Key Terms that May be Used in Future WHOIS Studies

Background and purpose: At the GNSO Council meeting held on 2 November in Cairo, the Council decided that it would be helpful to develop "working definitions" of several terms that are being used in the context of Council discussions of possible future studies of WHOIS. At the meeting, Council members identified the following eight terms and asked staff to develop initial working definitions that the Council could use as a starting point for further discussion and definition. In order to respond to the Council's request, staff solicited definitions from GNSO Council members and community stakeholders. We also researched and reviewed ICANN meeting transcripts, policy and compliance documents and constituency position statements, as well as other reference papers, noted below. The following is a compilation of that research, intended to respond to the Council's request. ***The following does not represent the viewpoints or positions of ICANN or ICANN staff and is for community discussion purposes only.***

1) **Undesirable Content**

Content that is intentionally annoying, offensive or inappropriate to the individual, the organization, the community or the society as a whole. Undesirable content may be objectionable as a matter of its form or function, or as a matter of its meaning, intent and context. Undesirable content may be material that is illegal; overtly threatening to national security; or politically, socially or culturally subversive or taboo.
http://www.law.indiana.edu/fclj/pubs/v51/no2/hoganmac.PDF

Examples of undesirable content may include:

- Information which is knowingly false, defamatory or intended to cause public panic or to incite illegal or immoral activity;

- Spam emails, including unsolicited emails that contain viruses, frauds or links to objectionable content. htp://www.sprintbroadband.com/undesirable_content.html

- Spam blogs and link spam causing annoyance, harassment or noise
  http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech467.pdf

- Child Pornography,

- Hate sites that intend to incite violence or other illegal activities

- Pirated or copyright infringed material

- Spyware and malware

Deleted: Pornography, hate talk, questionable chat rooms

Deleted: Gambling and violent gaming sites

- Government restricted or censored information

Internet content that is "undesirable" must be distinguished from content which may be troubling, troublesome or shocking but remains legitimate free speech. From a global perspective, the idea of free speech and largely unfettered communication is, of course, notional, not absolute. Democratic countries have the deepest commitment to free expression and the most liberal interpretation of what is acceptable content. Other countries view the Internet and the content it conveys as a means of reinforcing national cultural norms and values and social stability. Such countries may take a more restrictive approach to free speech and a much more expansive view of "undesirable" content.
http://bcis.pacificu.edu/journal/2002/06/kawamoto.php

Similar ambiguity surrounds the issue of criminalized speech on the Internet. Providing a counterfeiter with the tools needed to break protective encryption is the use of the Internet in the furtherance of a criminal act. Posting the tools for the world to see may be nothing more than a technologist engaging in activity with a variety of useful outcomes, such as demonstrating a technical innovation to spur discuss, promote a technical approach or advance research.
http://www.umass.edu/legal/Benavides/Fall2004/397G/Electronic%20Reserve/10%20Brenner.doc

2) Misuse

Misuse is an action that causes actual harm, is the predicate to such harm, is illegal or illegitimate, or is otherwise considered contrary to intention and design of a stated legitimate purpose. When applied to Whois data, such harmful actions may include the generation of spam, the abuse of personal data, intellectual property theft, loss of reputation or identity theft, loss of data, phishing and other cybercrime related exploits, harassment, stalking, or other activity with negative personal or economic consequences. The predicate to harmful action includes automated email harvesting, domain name registration by proxy/privacy services to aid wrongful activity, and support of false or misleading registrant data. Contrary acts might include the use of Whois data to develop large email lists for commercial purposes.

http://forum.icann.org/lists/pdp-pcceg-feb06/msg00528.html

http://cai.icann.org/files/meetings/cairo2008/Cairo01NOV08GNSOWSpm.txt

http://gnso.icann.org/issues/whois/whois-study-hypothesis-group-report-to-council-26aug08.pdf

http://forum.icann.org/lists/whois-comments-2008/msg00001.html

http://forum.icann.org/lists/whois-comments-2008/msg00026.html

3) Commercial Purpose

Related to a bona fide business use. In the Internet context, the bona fide use or bona fide intent to use the domain name or any content, software, materials, graphics or other information thereon, to permit Internet users to access one or more host computers through the DNS: to exchange goods, services, or property of any kind in the ordinary course of trade or business; or to facilitate (i) the exchange of goods, services, information, or property of any kind; or, (ii) the ordinary course of trade or business.
http://www.icann.org/en/tlds/agreements/biz/appendix-11-08dec06.htm

http://cyber.law.harvard.edu/tlds/001/

4) Proxy and Privacy Services

Proxy and Privacy services provide anonymity and privacy protection for a domain name user.   Though the terms are colloquially used interchangeably, there is a difference.

