DNS/ccNSO TechDay

EWG Directory Services & Botnet Mitigation

ICANN Durban Meeting
July 2013

Rod Rasmussen
President & CTO
IID

ICANN

Agenda

- Some thoughts on botnet mitigation in a TLD
- Quick overview of recommendations for next generation registration directory services from the ICANN Expert Working Group

Botnet Mitigation within a TLD

Botnets need domain names

- Command & Control (c2), rendezvous, and other communications functions
- Botnet operators code or configure their malware to contact designated domains/ hostnames
  - Hard-code specific domains
  - Use rendezvous to update configs
  - Use Domain Generation Algorithm (DGA) to specify specific domain during a single window
    - E.g. Conficker, various Zeus variants

These can be easy to find

- Often random-generated characters
  - Visual inspection, known patterns
  - Algorithms or machine learning will expose these
- Use the same nameservers
- Fast Flux hosted
- For a TLD operator, even more tools
  - Resolution of non-registered DGA domains at the TLD from many ISPs
  - Known registrar patterns
  - Real-time zone file access

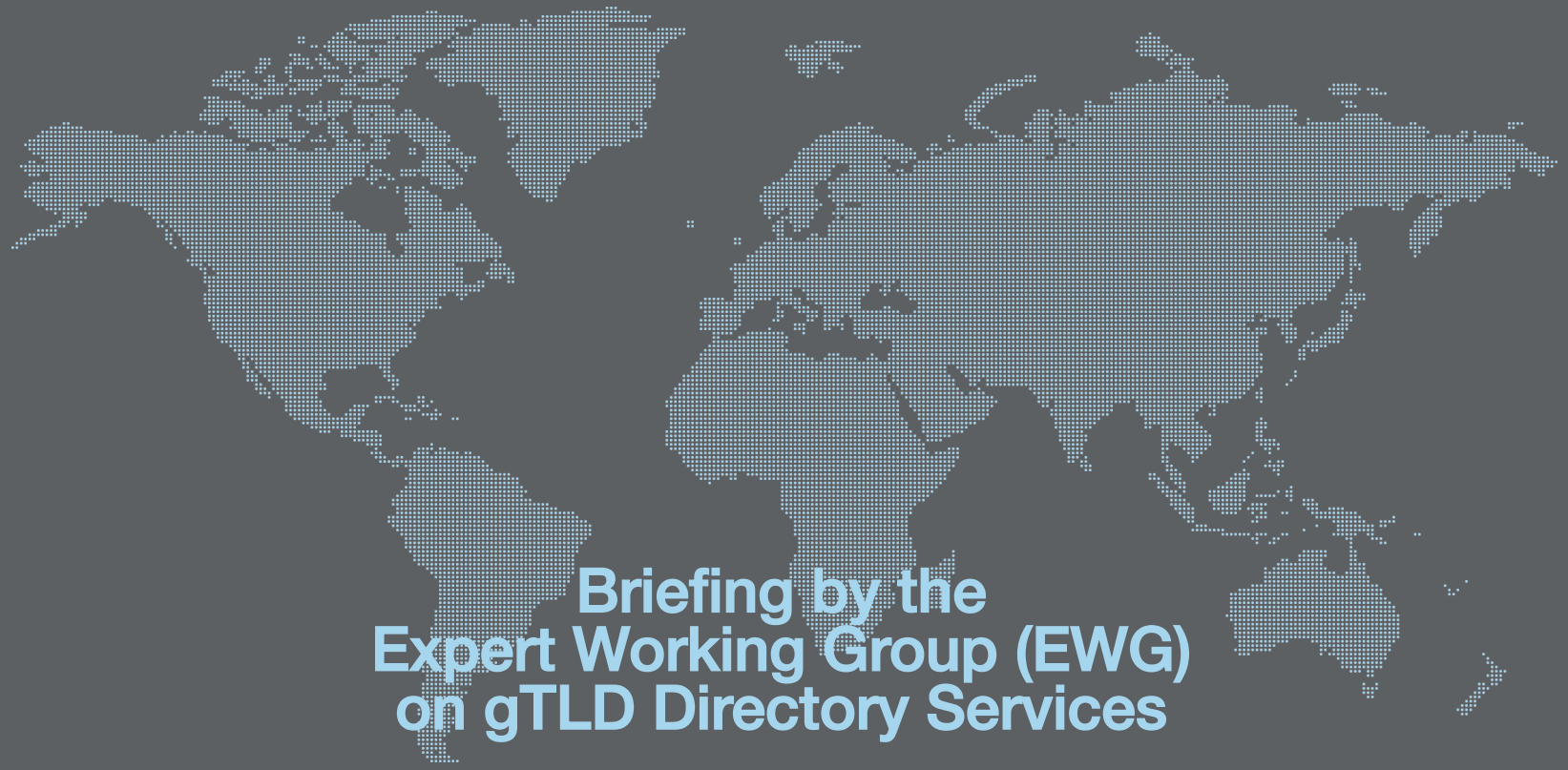
People will tell you about them

- LEA and Ops-sec personnel requesting shut-downs/sinkholing
  - What is your sinkhole policy?
- Reporting organizations (often free!)
  - SURBL, Spamhaus, ShadowServer, APWG, Stopbadware, Google Safe Browsing, Microsoft
- Commercial reputation/reporting services
  - Architellos, IID, Symantec, Websense, others

What is your policy?

- Range from “will not touch” to aggressively sinkholing servers
- How do you know if they are really c2s?
  - Need to be able to confirm claim or suspicion if you have policies to enforce
  - Threat team on-staff
  - Outsourced threat intelligence
- Suspend, delete, sinkhole, transfer to ???

A Next Generation Registration Directory Service (RDS)



Briefing by the Expert Working Group (EWG) on gTLD Directory Services

13 July 2013

ICANN

Mandate and Purpose

- ICANN Board directives
  - Implement the WHOIS Review Team recommendations
  - Redefine the purpose and provision of gTLD registration data
- EWG formed to assess the need for Next Generation Registration Directory Services and recommend a revolutionary approach

ICANN

Key Findings

- Initial Report published on 24 June

  https://www.icann.org/en/groups/other/gtld-directory-services/initial-report-24jun13-en.pdf

