NSF/OECD WORKSHOP -- WASHINGTON, 31 JANUARY 2007
SOCIAL & ECONOMIC FACTORS SHAPING THE FUTURE OF THE INTERNET
SPEAKERS' POSITION PAPERS

LESLIE DAIGLE, CHAIR, INTERNET ARCHITECTURE BOARD (IAB) – HOW TECHNOLOGY EVOLUTION CAN BE PARTNERED WITH SOCIAL POLICY AND REGULATORY DISCUSSIONS

Perspective: Today, I'm speaking as a technologist in a panel on social implications shaping the future of the Internet. What I'd like to do is share some experiences in developing a revision of one piece of Internet infrastructure to address competing legal, social and commercial interests that had evolved considerably since the deployment of the original technology. The purpose of this illustration is to examine one of the ways that technology evolution can be partnered with social policy and regulatory discussions. As a technologist, I'm not going to presume to offer answers to some of the hard social issues identified her, but rather respect those issues as real requirements for the development of the technology. While it's clear in this room that technologists should not "do policy", the reality is that the converse is equally true. We need better partnerships of discussion going forward.

When I started working with Internet technologies, well over fifteen years ago, the striking thing about the network was that it was a communal technological working environment. Anyone with suitable technological skills could put up a network host, and "be" "on" the Internet.

Innovations such as the World Wide Web were made possible by such techno-egalitarianism: new technologies could be made available and adopted by any "clueful" network user. One of the impacts of the World Wide Web was in turn to enhance the reach of new technologies by lowering the bar to developing and providing accessible on-line information and advertisement of the technologies. (People no longer had to know file names and use Archie to find current binaries in anonymous ftp archives; full-blown descriptions and discussions became ever more possible with HTML web pages and, ultimately, popular full-text WWW search engines).

A key feature of the Internet that made it possible to spark such waves of innovation was the fact that it was, essentially, a cooperative effort. Perhaps it was even a neighborhood. It was, therefore, reasonable to expect to have names and up to date contact information of the operators of hosts and networks – so that if any issues were detected, it was possible to contact the appropriate operator and resolve them. Thus, the "Whois" database was formed.

Spinning forward a decade, the Internet's commercial success and world wide popularity wound up attracting a wide range of less technical users, dependent on the network's stability for their livelihood. The cooperative neighborhood model no longer fit. Even the notion of "network operator" was stretched – because of their visibility in web addresses, common users (i.e., not technical operators) had registered millions of domain names, whether or not they ever themselves put a host on the network.

By 2000, there was a recognizable tussle between:

- The operational community's need to get access to reliable contact information for resolving network issues originating in remote networks (e.g., when there are issues in routing announcements)

- The law enforcement community's recognition of that information as a valuable source of information when tracking down criminal behaviour (e.g., Internet fraud schemes, or even non-network-based crimes)

- Trademark lawyers being asked to research and/or defend marks in the domain name system

- And the common user, who just wants a vanity name for their e-mail account or blog, and has privacy concerns (i.e., doesn't want to broadcast their personal coordinates to all and sundry).

At the same time,

- Registries and registrars would like to guard (domain name registrant) contact information as confidential customer information – providing completely open access to the information is an operational and commercial burden on them

- Spammers and other miscreants aim to mine the open whois databases for valid e-mail and physical addresses

- Some people use the whois database to update their holiday card mailing lists

- Yet others use it to find addresses to harass people

- And the Internet cuts across borders and philosophies – what is legal in one country is pursued by law enforcement agents in another

The original Whois technology cannot hope to address these issues. Indeed, there is no uniquely technical solution that will satisfy all parties.

However, there are some technological choices that can make it easier to implement the policies of access that are locally and globally defined to ensure the support of appropriate accountability of action (within the Internet).

The CRISP working group, within the Internet Engineering Task Force, developed the IRIS (Internet Registry Information Service) protocol, which is an open standard supporting decentralized storage of registry information (such as personal coordinates). It specifically allows tiered access, although the protocol is "policy-neutral".

What that means is that IRIS can be used to provide Whois-like information services, managed by individual registries and registrars, with access policies implemented to align with the global policies and/or local legal requirements. With authenticated access to the databases, the queries themselves are auditable and queryants are accountable.

As noted above, this does not provide answers to the thorny policy questions of access versus privacy. However, it does remove the technical implementation hurdle from the challenge of providing balance.

Ensuring "privacy by design": Can research help in reconciling the conflict between sharing personal information and safeguarding individual rights, in particular the right to privacy and the protection of personal data?

Yes, per the above – it's possible to implement more refined policies than access/no access. But doing so absolutely requires the pursuit of security credential and authentication technologies that can be established and managed with the flexibility needed for the whole real world. Some of that is advanced development – but much is needed in terms of research as well.

Can technical solutions help move forward with issues such as Whois?

Yes – see above.

Balancing law enforcement needs with freedom, privacy and business impacts: Anonymity can promote democracy and creativity. At what level do we need more traceability on the Internet for better law enforcement? What is the balance between law enforcement and freedom/privacy?

In order to continue to function and grow, the Internet requires accountability of its users. This is necessary in order to ensure it is possible to combat all manner of abuse found in the network today (or, in other words, not to turn the neighborhood into a squatted building). Certainly, with the upswing of "unwanted traffic" on the Internet, a subject that the IAB has been promoting as an issue requiring further exploration and understanding, it becomes clearer that there is a boundary beyond which technology cannot solve problems, and only policy & legal actions can take action.

What exactly accountability in the Internet means may vary from jurisdiction to jurisdiction. While there may reasonably be global policies established for what personal information must be made available in order to "put a host and pass traffic on the Internet", local variations on the appropriate use of that information will necessarily vary.

Discussion of the relationship between those global and local policies (and whether the Internet represents an independent state, with separate laws of appropriate behaviour) is a question for the legal and policy experts. From a technologist's point of view: we've demonstrated the power of the open, cooperative network; we can design and build deployable systems to support a flexible web of policies. Now, collectively, we must work to make those policies support (not hinder) the cooperative neighborhood of this century's global network.