The Future of the Internet

ICANN

Paul Twomey
President and CEO

9 September 2007

Media Connect Influence Forum
Hunter Valley, Australia

What I want to share with you today

- Brief introduction to ICANN – what it is and what it does
- My views on the future of the Internet
  - Its promise
  - Its challenges
- Some important challenges facing Australia if it is to play a role in that future
  - Broadband and the re-engineered economy
  - Building resilience against a worsening security environment
  - Importance of IPv6 readiness

ICANN mission statement

- To coordinate, overall, the global Internet's system of unique identifiers, and to ensure stable and secure operation of the Internet's unique identifier systems. In particular, ICANN coordinates:
  1. Allocation and assignment of the three sets of unique identifiers for the Internet:
     - Domain names (forming a system called the DNS)
     - Internet protocol (IP) addresses and autonomous system (AS) numbers
     - Protocol port and parameter numbers
  2. Operation and evolution of the DNS root name server system
  3. Policy development reasonably and appropriately related to these technical functions

Principles of Operation

- Contribute to the stability and security of the unique identifiers system and root management
- Promote competition and choice for registrants and other users
- Provide a forum for multi-stakeholder bottom-up development of related policy
- Ensure on a global basis an opportunity for participation by all interested parties

What do we stand for?

- Ensuring a single, interoperable Internet
- Providing a means for all to express their own language and identity, **but**…
- Providing access by all others
- Encouraging creativity, development, growth and innovation, particularly at the edge of the network
- Maintaining security of the network to ensure confidence in the model
- Ensuring stability of the experience for application development and consumer experience
- Deploying resources efficiently in support of a global network
- Ensuring all relevant stakeholders have a voice and role

Difficult to define what the Internet will look like in ten years, but…

- Usage limited by access to electricity – only 3 billion will enjoy a truly global Internet
- Many, perhaps most, will access by mobile devices
- Significant increase in broadband access (over 100 mb/sec) – developing countries adopting accelerated distribution programs
- Machine-to-machine Internet will overtake person-to-person Internet
- Billions of Internet-enabled appliances at home, work, in the car, in the pocket
- Third parties will be able to monitor all sorts of activities and utilities – washing machines to cars to electricity meters
- Geo-location and geo-indexed systems much more common and emergency services will be more precisely dispatched

Difficult to define what the Internet will look like in ten years, but…

- Significant improvement in spoken interaction with Internet-based systems
- Wider array of delivery methods for intellectual property (movies, sound tracks, books). VoIP will be prevalent with SIP the principal protocol for call setup. Voice communication will be essentially free except for calls terminating on PSTN devices, including mobiles
- Almost no industry will be offline – most will rely on the Net for customer interaction, customer discovery, sales, service, advertising, etc.
- Group interaction, collaborative support tools (including distributed games) will be very common.
- Internationalised domain names and much more multilingual Internet content

That Internet will allow us to . . .

- Manage appliances and home security online
- Make downloads an everyday practice – an natural extension of iPod/TiVo paradigm
- Talk to the Internet to search and interact – and it will respond
- Rely on more precise search systems through meta-tagging – moving toward semantic Web
- Key product/appliance maintenance histories to RFIDs or bar codes – one use of IPv6

What will the technical underpinnings of the Internet look like by then?

- Terabit-per-second local networking will be available – backbones for local nets
- Domain name system will operate in multiple language scripts
- IPv6 will be widely deployed
- Better confidentiality and authenticity through public key crypto – more authentication along the network
- Much more interdevice interaction, incorporating position location, sensor networks, and local radio communication
- Spam, phishing and denial-of-service attacks will continue a "cold war" arms race with defences and better authentication techniques
- Operating systems will continue to be troublesome sources of vulnerability

Continuing and new threats

- Spam and phishing
- Attacks on the domain name system
- Attacks at routing
- Fraud/IP spoofing
- Cyber espionage, cyber war, cyber terrorism, cyber protests

DNS infrastructure – future challenges

Threats

- Loss of service
  - Network outage
  - Machine or site failures
  - Overwhelming traffic (denial of service attack)
  - Business failure
- Hijacking
  - Cache poisoning
  - False registration
  - Fake zone transfer
  - Fake registrar-registry interaction
  - Private roots
- Loss of coherence
  - Unauthorised roots and TLDs
  - Private character set extensions

Countermeasures

- Excess capacity
- Distribution, replication
- Strong connectivity
- Multiplicity of businesses
- DDoS counters (long term)

- Protocol changes, DNSSEC
- Tight registrar controls
- TSIG (crypto)
- Crypto authentication
- DNSSEC

- DNSSEC, policy/political pressure
- DNSSEC, policy/political pressure

**Lots of work is under way. But threats are growing
and this will take more time and money than many expect.**

Consequences of that vision

- For Australia to gain the economic, social, and government services advantages promised by this future Internet
  - Near universal distribution of real broadband
  - Comprehensive approach to building resilience against cyber crime and cyber attack
  - Stakeholders — governments, ISPs, enterprises — must transition to IPv6, today's technology

Why near universal broadband deployment?

