Third Party Access to Non-Public Registration Data

A HOLISTIC APPROACH

For more information on InfoNetworks proposed approach, please visit: https://demo.verifyip.org

About WIPO

- WIPO is the global forum for intellectual property (IP) services, policy, information, and cooperation

- WIPO is a self-funding agency of the United Nations, with 192 member states

- WIPO's mission is to lead the development of a balanced and effective international IP system that enables innovation and creativity for the benefit of all

WIPO's involvement in Internet trademark policy

- WIPO has been actively involved with domain name-related issues since before the incorporation of ICANN
- In April 1999, WIPO published its *Report on the First WIPO Internet Domain Name Process*, leading to the adoption of the Uniform Domain Name Dispute Resolution Policy (UDRP)
- In September 2001, WIPO published its *Report on the Second WIPO Internet Domain Name Process* addressing identifiers considered as outside the scope of the First WIPO Process including:
  - (i) personal names; (ii) International Nonproprietary Names (INNs); (iii) names and acronyms of international intergovernmental organizations (IGOs); (iv) geographical indications, indications of source, or geographical terms; and (v) trade names

Problems with the current Whois / RDDS

- Under existing policies and contracts, ICANN is committed to maintaining “timely, unrestricted and public access to accurate and complete WHOIS information, including domain name registrant, technical, billing, and administrative contact information."
- The accuracy of domain name registration data (e.g., Whois / RDDS) has continued to be a concern since the formation of ICANN
- Historical challenges faced by third parties in accessing registration data for valid legal disputes have significantly increased due to changes made in response to the GDPR
- As recognized in the Temporary Specification, access to accurate registration data is critical in WIPO’s UDRP provider role
  - WIPO is the largest UDRP service provider, with thousands of cases each year

WIPO's continued thought leadership

- There is a continuing need to validate IP rights and IP right-holders as part of a UDAM framework, in addition to addressing data privacy
- WIPO has been approached about playing a specific / limited role in a UDAM framework given its institutional remit as the global forum for IP-related services
- WIPO has expressed its willingness to continue to engage with ICANN and other stakeholders in discussions regarding the evolution of a pilot of a UDAM framework, including a potential narrowly-defined WIPO role

Genesis of the InfoNetworks approach to UDAM

- Over twenty years heavy involvement in DNS governance and processes, including past few years of GDPR driven changes to Whois / RDDS
- Our approach using DNS-based digital ID's and verified credentials originated with the Universal Postal Union (UPU) and the .POST top-level domain
  - .POST is a registrant verified TLD
  - The UPU has promulgated their S68 Standard on Postal identity management trust
  - Several national Post Offices have been actively investigating digital identity initiatives
- We are prepared to pilot our UDAM solution ***now*** to test policy and approach criteria ***in parallel*** with ePDP policy development

Criteria for a successful approach to UDAM

- Benefits of our approach:
  - Addresses ***differing laws*** on privacy, data localization, and other regulations
  - Accommodates a variety of ***additional legitimate interests***; e.g.
    - Correlating pseudonymized data for security research and analysis
    - Verifying Registrant information and confirming data accuracy
    - Identifying parties for IP infringement and other legal claims
  - Uses ***open standards*** and ***proven technologies***
  - Requires ***minimal changes*** to existing systems, policies and data processing
  - ***Minimizes risk*** for data privacy non-compliance and data breach
  - Is ***economically self-sufficient***
  - Fosters ***competition, innovation*** and ***new opportunities*** for the DNS

