INTA Response to United Nations High-level Panel on Digital Cooperation (UNHLP) Call for Contributions Submitted January 31, 2019

I. Values & Principles:

a) What are the key values that individuals, organizations, and countries should support, protect, foster, or prioritize when working together to address digital issues?

Safety and trust, decent work and economic growth, innovation, fair competition and secure infrastructure should be the priorities for digital cooperation. The digital world should not unduly expose anyone to threats against their physical or economic safety. Among many facets of digital safety is the need to protect consumers from the many forms of fraud and abuse. Emails, websites, texts, or social media posts may seem to originate from trusted, legitimate companies by fraudulently using their names and logos. They may seek personal information, or they may invite the user to take action that will install malicious code (malware) that can disrupt or collect data the user's digital environment. In addition, these deceptive spoofing, phishing, and spamming practices can lead to identity theft and extortion.

The U.S. Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center received more than 1.4 million complaints between 2013 and 2017, and a total reported loss of $5.52 billion due to internet scams. (See Reference 1) In a 2016 alert, the FBI reported that in less than three years, losses from emails purporting to be from employers resulted in $2.3 billion in losses. (See Reference 2) The South African Financial Intelligence Centre (FIC) revealed that criminals are increasingly targeting South African internet users with multiple scams. According to its report, scammers target young people with higher-level qualifications by offering employment and jobs on the internet that do not exist. (See Reference 3)

Fraud can also take the form of counterfeits and pirated goods that are offered for sale online using trademarks of trusted and legitimate companies. Counterfeit pharmaceuticals and supplements may contain ineffective and/or affirmatively harmful or poisonous ingredients. Counterfeit electronics may not be properly assembled or tested. Counterfeit tires and light bulbs may explode. Counterfeit toys may contain harmful substances, and pose pinching, choking, and strangulation risks. The value of global trade in counterfeit and pirated goods in 2015 was estimated at $1 trillion and costing over 2.5 million jobs per year. (See Reference 4) This is a marked increase from 2013, in which the estimated value of global trade in counterfeit and pirated goods was calculated at $710-917 billion, and the wider economic and social costs was calculated at $717-898 billion, including fiscal losses, costs of crime, and displacement of legitimate economic activity. (See References 5 and 6.) (In 2022, the total estimated value of counterfeit and pirated goods including digital piracy is projected to reach an astounding $1.90 -

$2.81 trillion. The number of jobs lost due to counterfeiting and piracy is expected to reach upwards of 5.4 million jobs in 2022. (See Reference 4) As reported by UN Office of Drugs and Crime, counterfeit goods pose global dangers. They are typically produced in violation of environmental standards and fair labor practices, and often by organized crime, which may use the proceeds from, and routes established by, counterfeit goods trafficking to also traffic in humans, illegal weapons, and drugs. (See Reference 7) Fraudulent offers for services, such as education degrees and charitable services, may also rely on fraudulent uses of the trademarks of known and trusted organizations, like universities and charitable organizations may result in economic fraud, as well physical danger and human trafficking. (See Reference 8) Consistent with the value of safety, the digital world should serve, not burden, consumer protection; it should not enable or empower unlawful content; and it should not diminish the effectiveness of current laws. In terms of decent work and economic growth, intellectual property, is a key value generator for businesses. By building consumer confidence, trademarks allow businesses to emerge and grow, facilitating social and economic development. Small businesses have unprecedented opportunity for growth by increasing their integration into value chains and markets through digital technology. In most digital transactions the user is limited to whatever two-dimensional information a vendor chooses to convey. Therefore, the ability to protect trademark names and logos takes on increased importance, as these are the primary indicia consumers have to assess the trustworthiness of vendors online. Sustained growth and continued innovation require a scaffolding of reliable trademark enforcement mechanisms so that customers can rely on trustworthy innovators without being deterred and defrauded by bad actors.

Organizations and countries should support systems that foster and enforce justice; lawful and fair competition flourishes best if unlawful, unfair competition is monitored and penalized. Most countries have regulations against unfair competition. (See Reference 9) The digital world, by its geographical and multidimensional scope and its relatively low cost of entry, increases the need for fair competition standards that are easily understood, implemented, and enforced. Means of obtaining protection against unfair competition and enforcing rights should not unduly burden small businesses, and rules should apply equally regardless of economic status or gender. A digital economy requires infrastructure that enables personal information to be exchanged safely, without unwanted capture or misdirection of the information, and reliably, without distortion of the information or undue delay. To distinguish the intended and desired recipients of information from others, and to trace the source of fraudulent, unlawful information, harmonization of digital identification practice is necessary. While this must be balanced against legitimate privacy rights, the banner of privacy should not shield criminal activity or allow fraudulent uses of identification.

b) What principles should guide stakeholders as they cooperate with each-other to address issues brought about by digital technology?