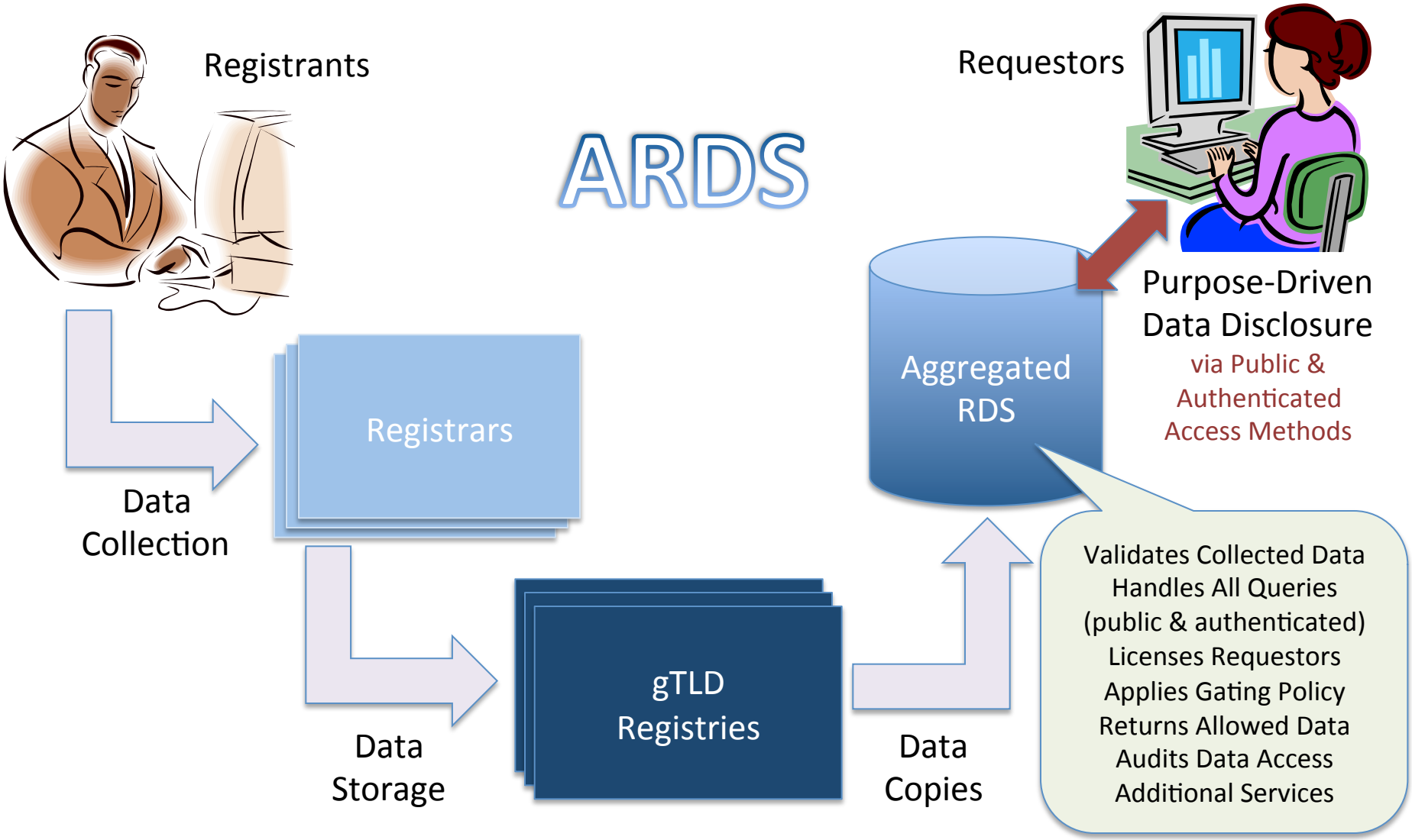
- Based on rigorous analysis of users and purposes
- Recommends paradigm shift
  - Abandon one-size-fits-all WHOIS system
  - Replace by purpose-driven system to improve privacy, accuracy & accountability

Desired Features and Design Principles

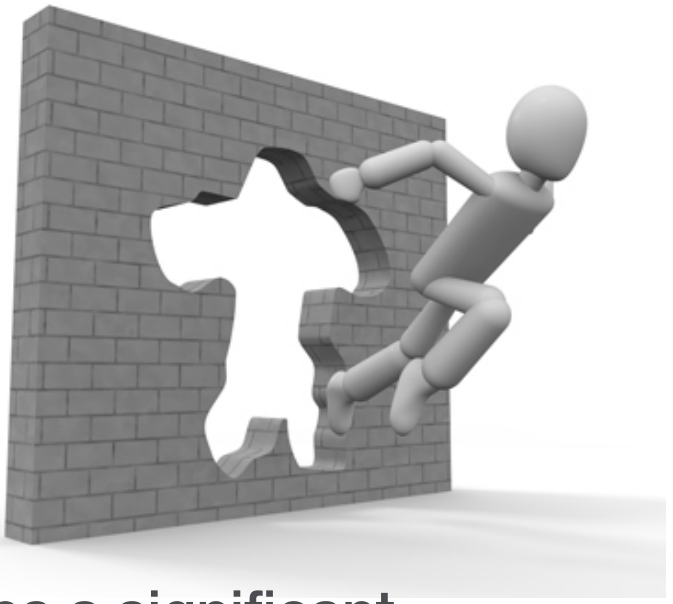
- Based on use cases, the EWG formed consensus on principles