Success requires a *holistic* solution: Policy-Technology-Legal

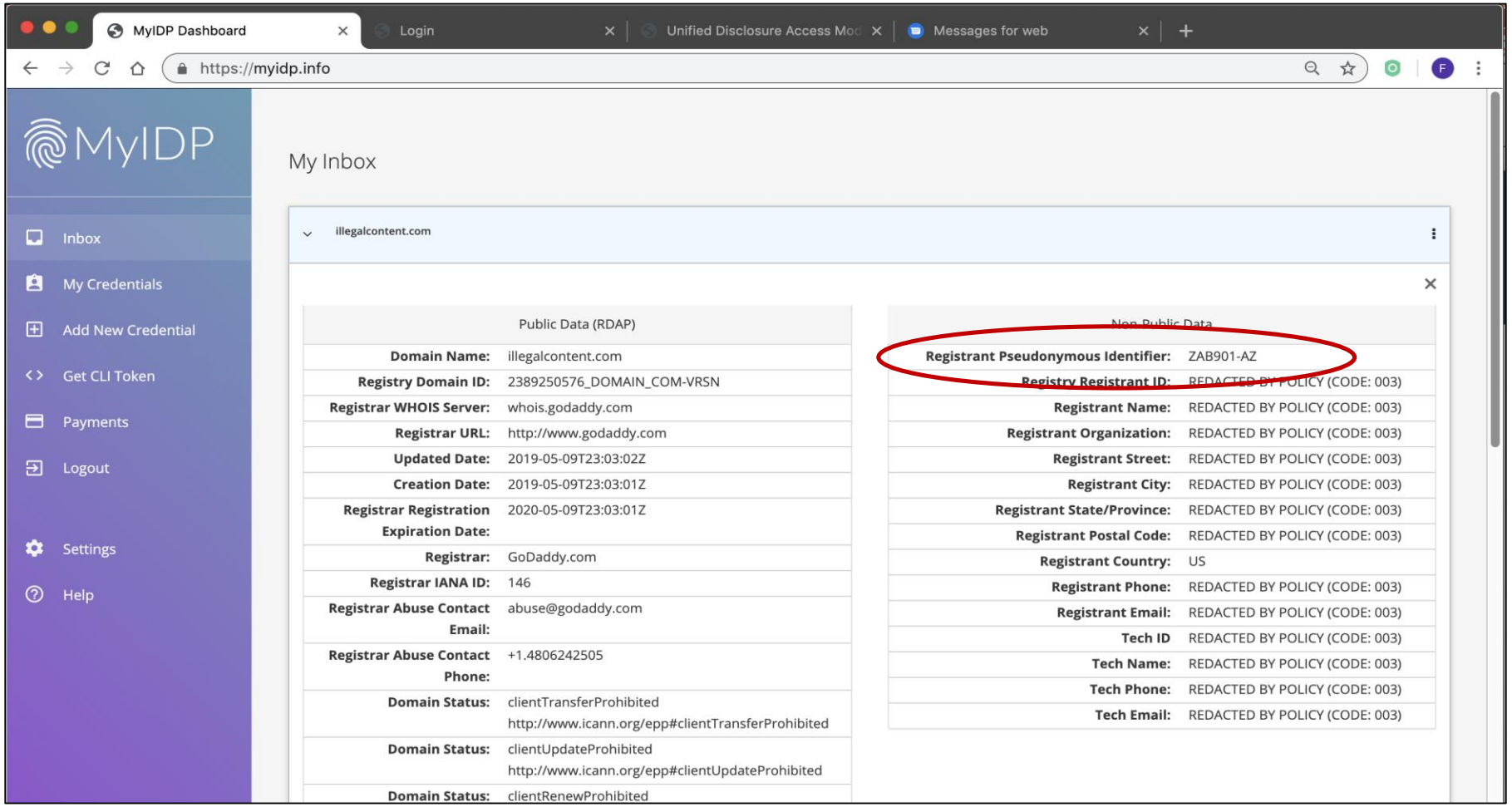
- ***Verification*** of Requestors for differentiated credentials subject to (i) a Code of Conduct, (ii) *ex post* dispute resolution, (iii) revocation for abuse, and (iv) financial requirements
- Request processing may be under both a ***"light touch" uniform consensus policy*** as well as enabling specific rules by Contracted Parties to meet local needs
- ***Customizable for manual review and/or automated rules-based processing*** of certain data in certain situations based on nature of the Requestor, the Request, and the Registrant
- ***Minimization of cost / risk*** with processing controlled by Contracted Parties, group cyber insurance, self-sufficient fee model, and implementing atop existing systems
- ***Local and centralized logging*** for abuse monitoring by Contracted Parties, and ICANN coordination and auditing for compliance

