

domain names as credentials

don't build for crooks



Frederico Neves

## **.br directory service**

- - Ownership / Technical / Contact data
- - Multiprotocol – RDAP/WHOIS
- - Single Point of [ab]use enforcement
- - Easy Explain/Understand Privacy Policy and Use
- aligned with legislation [1]
- - The main challenge lies in balancing level and reach of
- publicity with the need to maintain security for declared
- data in the Public Interest

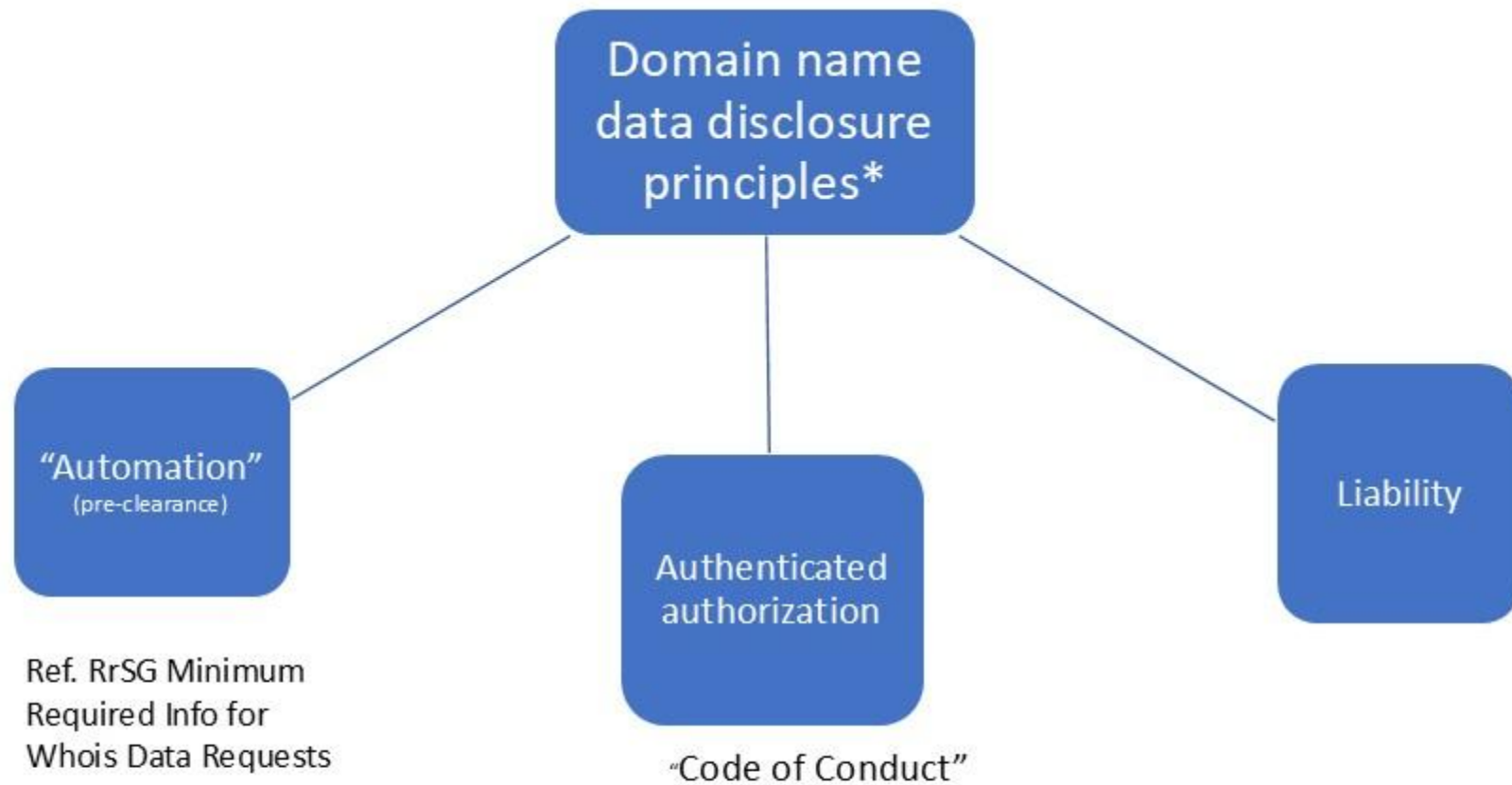
[1] <https://registro.br/politica-de-privacidade/en/>



GROUP TWO

James Galvin  
&  
Brian Beckham





\* Separate from/additional to broader data protection principles, e.g., fairness and transparency, purpose limitation, data minimisation, accuracy, security, accountability.