Applicability	Data Elements
International Considerations	Access Methods
Accountability	Validation and Accuracy
Privacy Considerations	Standard Validation Service
Permissible Purposes	Contractual Relationships
Data Disclosure	Storage and Escrow

Suggested Next-Generation Model



Consensus View



- Our initial report represents our consensus view on recommended principles and features
- Also reflects compromises and thus will not fully satisfy all stakeholders
- While not perfect, we believe it describes a significant improvement over today's WHOIS for everyone
- We invite your constructive feedback
  - Is there a better solution?
  - If not, how can this suggested solution be improved?

Your Comments Are Requested

- Community input on draft and discussion questions by 12 August
  - http://durban47.icann.org/node/39627
  - mailto:input-to-ewg@icann.org
- EWG work will continue on open areas
- Final report before Buenos Aires
- Deliver to CEO and Board
- Input to GNSO PDP

Discussion Questions

- Additional RDS model advantages and disadvantages?
- How would requestors be identified, authorized and issued credentials?
- Who would accredit law enforcement agents, based on what criteria?
- Could maximum protected registration satisfy at-risk individual needs? How might a suitable solution be identified and funded?
- Are there any significant gaps in EWG-identified users and purposes?
- How could new users and purposes be accommodated? Who would decide, using what criteria?
- Are there any significant gaps in EWG-identified data elements?
- How should public and gated data elements be classified? Using what criteria?
- Registration data storage duration, escrow and access log requirements?
- How could next-generating RDS operating costs be borne?
- Other questions or comments?

http://www.icann.org/en/groups/other/gtld-directory-services/share-24jun13-en.htm

Thank You & Questions?