Strong privacy while accommodating additional interests

1. Requestor logs in with their federated credentials at any Contracted Party's UDAM gateway
2. Requestor submits a request for one or multiple domains with an attestation of legal right and lawful basis (requirements for which are based on their differentiated credential)
3. A Contracted Party receives and processes a request for their non-public registration data using policy rules (manual review or automated engine) to determine the response; e.g.:
   - A security researcher may receive pseudonymized data for general analysis; certain data may be unmasked for contacting a party regarding an imminent threat
   - An IP attorney or owner may receive generally identifying information for any infringement claim; but certain data may be flagged for review
   - A Registrant (with their own digital ID and verified credentials) may grant a "special use" credential to a Requestor to gain access to their registration data for a specific purpose (e.g. due diligence)

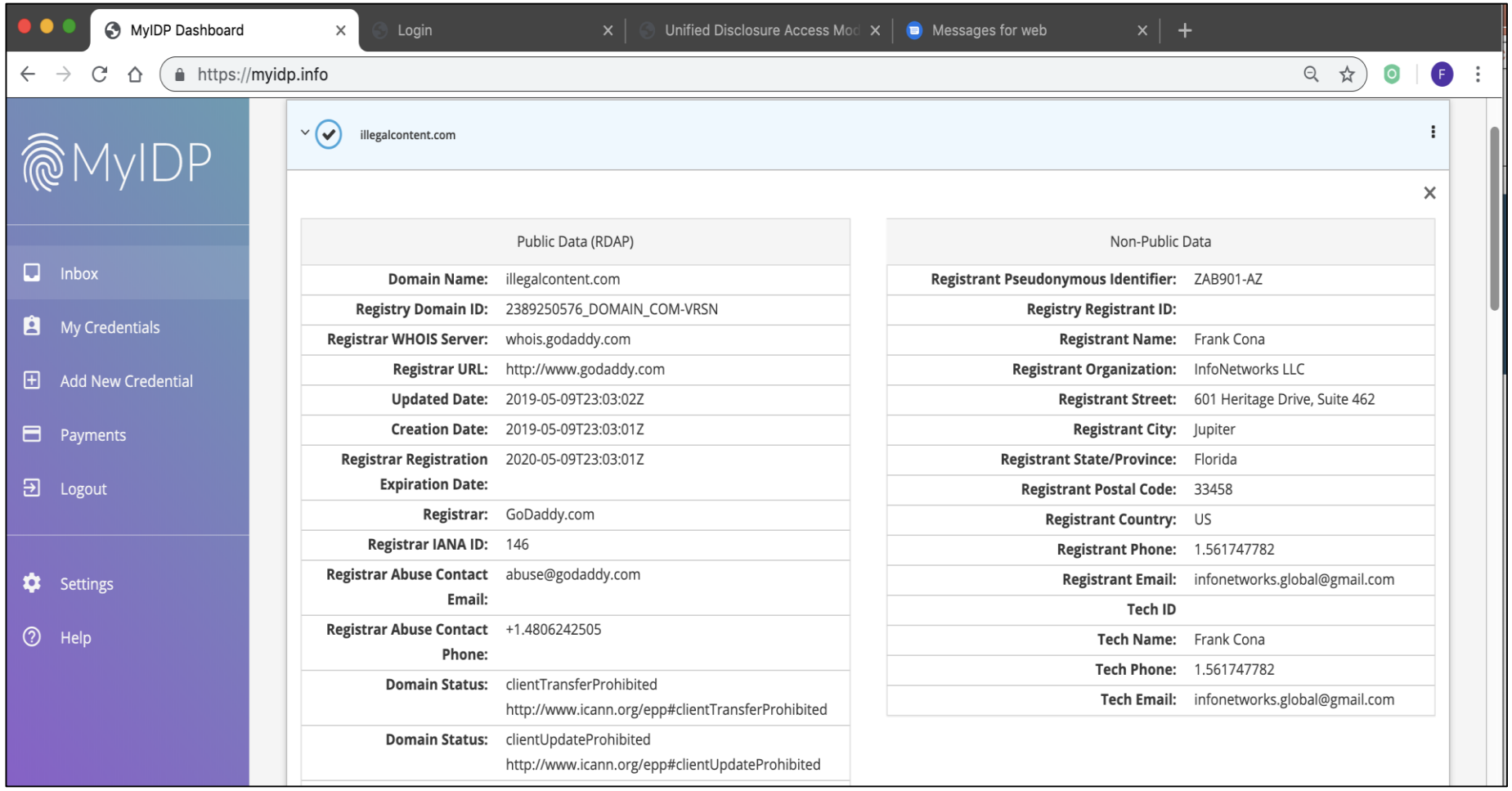
Strong privacy while accommodating additional interests