*“Protecting people must be the priority - I am warning organisations today that data protection law is not an excuse and it does not stop you sharing data that may assist with tackling fraud. Organisations acting responsibly can be reassured that we will take this into account if something goes wrong and we need to consider a regulatory response.”*

--UK Information Commissioner's Office

Steve Crocker



# What Does Good Look Like?

Steve Crocker

Edgemoor Research Institute

6 February 2025

# Surveying the Landscape

ENVIRONMENT

PROCESS

POLICY  
ENVIRONMENT  
S

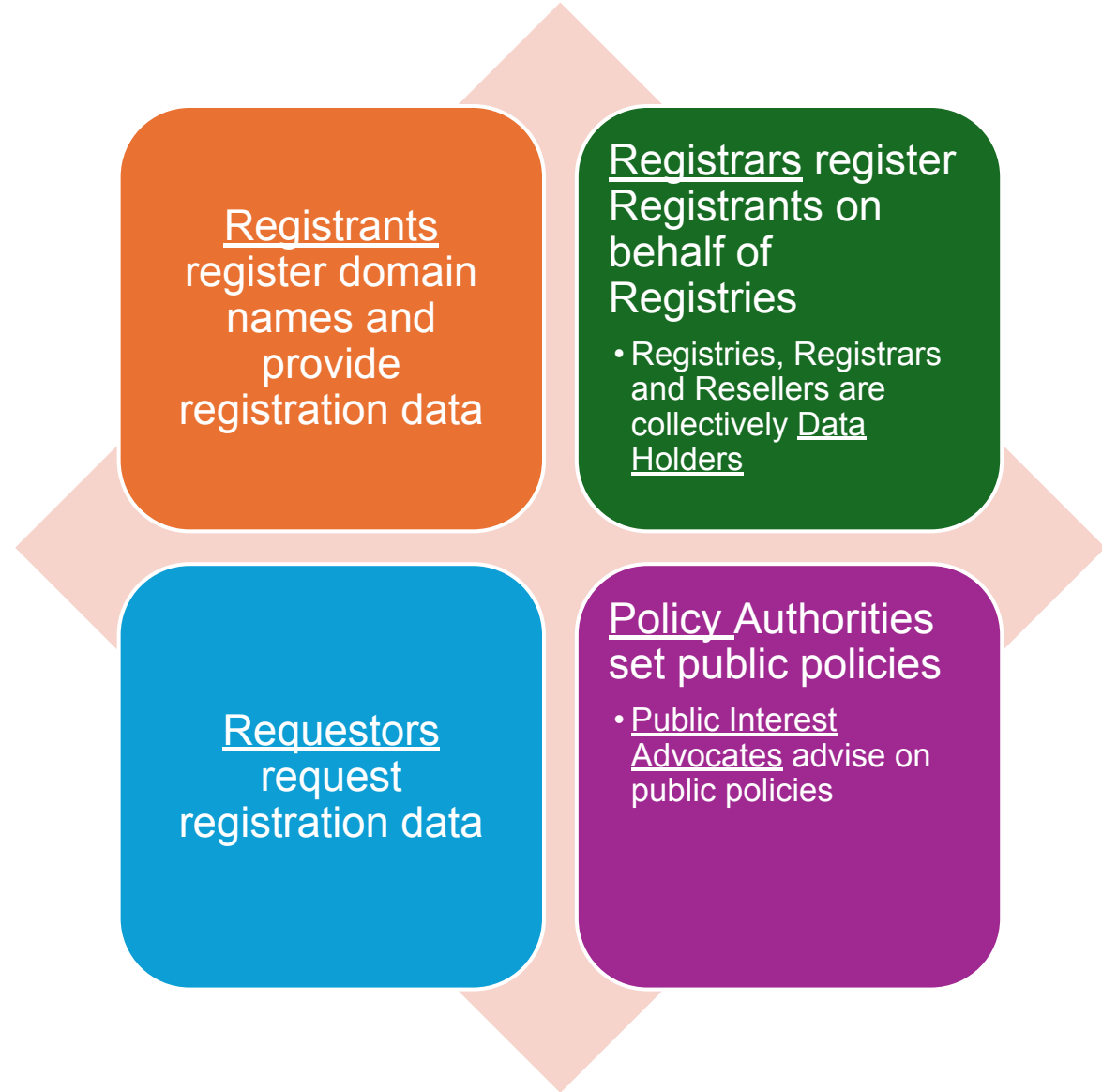
OPERATIONAL  
ENVIRONMENT

SEPARATING  
MECHANISM  
FROM POLICY

CONCERNS

GETTING  
THERE

# Environment



# Registration Process



During registration, registration data is collected



Which data elements are required, optional or not collected?