Rod Rasmussen
President & CTO
IID
rod.rasmussen@internetidentity.com

Backup Slides

Introductory Video

http://blog.icann.org/2013/07/replace-whois-with-the-ards/

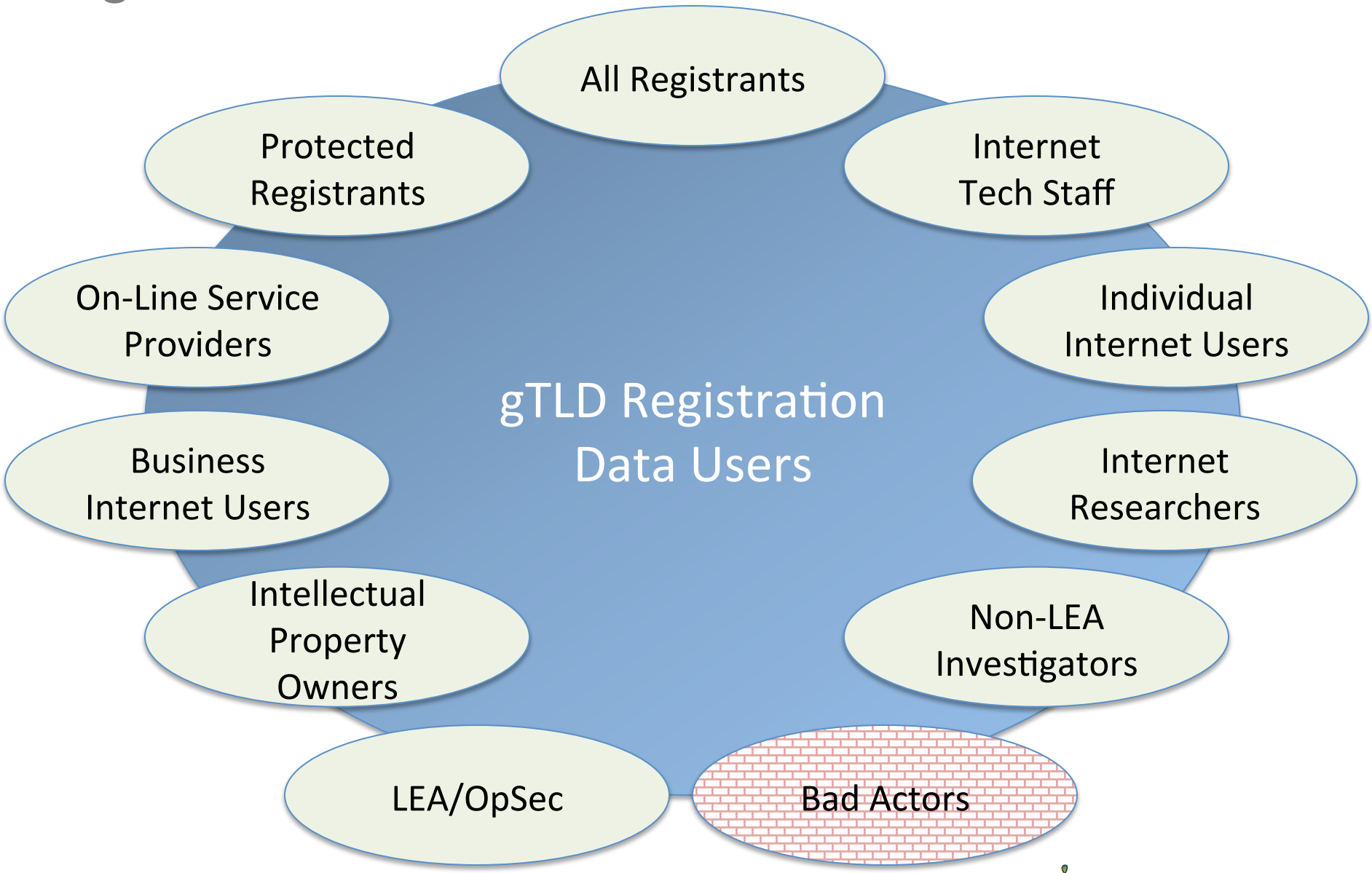
EWG Members

Jean-Francois Baril (Lead Facilitator)	
Pekka Ala-Pietilä	Michele Neylon
Lanre Ajayi	Michael Niebel
Steve Crocker	Stephanie Perrin
Chris Disspain	Rod Rasmussen
Scott Hollenbeck	Carlton Samuels
Jin Jian	Faisal Shah
Susan Kawaguchi	Fabricio Vayra
Nora Nanayakkara	

