CDT Discussion Draft
Technical Requirements for Whois

The Whois database must accommodate important and legitimate needs for access to registration data, but it also continues to raise privacy questions, particularly regarding inappropriate secondary use of sensitive personal data in some circumstances. VeriSign's Whois consultations offer a valuable opportunity to discuss technical specifications that may be helpful in addressing both legitimate access to Whois information and important protection of private and sensitive data.

In the hopes of furthering constructive conversation, CDT believes that several areas of technical requirements might prove fruitful in accommodating these needs.

1. "Tiered" Model of Data Availability. Whois data is currently made available in a "one-size-fits-all" format that provides the same level of access for an anonymous inquiry by a spammer as for an urgent law enforcement request. Individual privacy could be enhanced by the introduction of a layered access model, in which different data fields are provided in response to different types of inquiries:
    - Different data tiers could support different rules for availability of data classified as most sensitive;
    - Different access/user tiers could provide access to more data, more quickly, for classes of users such as law enforcement or other bona fide requesters.

2. Audit Mechanisms. Inappropriate or abusive secondary use of registrant data could be substantially curtailed if mechanisms were in place to audit and review requests for data. Records could be kept of Whois requests, the requesting party, and Registrants could even receive, or at least have access to, regular updates concerning access to their Whois records and, if known, the purpose for which that access was granted.

3. Support for Third-Party Proxies. One popular solution to dealing with privacy questions is to allow registrants to designate responsible third-parties who serve as administrative or technical contacts, allowing registrants to protect private information. Many companies currently use such proxies. Whois could support such third-party proxies, possibly through the introduction of data fields that indicate when a third-party is being used.

4. Different Whois Rules for Different TLDs or Other User Categories. Whois could support a variety of access rules based on the TLD or some other classification of registrant. For example, some have indicated that the privacy interests of individuals differ from the privacy interests of companies doing business online. Whois could support differing access rules for registrants in a hypothetical ".individual" (say of non-commercial individuals) versus data of registrants in a ".business" (say of commercial organizations only.) Whois could support, at an administrative level, development of distinctive data practices for differing classes of registrants. The

distinction between records need not be binary—for example, unique data practices could be developed for registrations made for political uses, personal uses, technical uses, etc.

5. User Control. Under the current system, domain name registrants have extremely limited control over the secondary use of their personal data. An upgraded Whois that incorporates greater user-control into the infrastructure, akin to the P3P specification for web communications, could prove fruitful especially in conjunction with different types of data access.

We note that many of these ideas are most powerful when used together. We also note that some of these concepts may make bona fide access to data for important purposes either slower, or more expensive – though perhaps not unreasonably. For these reasons, these suggestions are put forward in draft form as a starting point, and we look forward to further discussion of their implications.