Privacy services hide customer details from going into WHOIS. Privacy service providers, which may include registrars and resellers, may offer alternate contact information and mail forwarding services while not actually shielding the domain name registrant's identity. By shielding the user in these ways, these services are promoted as a means of protecting personal privacy, free speech and human rights and avoiding personal data misuse.
http://gnso.icann.org/drafts/icann-whois-wg-report-final-1-9.pdf
http://gnso.icann.org/mailing-lists/archives/tf2-survey/doc00003.doc

Proxy services protect users' privacy by having a third-party register the name. The third-party is most often the Proxy service itself. The third-party allows the user to access and use the domain name through a separate agreement or some other arrangement directly with the user. Proxy service providers may include web design, law, and marketing firms; web hosts, registrar subsidiaries, resellers and individuals.
http://gnso.icann.org/drafts/whois-study-overview-gnso-council-04oct07.pdf.
http://www.icann.org/en/topics/raa/amendments.html#escrow

5) Relay Information Requests

Problems arise from time to time in connection with registered names. Allegations of actionable harm require copyright owners, law enforcement officials and others to be able to operate through a proxy or privacy service provider to contact the domain name user. Potential "harms" could include suspected fraud, intellectual property rights infringement, or the infringement of other civil or criminal laws. To support the relay of

Deleted: p

Deleted: Essentially, proxy services are a subset of privacy services. Privacy services hide customer details from going into WHOIS.

Deleted: Proxy services do that by having a third-party register the name.

Deleted: Non-proxy p

information requests, service providers must have reliable and timely means of communicating with their domain licensees. The ICANN Registrar Accreditation Agreement stipulates that the proxy registrant reveal the identity of the domain licensee upon reasonable evidence of actionable harm or risk liability for resulting harm.

http://forum.icann.org/lists/whois-comments-2008/msg00023.html
http://forum.icann.org/lists/gnso-whois-wg/pdfi6hAmW7P6J.pdf
http://gnso.icann.org/issues/whois-privacy/whois-wg/whois-working-group-charter-16apr07.pdf

6) Falsify Whois Data

Falsifying Whois data is an issue that balances the need to balance the technical and legal requirements of Whois domain name registration records with the right to registrant privacy. http://www.icann.org/en/committees/security/sac003.htm The security and reliability of the Whois data base depends on data accuracy. ICANN therefore expects registries and registrars to collect accurate information and to take appropriate action if false information is discovered or suspected, while at the same time providing mechanisms to protect privacy.
http://www.icann.org/en/committees/security/whois-recommendation-01dec02.htm#1.1

| Deleted: prevent |
| Deleted: n |
| Deleted: registrations |

7) Natural Persons

A real, living individual as opposed to a "legal person" which may be a company, business, partnership, non profit entity or trade association. Registrants indicate whether they are registering a domain name as a "natural person" or a "legal person" at the time of registration. In the Whois context, personal data refers to any identified or identifiable natural person.
http://gnso.icann.org/drafts/draft-report-whois-wg-28jun07.pdf
http://gnso.icann.org/mailing-lists/archives/council/msg02742.html

| Deleted: is |
| Deleted: declare |

8) Adequate Protective Measures

Countermeasures designed to thwart the automated collection of domain records via query based Whois services. Examples include the Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), which requires the querying part to perform certain tasks, such as verifying an access code by typing it into a text field or interpreting a visual image. Privacy services are also used as WHOIS protective measures, making personally identifiable domain name user information unavailable to automated query.

| Deleted: Proxy and p |

http://www.icann.org/en/committees/security/sac023.pdf