Contributions from ICANN on Privacy & Security Implications of the Internet of Things

31 May 2013

The Internet Corporation for Assigned Names and Numbers (ICANN) respectfully submits these comments in response to the US Federal Trade Commission's public comment inquiry on the Privacy and Security Implications of the Internet of Things, http://www.ftc.gov/opa/2013/04/internetthings.shtm.

About ICANN

ICANN is a global organization that facilitates the security, stability and resiliency of the Internet's unique identifier systems through coordination and collaboration.

Within its technical mission, ICANN's security, stability and resiliency role encompasses three categories of responsibilities:

- ICANN's operational responsibilities (organizational risk management of internal operations including L-root, DNS operations, DNSSEC key signing operations, IANA functions, new top-level domain operations, Time Zone Database Management);
- ICANN's involvement as a coordinator, collaborator and facilitator with the global community in policy and technical matters related to the Internet's unique identifiers;
- ICANN's engagement with others in the global Internet ecosystem.

Further information can be found at icann.org.

Comments

The FTC announcement from 17 April 2013 indicates that inputs received will be used to support a public workshop in November 2013 regarding the Privacy and Security Implications of the Internet of Things. ICANN wishes to bring to the FTC attention that these issues are already being examined in multistakeholder fora. Before commencing a parallel effort, the FTC may wish to review and consider participating in these ongoing multistakeholder discussions.

The Internet Ecosystem

The Internet is now an essential enabler for global knowledge and information exchange, commerce and governance. UNESCO Vancouver Declaration, September 2012 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_en.pdf) and WSIS+10, Toward Knowledge Societies for Peace and

Development, Final Statement, 27 February 2013 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf).

The Internet is recognized as fundamental for supporting the world's economy and sustainable development (see OECD Internet Economy Outlook 2012, http://www.oecd.org/sti/interneteconomy/ieoutlook.htm).

The Internet serves as a platform for a diverse range of devices, networks and systems. The "Internet of Things" will grow that number by a huge scale and with a global impact.

The Internet is successful and thriving because its ecosystem is open, transparent, interoperable and collaborative. ICANN supports the study of Internet policy issues within the context of multistakeholder fora to sustain a healthy, sustainable, resilient Internet ecosystem. The existing ecosystem contains a broad network of organizations and communities. These organizations and communities work together and in their roles.

The Internet Ecosystem is made up of a number of organizations and processes that shape the coordination and management of the global Internet and enable its overall functioning. These organizations include: technology and engineering organizations, network operators, resource management organizations, users, civil society, commercial and non-commercial entities, educators, policy-makers, law enforcement and governments.

Unique Identifier Systems in relation to the Internet of Things

An examination of the privacy and security implications of the Internet of Things relates to the existing unique identifier systems and protocols that will provide the underlying platform to support the Internet of Things. The technical community expert in these areas is already actively considering privacy and security issues in other fora.

Conclusion

Discussion of issues related to the Internet of Things, including privacy and security implications, should be conducted in a multistakeholder, collaborative environment. Before commencing a parallel effort, the FTC should consider joining in existing efforts to understand the implications on the privacy and security of the Internet of Things.