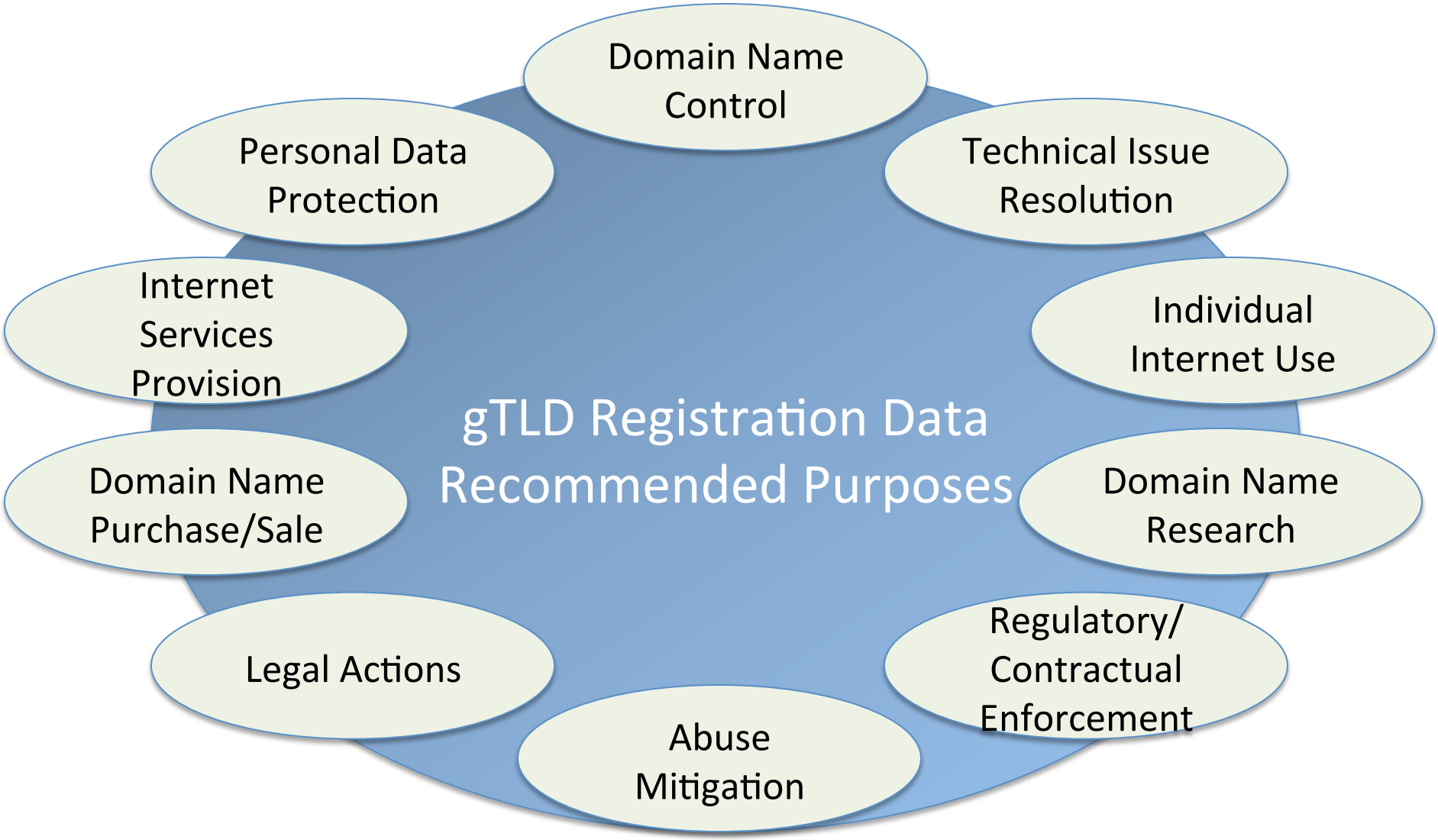
EWG Methodology

+ Comprehensive issue review
+ Examined stakeholder needs
+ Adopted Use Case methodology
+ Identified users and their purposes for wanting access to registration data

Registration Data - Users



Registration Data - Purposes



Recommended Principles – Privacy

- Enhanced Protected Registration Service
- Maximum Protected Registration Service
- Privacy/Proxy Provider Accreditation
- Further recommendations expected
  - Standardized processes for requests made by Law Enforcement, other licensed requestors
  - Model for accommodating domain registration using Secure Protected Credentials

