PRIVACY PROTECTION FOR DOMAIN NAME REGISTRANTS AT ICANN: WHAT DO WE NEED TO BE GDPR COMPLIANT?

Stephanie Perrin

GNSO Councillor, NCSG

Graduate of PhD program 2018, Faculty of Information U of Toronto

Topic: The Struggle for WHOIS Privacy: Understanding the Standoff Between ICANN and the World's Data Protection Authorities

OUTLINE

1. Basics of the General Data Protection Regulation (GDPR)
2. Brief summary of the WHOIS directory and new registration data services
3. Privacy issues in registrant data collection, use and disclosure
4. Two problems in the arguments: purpose of collection and consent
5. Key issues flagged in the Article 29 letter out for comment

BASICS OF GDPR

- http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517578296944&uri=CELEX%
- Provides a more harmonized approach to law and enforcement
- Fines of 4% of revenues
- Article 29 Working Party of data commissioners becomes Data Protection Board, more powers

PRINCIPLES OF GDPR

- Data Minimization
- Purpose decided prior to processing, limited to core activities of organization
- Proportionality principle governs all processing actions
- Concept of data controller, co-controller, data processor, shared liability

WHOIS

WHOIS is a service that provides data on who has registered a domain name and what registrar they are using. The Internet Corporation for Assigned Names and Numbers (ICANN) inherited the service when it was established in 1998. WHOIS contains sensitive and sometimes personal information of domain name registrants.

WHOIS: A LONG STRUGGLE

- First WHOIS committee in 2000
- First Task Force 2001-3
- Second Task Force2003-4
- Combined Task Force 2004-5
- WHOIS Review Team 2010-12
- Experts Working Group 2013-14
- Registration Data Services 2015-???
- Transition to Thick Registries 2011-13
- WHOIS conflicts with law implementation 2015-16
- Privacy Proxy Services Accreditation 2014-2015
- RDS Committee, 2016-18

2013 REGISTRARS ACCREDITATION AGREEMENT

1. WHOIS data delivery requirements
2. Registrant data collection and retention requirements for law enforcement purposes (2 years after last contact with registrant)
3. Registrant data escrowed in US for recovery and legal issues (exceptions in EU, China)
4. Data must be available for bulk processing by third party service providers

THE DATA PROTECTION ISSUES

1. ICANN is the controller, sets requirements for registrars and registries who become data processors
2. Purpose of collection, use and disclosure is unstated except for a provisional agreement reached in 2006
3. Individuals are not informed of their rights under data protection law
4. Bulk access to data is required by the agreement, except for the purposes of spam or marketing
5. Value added services have proliferated (eg. whois.domaintools.com,)

THE DATA PROTECTION ISSUES

5. Registrars in jurisdictions with data protection law are required to seek a waiver of these requirements, must prove they have an enforceable order (WHOIS conflicts with law procedure)
6. Accuracy requirements are for the purpose of law enforcement, registrars forced to verify data and suspend domains where contact in question
7. Data elements include name, address, phone, fax, email contact
8. Data retention elements include metadata, financial information, IP address, all email traffic

PROPOSED SOLUTIONS: PURPOSE

- Purpose of RDS data collection, use and disclosure (processing) must match narrow ICANN remit
- Public safety actors and private sector security firms want easy public access to data, but is lawful investigation and trade mark enforcement a purpose of registration data collection?
- Risk of purpose of RDS data collection being broadened through "public interest commitments" (PICS) in new top level domains
- Language barriers: use case vs purpose of processing

PROPOSED SOLUTIONS: CONSENT

- Individuals unable to comprehend subsequent data flows and 3rd party access
- Consent is for all aspects of RDS requirements including data retention
- Withdrawal of consent meaningless due to value added services
- Layers of resellers and service providers, "sponsors" are the accredited registrars

RECOMMENDATIONS IN THE LETTER TO THE ARTICLE 29 WP

- Embrace the spirit, focus on risk to registrants
- ICANN should not be running a data repository for third party actors
- Law enforcement is not a legitimate purpose of processing data

RECOMMENDATIONS IN THE LETTER TO THE ARTICLE 29 WP

- Natural person v legal person
- Tiered access means accreditation and authorization …no self-certification, we need standards and independent audit
- Cybercrime fighting is a legitimate reason to disclose but it needs to be on an accredited basis, anonymized data analytics, etc.
- Need for a comprehensive privacy policy that covers ICANN's activities as a data controller. RAA could be transformed as a set of binding corporate rules.

RECOMMENDATIONS IN THE LETTER TO THE ARTICLE 29 WP

Registrant data beyond WHOIS:

- Data retention too long
- Escrow needs procedures, documentation
- TBDF issues for escrow, Thick WHOIS
- Zone files

QUESTIONS?

stephanie.perrin@mail.utoronto.ca

stephanie@digitaldiscretion.ca