Summary of Positions

I. IPC

A. IPC supports, in principle, the use of query volume limitations on Port 43 access in order to discourage data mining.

B. Being supportive of the debate, the IPC submits that any changes in practice or regulation have to be designed in a manner that does not inadvertently have detrimental effects on the legitimate use of Whois.

C. Specifics:

a. Any provision should maintain and ensure availability of unhampered access to Port 43 for legitimate applications that require high volume access to domain name Whois for use in creating value-added products and services that are of great value to the intellectual property community and to the business community in general.

b. Adequate provision must be made for intermediaries which aggregate low-volume requests from end-users into a relatively high volume of queries through Port 43.

c. A solution must identify realistic volume break-points between low-volume queries via Port 43 that should remain unrestricted, and a very high volume of queries that could, in principle, require an efficient and workable form of disclosure to registrars (or registries in the thick registry model) of the uses to which query results would be put.

d. The solution should also preserve the unrestricted availability of Whois queries through a web-based interface, and the status of Port 43 as a service available free of charge.

e. The solution must be accompanied by proactive enforcement of the obligation to make bulk access available.

II. ALAC

A Two-tiered system.

- Tier 1: Public Access. Users who access a future WHOIS-like system anonymously get access to non-sensitive information concerning a domain name registration, to be defined in detail by task force 2.
- Tier 2: Authenticated access. Users who want to access a more complete data set (to be defined in detail by task force 2) need to reliably identify themselves, and indicate the purpose for which they want to access the data. The identity of the data user and their purpose is recorded by registrars and registries, and made available to registrants when requested. This information could be withheld for a certain amount of time if the data user is (1) a law enforcement authority that is (2) accessing the data for law enforcement purposes.

B. Implementation: No specific implementation ~~although recommends SSL for I~~recommended; example: SSL client certificates. [~~Possibly use~~Prefer IRIS or other dedicated protocol over web forms~~].~~]

C. Rationale:

- Find out purpose of use of Whois data. Registrars would have to verify purpose, but can't. Resort to heuristics.

- The best heurisitc we know of is to hold data users accountable for their activities, and to put enforcement of purpose limitations into the hands of registrants. This can be achieved by reliably identifying data uses and putting their identity, contact information, and purpose indication in the hands of registrants.
- At the same time, a tiered system -- if implemented reasonably -- could preserve the ability of data users to automatically access WHOIS data in reasonable quantities. Registrars, on the other hand, would be enabled to limit the amount of data any particular party can access in a given interval of time.

B. Discussion of other proposals

- CAPTCHA: There have been suggestions that "automated access" could be used as a heuristic to determine illegitimate access. In this scheme, automated access is blocked by attempting to require human attention with all queries. One set of implementations of these kinds of tests is known as CAPTCHA.
  - CAPTCHA blocks legitimate automated access
  - Easy to circumvent because of design problems (See http://boingboing.net/2004_01_01_archive.html#107525288693964966 and http://www.cs.berkeley.edu/~mori/gimpy/gimpy.html
  - Accessibility issues: http://www.w3.org/TR/turingtest/
  - In Sum: Do not recommend.

III. Noncommercial Domain Name Holders

A. ICANN must recognize that the purpose of Whois originally was identification of domain owners for purposes of solving technical problems. The purpose was not to provide law enforcement or other self-policing interests with a means of circumventing normal due process requirements for access to contact information.

B. NCUC does not believe it is possible to develop technical mechanisms that can restrict port 43 or port 80 access only to a specific type of purpose; e.g., "nonmarketing uses." Access restrictions imposed by TF1 will inevitably apply to any whois user regardless of purpose. Moreover, restricting Port 43 access while leaving Port 80 open will only drive the automated processes to Port 80.

C. Therefore we question whether TF1 can achieve anything of value. Task force should refrain from making judgments about the legitimacy of, justifications for, or "need" for any non-marketing uses. It is outside the scope of TF1 to make any such determinations.

D. Automated scripts or programs using port 43 are effectively a substitute for bulk access. A policy determination on port 43 access is best made in conjunction with a determination on bulk access.

E. Fifth, the best way to stop abuse of ports 43 or 80 is to get data that is valuable to spammers out of the public Whois database. [TASK FORCE 2]

F. Changes to Port 43 are not a substitute for privacy protection.