- Internet will continue to reduce costs in a global economy and drive innovation in delivery of private and public services
- Australia’s modern trading economy is based on swift uptake of information and communications technologies — which continue to evolve
- To participate in the future Internet, broadband speeds must be in the 100s of megabits per second

Why near universal broadband deployment?

- Debate must shift now from **how** to **why**
- Question: **Broadband for what?**
- Answer:
  - Revolution in delivery of private and public service to citizens and global customers alike
  - Rapid growth in video-based applications will be the foundation of more human-centric online interaction

Broadband will drive the re-engineering of Australia’s economic and social delivery systems.

Why build resilient networks and systems?

- April 2007 cyber attack against Estonia signaled a new battlefield ─ new strategies, new tactics, new players, new timelines
- New “cold war” is launched from a virtual world to cripple real world infrastructure
  - Botnet zombie armies can be used for economic, political, or terrorist purposes
  - Targets can range from Internet infrastructure to core enterprise systems to physical plants
  - Botnets are becoming increasingly sophisticated ─ one step ahead of the good guys

Why build resilient networks and systems?

- January 2007 trojan infestation – "Storm Worm" – attacked MS Windows OS in Europe and quickly spread to the U.S. and Canada
- In just 5 days, it accounted for 8% of all infections worldwide – between 250,000 and 5 million computers

Goal: To acquire and propagate a huge botnet capable of completely crippling targeted computers, systems, networks.

Why build resilient networks and systems?

- The real money lies in other, multi-purpose malware programs
- Phishing and keystroke loggers are most alarming
  - Collect personal and financial data for botnet herders
  - Herders auctions data to highest bidders or uses it to siphon cash from accounts
- Today's bots are programmed and managed by professional criminals and espionage agencies

Cyber crime no longer just about weekend hackers showing off.
It's big business.

State of readiness in Australia

- Australia could probably survive an Estonia-style attack
- But there is still much to do toward national preparedness
  - Federal agencies' work is under way, but . . .
  - Most Internet resources are in the private sector
- Estonia targeted financial services, media, retail, energy, wholesale, trading, and similar sites

Cyber crime and cyber attacks require a very broad-based response.

A new reality

- Government regulation and response is not the key to online security
- Coordination with a broad and deep private sector will protect our citizens and our economy
  - Education and engagement at all levels of business is a must
  - Our major banks have shown leadership – others must follow
  - Leaders must become involved – defence cannot be left alone to technicians and officials
- It's about resilience, which is achievable – not water-tight defences, which are not

Priorities in the face of cyber attack

- Coalitions of government agencies and industry sectors must practice war-gaming in domestic scenarios to prepare
  - – Exercises must include business and political leaders
  - – Clear messaging must be established
  - – Government and industry associations must work closely to understand and shore up vulnerabilities
- Estonia showed that technology is increasingly a conduit for action and reaction by the disaffected
- London’s response to the July 2005 bombings is a model

Why IPv6 readiness now?

- The unallocated pool of IPv4 addresses will exhaust within 3 to 5 years
- However, IPv4 will not disappear any time soon
  - No set cutoff date for IPv4 address block allocations
  - Both IPv4 and IPv6 will run in parallel for the foreseeable future
  - Reintroduction of unused IP addresses is being explored

Why IPv6 readiness now?

- But besides supporting continued Internet expansion, IPv6 will
  - Allow every machine or device to have its own IP address
  - Allow for very high bandwidth networks
  - Open the door to next generation devices
  - Enable better connectivity worldwide
  - Increase real-time data retrieval and transmission
  - Help enterprises/other entities gain an understanding of new technology sooner rather than later

Where we are now

- Pool of unallocated IPv4 addresses will be fully distributed in 3 to 5 years
- Perception as merely a technical issue – and disagreement within the technical community – have slowed movement to IPv6
- Now, many organisations and governments are stressing its importance publicly

What remains to be done

- Five Australian groups that can and should move toward adopting IPv6
  - Federal/state governments must revisit policies to encourage IPv6 adoption
  - ISPs must offer IPv6 transport services and require vendors to supply IPv6 capable equipment
  - Enterprise CIOs must plan IPv6 transition now
  - Vendors must continue to develop fully capable IPv6 devices compatible with IPv4 standards

Conclusions and observations

- The Internet is the most powerful and pervasive technology for empowering individuals
- It is part of the glue which ensures a rapid unleashing of humanity's knowledge and possibilities for all persons no matter what age, sex, creed, class, ethnicity or – at least to some degree – wealth
- It is radically reducing transaction costs and barriers to markets across a globalised economy
- Stakeholders across the board must continue to preserve and strengthen this model

Thank You

www.icann.org