How thoroughly is accuracy checked?



What is the privacy sensitivity level for each data element?

This is a generalization of “public” vs “private”



These rules may depend on type of registrant and registry

Individual vs business; requires protection; has PII, etc.

# Disclosure Process

Requests  
for  
disclosure  
have  
several  
checks

---

Is the purpose of this  
request legitimate?

---

Is the requestor  
appropriate for this kind of  
request?

---

Is the requestor trusted  
and accountable?

---

# Dealing with Uncertainty

**What happens if the Registrar doesn't know the type of the registrant?**

**The rules should cover both known and unknown values**

E.g. Registrant is either individual, business or unknown

“Unknown” may be treated the same as one of the known types



# Policy Environment

Everybody has a policy. Often more than one.

Everybody...

These interact

Registries

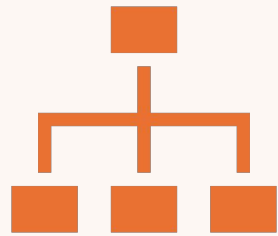
Registrars

Policy Authorities,  
e.g. ICANN, regional  
bodies, et al

Governments

Registrar must conform to Registry,  
Policy Authority,  
Government

# Operational Environment



## Distributed

There is no central place for policy development

- (ICANN gTLDs is large but only half of domains under management)

Operation of Whois was distributed. Next system should be too.



## Incremental

Different rates of adoption  
Policies evolve => iterative adoption

# Separating Mechanism and Policies

---

## Mechanisms

Protocols, e.g. RDAP

Data Element designations and definitions

Policy language and tools

## Policies

Collection, data element validation, sensitivity labelling

Disclosure

Interactions among different layers – Policy Authority, Registry, Registrar

# Concerns

Group	Concerns
Registrants	Privacy
Data Holders	Cost, Risks, Conformance with laws and regulations
Requestors	Clarity, Accuracy, Effectiveness, Speed, Cost
Governments, Public Interest Groups	Protect Privacy, Serve legitimate needs



Concerns

## Getting from Here to There

- **Clarity**
  - Requestors need clarity regarding requirements for disclosure
  - Registrars should specify requirements
  - Registrars can choose to consult with each other
  - Requestors should be able to predict outcome
- **Efficiency**
  - Prearrangement of trust
  - Prearrangement of request templates
  - Automated interfaces
- **Risk Reduction**
  - Insurance
- **Reporting, Auditing, Enforcement**



**Stay Tuned:**

**Webinar 2  
27 Feb 2025**

---



**Questions and comments:  
[info@edgemoorresearch.org](mailto:info@edgemoorresearch.org)**



GROUP THREE

**Anne-Sophie De Brancion**

Dave Piscitello

# Registration data: a research & responder perspective

- Researchers need real-time registration data for many of the same reasons as first responders
- Access to contact data is only part of the problem space
  - “Immutable” whois data – creation, registrar, name server – must be accessible in real time
  - Current rate-limiting practices impede efforts of first responders and researchers
- Regarding “protecting people must be the priority”... the domain community tends to consider personal data protection only in the contexts of the registrant and the liability of the registry/registrar operators
  - Registrants, especially natural persons, are a small percentage of the people who deserve protection
  - If we are to protect people as a priority, then the solution should consider the needs of those who speak for the victims
- A uniform and timely access framework across all TLDs would go a long way to ensuring that the needs of public safety, registrant, and the public are satisfied.

**Elliot Noss**

# Issues with the existing situation

- **We have a system that has worked for 6.5 years**
  - **Handled over 6k requests**
  - **Represents > 10% of the namespace**
- **Requests are way too often uninformed both as to the purpose and rules**
- **Requestors desire anonymity and just “want what they want when they want it”**
- **Compliance does not hold other registrars to ANY standard**
- **So many of the “complaints” resolve down to “my commercial business is not able to use this data to make money”**

**Nigel Hickson**