Has the EWG Evaluated Closely What is at Stake for Registrants?

As trumpeted at the ITU meeting in Dubai, and on news programs across the globe, the Internet is the greatest form of communication known to mankind – a link across individuals, organizations and companies that can help bring down dictatorships, bypass state-controlled media and allow individuals to communicate the most interesting and controversial ideas directly to each other.

I. Privacy is a Human Right

As has been shared at ICANN since its founding, privacy is a human right firmly rooted in the United Nations' Universal Declaration of Human Rights (UDHR), and it states, in Article 1, that ***"all human beings are born free and equal in dignity and rights."*** The UDHR specifically protects privacy in Article 12. Furthermore, the United States, European nations, and almost all of the governments that participate at ICANN, have signed and ratified the International Covenant on Civil and Political Rights (ICCPR), which codifies the Universal Declaration of Human Rights, including Articles 17 (privacy) and 19 (freedom of expression).

Article I of the 1948 American Declaration on the Rights and Duties of Man, articulates the right of every human being right ***"to life, liberty and the security of his person."*** Article IV declares ***"the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever."*** Above all, Article V notes ***"the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life."***

In Latin American nations, there is a recent trend towards data directives, and in the case of Argentina, Peru, Colombia, and Mexico, these nations have enacted data protection laws. Similar guarantees exist in the 1969 American Convention on Human Rights (Art. 11), and the 1950 European Convention on Human Rights and Fundamental Freedoms (Art. 8). The European Union Data Protection Directive (95/46/EC) of 1995 addresses the collection and disclosure of personal information. The Directive has been enacted into national laws by the 27 member states.

Articles 1(1) of the Directive states that member states ***"shall protect the fundamental rights and freedoms of natural persons, and …their right to privacy with respect to the processing of personal data."*** According to Article 6, member states are obliged to handle personal data lawfully, collected for specified, explicit and legitimate purposes, having regard to the purposes for which they were collected, and appropriate safeguards for personal data stored for longer periods.

This protection is further enhanced for the 47 member states of the Council of Europe in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1980, and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 2001. Human rights are also recognized in the constitutions and other legal acts of nation-states around the world. These documents demonstrate a worldwide consensus on the existence of the universal right to privacy.

II. The Internet is the Greatest Avenue Ever Created for Minority Speech

That the Internet has become an avenue for minorities to communicate ideas is clearly known. Those who felt they could easily communicate ideas in person – because their religion is a minority in their region, because their political ideas are a minority in their state, or because their ideas off challenge and competition to those bigger and pre-existing, now have an avenue in the Internet for communication, cooperation and challenge that never before existed.

And people, governments, companies, and attorney want to stamp them out. Oppressive governments want to arrest the leaders of movements that want to challenge their leadership, even those seeking more human rights and democracy. Oppressive companies want to find and drive out of business new and small businesses with ideas that rival, challenge and threaten marketshare. Many seek to seize pithy domain names, without a legal basis, but through threats and intimidation.

The ability of the world to come knocking on an individual, small organization or small businesses' door to contend, confront, accuse,

threaten, harass and object has been the direct result of the publication of data in the gTLD Whois databases. Never before has such an inequity existed – because traditionally names and addresses are not associated with speech. Traditionally political ideas (by individuals or organizations) are published with the name of the organization – not the place you can throttle the organizer.

Pamphlets, brochures, signs worldwide traditionally trumpet the ideas, but not the physical location of where those ideas originate – a right and protection embraced by the US Supreme Court in 1995 in McIntyre vs. Ohio Elections Commission, citing not only US law, but a worldwide tradition of writing our most dramatic and world-changing ideas under anonymity or pseudonyms to allow the idea to percolate and disseminate before the writer was burned at the stake (literally or figuratively).

It is this ability to disseminate ideas without direct connection to our home addresses, our organization's small offices, the location of our children, spouses and parents that has allowed such an array of political, religious and personal ideas to proliferate in the 20th and now 21st century. The Internet is every man (and woman's) printing press and the ability of so many to help, support, cajole, implore, expand, challenge and inspire has opened new worlds, new ideas and new opportunities in every region of the world that the Internet hits – which is every region of the world.

III. Privacy and Speech Protections Must be Built Into a Streamlined, Minimized Set of Whois/Directory Data Upfront – Because Persecuted People have a Very Hard Time Seeking Remedies After-the-Fact.

It is absolutely critical that the entire system of the Whois/Directory Services system be designed upfront – not for law enforcement but for Registrants! The privacy and protection of Registrants, the customers and huge base of the ICANN pyramid and system, must be of paramount and primary importance to the EWG work.

Registrants are not "guilty until proven innocent," and the unbounded uses to which Registrants have put domain names has changed the face of

the world, the leadership of countries, the actions of militaries and expanded the freedoms of millions.

We do not see within the EWG work the deep understanding and appreciation of the Internet as the greatest form of communication ever created, and one in which speakers are threatened by virtue of the very communication they are sharing. The Whois/Directory Service must protect, not expose, those who use domain names for personal, political, religious, ethnic, racial, robust and challenging speech, and protect (through lack of collection of data) groups that include:

- Synagogues located in areas in which Jews are persecuted minorities that seek only to publish the times of their services, but where the synagogues have been removed from the local maps as repeated targets of bombings. (Why should collection, storage and publication of physical address be the price for making information about their services available?)

- For Mosques in US states with populations not pleased with local Moslem populations and where the mosques are hidden from easy view of public streets (same questions as above: why should their threat level and fears be raised because they have shared the times of services or lessons online?)

- For organizations that foster ideas now, and in the future, that challenge the standard thinking of tribal leaders, local City Councils, regional governors and national leaders

- For women's groups around the world seeking to bring education and employment to women where well-armed groups seek neither (and whose leaders, old and young, we know are targets of attack)

- For gay and lesbian organizations who seek to continue to fight for their rights without identifying the physical location of their members to face the physical violence that has haunted this movement for years

- For small businesses and entrepreneurs that seek to challenge the IBMs, Time Warners, Estee Lauders and Facebooks of the world with new ideas, alternative technologies and who seek not to be eliminated in their infancy by threats, intimidation or unfair competition (much easier when you know the physical address of the entrepreneurial founder and where her children live).

Domain names are the street signs of the Internet – the guide to where content might be found – be it websites, listserves, emails and more. The person who posts the street signs has never before had to autograph it with her/his physical address, phone number, IP number, email and more. That should not be the case now.

IV. Our Hopes for the EWG

We expect more from the EWG. We hope that you will rise above the interests of individual companies and constituencies to give us a new vision:

- ***of less information***
- ***of information tailored for the needs of the infrastructure, not the needs of the content police (public and private), and***
- ***of contactibility (the goal set by the Whois Review Team), not reachablility and potential arrest and harassment for any type of message and content online.***

Thank you!