Recommended Principles – Data Elements

+ Collected by registrars
+ Stored by registries
+ Purpose-based collection

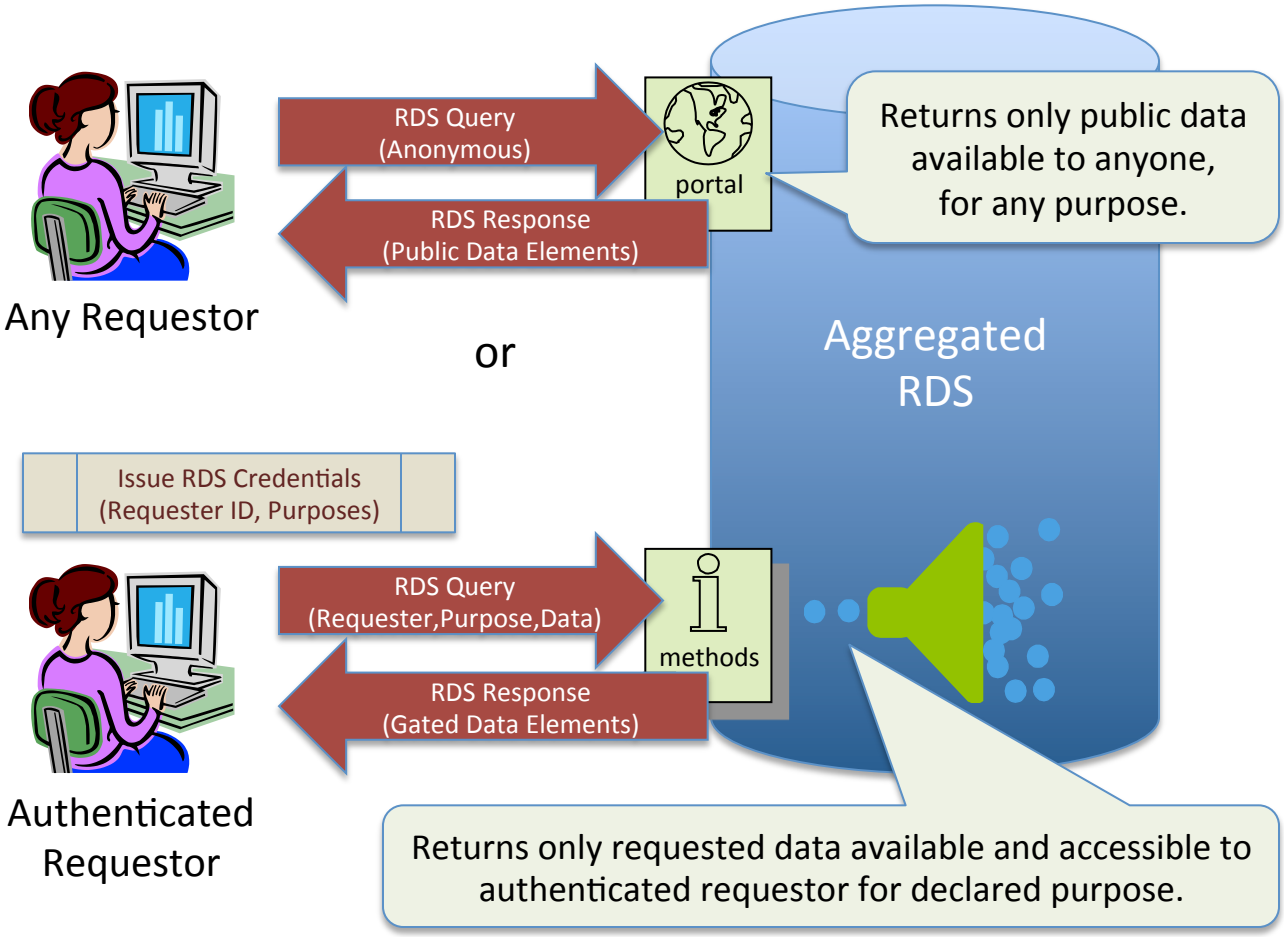
Data Element	Purposes
Registrant Name/Organization	Domain Name Control Personal Data Protection Technical Issue Resolution Internet Services Provision Individual Internet Use Business Domain Name Purchase/Sale Legal Actions Domain Name Research Regulatory/Contractual Enforcement Abuse Mitigation

+ Allow for extensibility

Recommended Principles – Data Disclosure

- Copied from registries
- Aggregated by RDS
- Purpose-based disclosure
- Public access to minimum data set, with restrictions to deter harvesting
- Gated access to other data, based on requestor identity and purpose

Recommended Principles – Access Methods



Recommended Principles – Validation and Accuracy

- Registration data should be validated syntactically when collected
- Name/contact should also be validated operationally
- Optional pre-validation of reusable registrant name/organization/contact
- Periodic time-stamped re-validation
- Standard validation service