A security researcher may receive pseudonymized data for general analysis; certain data may be unmasked for contacting a party regarding an imminent threat



Strong privacy while accommodating additional interests

An IP attorney or owner may receive generally identifying information for any infringement claim; but certain data may be flagged for review

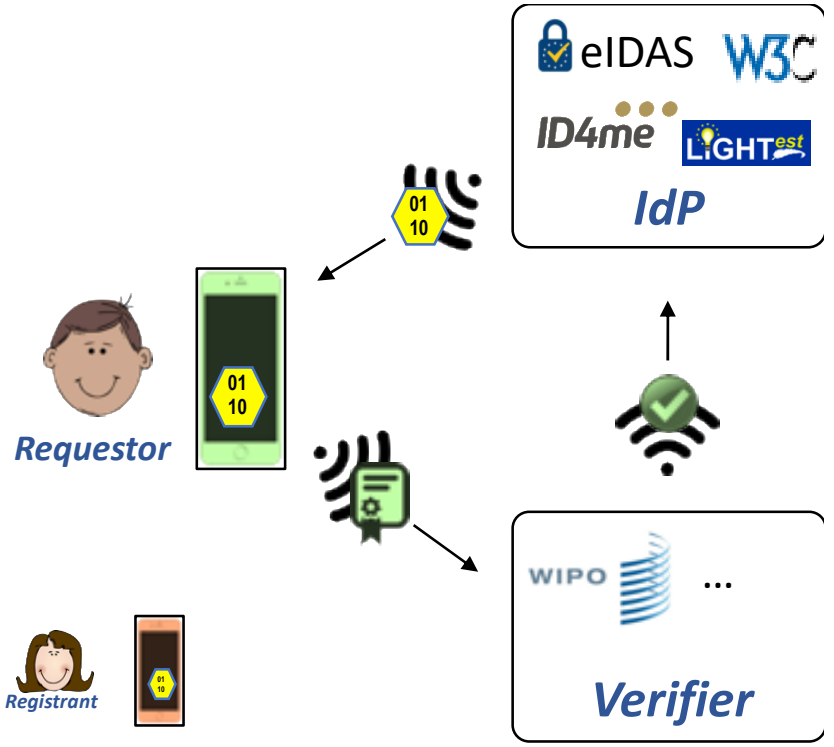


Strong privacy while accommodating additional interests

4. Each relevant response and/or data element is delivered to the Requestor's desired endpoint as review is completed
5. The request is pseudonymously logged by each Contracted Party and with ICANN
6. The request and Requestor details can be provided for compliance review or dispute resolution (may use a request process as well)

Foster competition, innovation, and new opportunities

- Promotes new use of the DNS as a discovery service for digital identity
- Creates new business opportunities for the DNS community in identity services
- Promotes Registrant verification, data accuracy, and verified ”chain of title”
- Potential framework for solving Privacy/Proxy Implementation
- Empower Data Subjects to exercise more control over their PII.



Thank you!

Brian Beckham:
brian.beckham@wipo.int

Michael D. Palage:
mpalage@infonetworks.global

More information available at:
https://demo.verifyip.org/

Key Takeaways

Our approach:

- Enables strong data privacy with minimal disruption
- Accommodates various additional concerns of different stakeholders
- Fosters competition, innovation, and new opportunities