Domain Name Registrant Data: The Privacy Questions

Alan Davidson
Center for Democracy and Technology
http://www.cdt.org

Understanding the Privacy Questions

- Goal: A framework for considering potential privacy questions raised by collection of and access to DNS registrant data.
- Context: What data is collected, why is it needed, and who is it collected about?
- Privacy: What privacy questions are raised?
- Best practices: Ideas for reconciling privacy questions and data access needs.

Context: The Need for Registrant Data

- Technical stability
- Law enforcement
- Consumer protection
- Intellectual property protection
- Competition

A Spectrum of DNS Registrants

- Range of domain name registrants: From large companies to individuals pursuing non-commercial purposes.
- Increasing number of individuals in gTLDs. (Verisign estimate: 15% “non-business” and growing)
- Note: Very different privacy expectations for different types of users.

Data Collection and Access Requirements

The gTLD experience:

- Data collected: Technical, billing, and administrative contact. Require name, address, phone, and email.
- Access to data: Full public access, as quickly and completely as possible, for anyone online.
- Bulk access: Both individual queries *and* bulk transfer to compilers and resellers of registrant info.

Privacy Questions

- Note: Wide range of cultural perspectives and national laws.
- *Is personal information collected?* For businesses, almost certainly not. For individuals, data can be personally identifiable and sensitive. (ex. home phone number)
- *Is there an expectation of privacy?* For businesses, should be no. But for individuals, possible expectation of privacy today.

Privacy Questions II

For individuals with a privacy expectation:

- *Are Fair Information Practices followed?* Key issue is use of data.
- *Is the data used solely for the purpose for which it was collected?* Difficult to enforce against secondary uses today. Possible unintended uses: Marketing and unsolicited email. Criminal use. Government persecution.
- *Other concerns?* Some will not want to sacrifice privacy in order to access the DNS.

Reconciling Privacy Questions

Some ideas for dealing with individual privacy::

- Public education: Good notice, clear understanding of alternatives
- Meaningful alternatives to registration
- Allow proxy contacts (like “unlisted” numbers in the telephone book) for some registrant data

Reconciling Privacy Questions II

Other ideas, raising implementation difficulties:

- Limit secondary uses (allow bona fide requests, prohibit others)
- Make only some data widely available (such as tech contact, legal address)
- Separate commercial actors and non-commercial individuals (difficult!)
- Create audit system and allow review of database queries (with delay as needed)

Conclusion

- Range of important demands for fast access to registrant data.
- Privacy questions limited in commercial setting, but raised by individual registrants and secondary use of information.
- Look forward to working on ways to balance these concerns and reconcile privacy questions.

Fair Information Practice Principles

- Openness (Notice)
- Consent (Choice)
- Access
- Security
- Accountability (Enforcement)

- Collection Limitation
- Data Quality
- Use Limitation