Submission No 77

Inquiry into potential reforms of National Security Legislation

Organisation: Dr Paul Scully-Power AM

The New Internet Protocol Numbering System and its implications for Civil Society: Government Regulation Is Needed

Background: Internet Protocol (IP) addresses, the numbers that are integral to sending and receiving messages over the Internet, are assigned for use by a central authority, the Internet Assigned Numbers Authority (IANA). By coordinating these unique identifiers globally, IANA ensures a viable global Internet. This critical function was originally performed under a U.S. Government contract to IANA, but is now self-administered by the Internet community.

In turn, IANA delegates the actual responsibility for management and allocation of IP number resources to five continent-sized Regional Internet Registries (RIRs). Part of the responsibilities of the RIRs is to maintain a definitive regional directory of the IP addresses that they allocate.

These addresses function as the unique identifiers of specific devices connected to the Internet, together with the routing instructions that allow for the accurate and timely delivery of communications between those devices. The global Internet community has, since the beginning, consistently adopted policies that IP numbers are not property to be sold, but are “loaned” freely for use to those who have a demonstrated need. This granting of 'right to use', not 'ownership', has a well-established set of protocols that are subscribed to by all users and these protocols also protect the privacy of the individual.

With the success of the Internet, the 4.3 billion of originally available IP addresses, called Internet Protocol version 4 or ‘IPv4’, has been exhausted at the IANA level, and several RIRs that still have the last of these numbers will be issuing them in the near term. In Australia new IPV4 supplies have been unavailable from the Asia Pacific registry (Brisbane based APNIC) since 2011.

Hence the Internet Engineering Task Force (IETF) has devised a new protocol, called Internet Protocol version 6 or IPv6, which enlarges the pool of IP numbers from 4.3 billion to 2^{128} (or 3.4×10^{38}), i.e. 340 billion, billion, billion, billion. To gauge the size of this gigantic number, there are only about 4×10^{22} stars in the universe, i.e. there are 10 million billion IPv6 addresses for every star in the universe.

Hence the world will not run out of numbers again for a long time, perhaps for centuries or longer, but this new system creates other policy issues that must be addressed.

Issues

Issue 1: *Internet Protocol numbers should not be treated as ‘property’ but exclusive rights to use*

The global supply of unissued older protocol IPv4 numbers ran out in 2011. Hence issued but currently unused IPv4 numbers have become valuable for the first time and there have been sporadic recent attempts to sell the right to use these blocks of addresses, sometimes in accord with or sometimes in contravention of, ‘transfer’ policies maintained by the RIRs. If transferred in contravention, those addresses would no longer be accurately registered with a central authority and the structure of the Internet would have been violated. They would have become 'black' addresses.

Moreover, designating such blocks of addresses as “property”, rather than as having the exclusive rights to use conferred – ownership rights rather than exclusive rights to use – would contravene existing understandings and undertakings of IANA and the RIRs and would create de-aggregation concerns that could slow the Internet significantly.

Such “ownership” would fundamentally and irrevocably change the architecture of the

Internet, place its operation and sustainability at considerable risk, and potentially allow a two-tier Internet with the concomitant opportunity for criminals, fraudsters, hostile foreign governments, hackers or terrorist groups (not to mention illegal spam houses) to operate with complete anonymity in the 'black' parts of the Internet, so long as some ISP's (Internet Service Providers) would be willing route such traffic.

Issue 2: The Need To Avoid *Corruption of the Whois Database of Internet Protocol Numbers*

With the current change over to the new IPv6 address system, the vulnerability to losing the accuracy of the IP address registration system known as the Whois database becomes a serious issue. The standard IPv6 assignment to each ISP is over four billion[1] addresses at a time -- more than the entire global IPv4 number pool. There is no meaningful commercial incentive, or indeed any legal or regulatory compulsion, for any ISP to report further sub-distributions within the enormous IPv6 block given to it. Thus the "allocation based on need" self-regulation of the Internet has dissolved and the database of assigned numbers could be rendered far less useful because many ISP IPv6 number recipients, unlike IPv4 recipients, will not likely ever return for more numbers.

There is therefore a substantial risk that this will create large blocks of unknown delegated addresses, or 'black holes' in the Internet. This will erode the ability to trace Internet addresses, which in turn will impact law enforcement agencies as well as banks, Internet commerce, and private citizens. Indeed if private citizens ever lose trust in the Internet either by ID theft, bank account theft, privacy violation or general commerce fraud, the whole structure of the Internet could unravel, confidence in the Internet could evaporate, secure transactions could be undermined, normal Internet operations placed in jeopardy, and the global Internet thereby reduced to a lawless society.

This can only be obviated by applying the same standards to the Internet as apply to civil society, namely the ability to identify and punish those who commit crimes or engage in civil offences as defined by the law.

Hence each IP address needs to be identifiable in cases of suspected criminal or unlawful civil activity, which can only be achieved by a reliable and up to date registry of Internet numbers. This will place a burden on ISPs, but no more so than currently exists -- and that the ISPs imposed on themselves in self-government with the RIRs, together with the extant privacy rules pertaining thereto.

ISPs obtain close to free allocations of internet protocol numbers from which they can profit by further allocation to their customers, so it is not unreasonable to insist that they keep accurate and up to date records of IP numbers if only to ensure that they are fully recompensed for the services provided and to ensure the integrity of the Internet in the interests of the community.

Resolution: Currently the data from ISPs related to usage of numbers is publicly available for free in the Whois directory, the Internet equivalent of the phone directory. This public Whois data has been a critical resource for law enforcement and counter-terrorism agencies as well as the commercial sector of the economy (to prevent counterfeiters from stealing music or movies, for example), but keeping it updated has been a "side effect" of the documentation of need for the allocation of IPv4 resources.

---

[1] The RIRs allocate to each ISP a large number of IPv6 network prefixes/identifiers. Each network prefix can serve all of the IPv6 devices (e.g. RFID devices) ever made, and ISP's are encouraged to assign each organization 65,536 network prefixes. This large allocation block was specifically chosen by the IETF to ensure a speedy Internet -- any further de-aggregation would slow Internet performance.

Because IPv4 numbers were “scarce” they were only issued based on demonstration that previous allocations were used and hence further allocations were needed.

While these same stewardship and conservation policies apply for IPv6, the size of the IPv6 address space being issued is so large that on a practical basis, ISP carriers could choose to be decades behind in updating their information, as they will not come back to the RIR every few months, or years, for new numbers, a time when such records are traditionally checked and reviewed. The future IPv6 Whois directory will not be effective unless enforceable standard-making activity occurs to call it into being.

The fundamental problem is that there are no current legal or regulatory requirements in Australia (as opposed to a policy requirement by the regional registry) for ISPs, and others receiving allocations of IPv6 numbers in bulk through delegation to the next level, to timely create a similarly granular database of their delegations, data essential for example to law enforcement. But properly authorized law enforcement, counter-terror or civil investigations will be hampered without such data being available in a quick and accurate manner.

This will require national and international efforts to agree on the requirements for assigning Internet addresses that maintains and ensures the integrity of an accurate Whois database while protecting individual privacy through updated and enforceable policies for ISPs in conjunction with RIRs. Otherwise cyberspace will become the new Wild West with lawlessness, crime, and a safe haven for unlawful perpetrators.

A suggested regulatory framework to ensure the rights of civil society is attached hereto (Annexure A), together with an explanatory memorandum (Annexure B).