Recommended Principles – Accountability

- All parties in the domain name ecosystem have responsibilities
- Current, accurate, timely data
- Reachable for timely resolution
- Responsible for registration and use
- Repercussions for misusing data or providing inaccurate data

Suggested Model: Aggregated RDS

- **Considered alternative models and Zone File Access Advisory Group findings**
- **Suggested Aggregate RDS (ARDS) model**
  - Non-authoritative copy of all data elements
  - Copied from authoritative gTLD registries
  - Registrars/registries relieved of port 43 and public access requirements
  - ARDS provides public and gated access to cached data, with option to query live data upon request
  - ARDS audits access to minimize abuse and handles accuracy complaints

Potential Advantages of Model

- ✓ Scale handled by a single point of contact
- ✓ Potential improvements in transport and delivery
- ✓ “One stop shop” for requestors of Registration Data
- ✓ Greater accountability for validation and access
- ✓ Ability to track/audit/penalize requestors across TLDs
- ✓ May reduce costs borne by Registrars and Registries
- ✓ Normalization or filtering of the data could be provided
- ✓ Reduces bandwidth requirements
- ✓ Facilitates approaches to satisfy local data privacy laws
- ✓ Enhanced search capability across TLDs
- ✓ Minimizes transition and implementation costs
- ✓ Enables validation/accreditation of requestors
- ✓ Facilitates more efficient accuracy report management
- ✓ Enables more efficient random accuracy checks

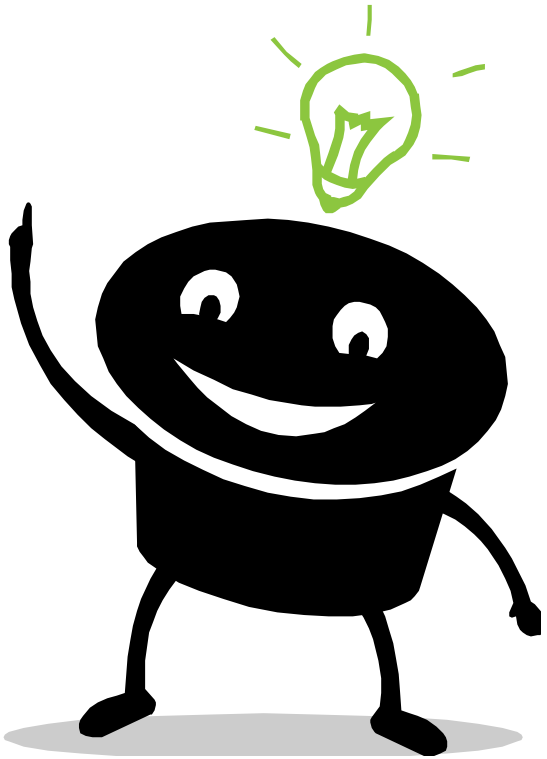
Potential Disadvantages of Model

- Potential for data latency
- Valuable “Big Data” source with potential for misuse if not properly audited and maintained
- Increased risk of insider abuse and external attack, requiring greater attention to security policy implementation, enforcement and auditing
- Registries/Registrars collect and store but are no longer in direct control of registration data delivery

Next Steps

- **EWG will continue to work on key issues…**
  - Privacy recommendations
  - Required/optional public/gated data elements
  - Pre-validation and inaccuracy remediation
  - Areas requiring risk and impact analysis
  - Storage and escrow requirements
  - Costs, impacts, ways they might be borne
  - Multi-modal access methods/protocols

How to Comment



Durban Public Session: Monday, 15 July
http://durban47.icann.org/node/39627

Calls, briefings, meetings upon request

Online Questionnaire:
https://www.icann.org/en/groups/other/gtld-directory-services/share-24jun13-en.htm

Comment via Email:
mailto:input-to-ewg@icann.org