**NCSG Comments on the ICANN Privacy Policies**

During the NCSG meeting with the ICANN Board at ICANN 49 in Singapore, we made the observation that it is time ICANN had a proper privacy policy which covered all of its personal data collection, use and disclosure. Different provisions of what ought to be in a comprehensive policy are scattered in various places (eg. a web policy, a new Gtld policy, data retention provisions in the 2013 RAA) but it is our view that this is not a comprehensive policy such as is expected in 2014. It is not suitable for a global organization such as ICANN, which has a leadership role in shaping the Internet as a bottom-up, multi-stakeholder organization, to not explain comprehensively how it seeks to comply with not only the various data protection laws which affect its operations and the lives of its stakeholders, but expected norms of Internet policy leaders. In our comments to the *Status Update Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service* we indicated that we think it is time to develop a set of Binding Corporate Rules for the entire ICANN ecosystem, in order to set a high standard for respect for privacy. These comments on existing policies should be read as a first step in our efforts to help develop those higher standards in respect for privacy.

**Framework for Analysis**

There are many purposes for having a privacy policy.

1. A document which gathers all privacy practices in one place is the clearest, most transparent way to develop trust in the clients, partners, users, or stakeholders of the organization, that their personal data is being protected.
2. A full disclosure of management practices helps implement various compliance requirements under data protection law, such as notice, transparency, provision of information about how to access and correct personal information, and notice of any appeal mechanisms.
3. One document that focuses on management practices, (as opposed to a public relations piece which gushes on about how much the organization cares about your privacy), will provide a platform for staff training. This can then easily be supplemented with further information for staff as to how to actually implement the promised protections
4. Having a set of management practices formatted around generally accepted legal principles enables good qualitative and quantitative metrics for performance measurement.

There are numerous models for drafting privacy policies:

1. The 1980 Organization for Economic Cooperation and Development (OECD) Guidelines: <http://www.oecd.org/sti/ieconomy/privacy.htm> Note that these guidelines have been significantly updated in 2013, with elaboration of accountability and global data flow management. The following countries are members: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.
2. The Council of Europe Convention 108: <http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA%282014%2901_En_%20Working%20doc_Convention_108.pdf>. At the moment, the Convention originally drafted in 1981 is under revision, the link we cite is the current working document available online with the proposed changes.
3. European Union draft Regulation: <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_dp_plenary_vote_140312_en.pdf>. The EU is revising its 1995 data protection directive, which required members states to enact data protection law to give effect to the Directive, and replacing it with a single Regulation which will apply to all member states, and will require non-member states who process personal data to meet higher standards. While this regulation has not been passed by the EU Council of Ministers, the EU Parliament has voted overwhelmingly in favour of the Regulation and the Directive as of March 14, 2014. The text of the draft Regulation is available here: <http://eur-lex.europa.eu/legal-content/en/ALL/;jsessionid=DhLMT7WLLDTJ7Qd9jzkFwHgBHSL1HFh9RgJlDCpR2Gm11Kyg0hlJ!-213175582?uri=CELEX:52012PC0011>
4. Information concerning binding corporate rules, a method for companies wishing to transfer personal data from EU countries to states without adequate data protection, is available here <http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm>
5. The Asia Pacific Economic Cooperation (APEC) privacy framework and principles are available here: <http://publications.apec.org/publication-detail.php?pub_id=390> These principles are based on the OECD Guidelines, and the following 21 economies are members of APEC: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, Viet Nam.
6. Canada drafted a quality standard, and attempted to introduce it at ISO. This standard CAN/CSA-Q830 Model code for the protection of personal information is the basis for the Canadian private sector legislation (available at <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/>) , and provides detailed instructions for developing a privacy code. Since it is easy to follow, was based on the OECD Guidelines with additional detail, is accepted as adequate by the EU, and was one of the inputs to the APEC Guidelines, we propose to use its principles to analyse the ICANN privacy documents which we have found.

**Principles Necessary for a Privacy Policy**

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

**Process for Analysis**

A common first step in doing a privacy review of an organization, is to map the personal data which is collected, used and disclosed by the organization. First the data elements under the control of the institution are compiled, then they are mapped in terms of data flow and touch points within the organization. This is how most organizations manage a review of where the risks are, whether security safeguards are adequate, and whether staff training is up to date. The NCSG is curious as to when the last review/audit of ICANN personal information handling practices was conducted, and what training has been done.

Based on the knowledge that we have as stakeholders, and without the benefit of detailed conversations with those who actually manage data within ICANN, here is a list of data collected, used and disclosed within ICANN. Please note that we understand that ICANN is an extremely transparent organization which expects participants and stakeholders to consent to the release of a great deal of otherwise personal data, in the interests of transparency and full interaction, but this fact does not release ICANN from an obligation to figure out what data it controls, and map it.

1. Personal data of staff, including resumes, staffing information, salary information, banking data, health data, travel data, identity card information and records of movements tracked by such cards and through video surveillance, any data tracked through information processing equipment such as computers and smart phones, remote employment data (i.e. working from home), performance management data, staff relations data, voice recordings of interactions with stakeholders, any information related to Ombudsman investigations which is in ICANN control through its control of the Ombudsman, etc.
2. Personal data of stakeholders who participate in committees, including resumes, applications for positions on committees, travel data, tax data, voice recordings of interactions with stakeholders, any information related to Ombudsman investigations which is in ICANN control through its control of the Ombudsman, etc.
3. Personal data of users of the websites, including any transactional data acquired through the use of cookies and other web tools, any mailing lists, participation in meetings, webinars, or consultations, etc.

Through its role as a data controller (see the definitions of data controller agreed by the EU Article 29 Working Party <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> , and that agreed by the APEC member states[[1]](#footnote-1)), ICANN directs the collection, use, retention and disclosure of personal information of all domain registrants, of actors in UDRP disputes, and in the application for and dispute resolutions surrounding new gTLDs. Every contract that sets out requirements for data collection, use, disclosure and retention is an enactment of data controllership, and therefore this should be accounted for in a privacy policy. While we have not done a comprehensive review of those contracts and arrangements, we clearly see the following major data collection activities:

1. Pursuant to the 2013 RAA, a series of requirements for the collection, verification and disclosure of registrant information in the WHOIS.
2. Pursuant to the 2013 RAA, a series of requirements for the retention of a more complete set of data elements including IP address metadata, and transfer of the dataset to an escrow agent, for the purposes of potential law enforcement access.
3. ?
1. The APEC privacy framework is widely regarded as a less stringent standard than the EU data protection laws and Directive 95/46, but even it defines a data controller as follows: “10. Personal information controller means a person or organization who controls the collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual’s personal, family or household affairs.” (<http://publications.apec.org/publication-detail.php?pub_id=390>, p.06) [↑](#footnote-ref-1)