1. Transparency and open access. The deliberations and determinations of standard setting organizations should be accessible to all through digital means and easily accessible

reporting. Those able to contribute with ideas and perspective should have the necessary channels to do so, but they should accurately identify the interests they represent.

2. Collaborative and inclusive regulation. The practical experience of digital platforms and brand owners should be accounted for, as well as the needs and interests of consumers and vulnerable populations.

(c) How can these values and principles be better embedded into existing private and/or public activities in the digital space?

1. Mechanisms should be added or supplemented to better and more uniformly support trademark protection and enforcement to maximize speed of results with minimal cost and inaccuracy. This is necessary to reduce the kinds of fraudulent activities that violate digital user safety, to protect consumer trust in legitimate companies, and to enforce fair competition, all of which, in turn, foster innovation and growth. These include:

(a) Evaluate national trademark registration systems to ensure accessibility (for example, through online mechanisms and low-cost fees) and equal treatment of applicants.

(b) Create uniform dispute resolution systems for unlawful trademark uses on website pages and social media;

(d)Acknowledge the importance of transparency in the ownership of domain names and ensure that exceptions are built into regulatory models to ensure an open registrant directory system at global, regional and national levels. Consumers, brand owners, and law enforcement are all hindered in their efforts to prevent deception and seek redress if the true owners of websites engaged in commercial activity are cloaked in secrecy.

2. Public education about digital fraud should be globally accessible (in local languages and through local means) and targeted to reach everyone, including the very young, teenagers, workers, and the elderly. The messaging should be age-appropriate and broadly address digital fraud, including:

(a) The means of digital fraud and deception (such as spam, spoofing, phishing, pharming, and offers for counterfeit, pirated, and fraudulent goods and services);

(b) The harms digital fraud creates to the direct victims of the fraud (losing money, getting inferior or dangerous products, identity theft, blackmail, possible physical harm, capture, or death) as well as others (labor and environment violations, supporting trafficking of illegal weapons, drugs, and people, loss of jobs, reduced incentives for innovation in technology, arts, music, and literature);

(c) Tips for best avoiding digital fraud; and

(d) Resources for victims of digital fraud, including local and national law enforcement, legitimate brand owners, and financial institutions.

II. Methods & Mechanisms

a) How do the stakeholders you are familiar with address their social, economic, and legal issues related to digital technologies? How effective or successful are these mechanisms for digital cooperation? What are their gaps, weaknesses, or constraints? How can these be addressed?

There are a number of methods for protecting and enforcing trademarks and stopping untruthful statements, each having its own benefits and drawbacks. Some methods have improved over time, others have become less effective. In some countries trademark rights are obtained through use alone, although this option is subject to uncertainty of geographic scope, strength, and validity, as well as proof challenges. Commonly, trademarks are protected through registration. The protection offered by many trademark registrations is limited to the country in which they are obtained. As such, individual trademark applications are typically filed in each country in which protection is sought. However, there are initiatives that enable trademark owners to cover multiple countries with a single trademark application. For example, the European Union Intellectual Property Office is the official name for the European Union's (EU) trademark office, where a registered EU trademark or Community design is valid in all member countries of the European Union. Africa offers a similar filing alternative through the Organisation Africaine de la Propriete Intellectuelle (www.oapi.int) (See Reference 10)

It is also possible to file a single international trademark application to obtain registrations in multiple countries under the provisions of the Madrid Agreement or the Madrid Protocol, further reducing the complexity and costs associated with obtaining trademark protection in multiple countries. (See References 10 and 11) (http://www.wipo.int/madrid/en/index.html). Both treaties permit an international trademark application to be filed with the trademark office in the home country in a single language. Other benefits of an international trademark registration include the ability to transfer the rights in all of the covered countries through a single assignment of the registration (assuming the assignee is in a member country) and the ability to renew the registration through a single filing. It is also possible to designate additional countries after the application is filed. There are over 80 countries that can be designated in an international trademark application under the Madrid Protocol. These countries are located primarily in Asia and Europe, but other notable countries are Australia and the United States. (See Reference 10) On the whole, the Madrid Protocol facilitates protection at a reasonable cost.

In terms of trademark enforcement, many reputable, larger companies provide online forms to identify wrongful trademark (and copyright) uses by vendors and quickly disable them. Once the infringement is identified, this procedure is relatively quick, low cost, and effective for stopping a particular use. Another enforcement method is to send a demand letter. This method depends on the ability to accurately identify contact information for the infringer. With WHOIS directories no longer providing easily accessible information for domain owners, this has become more difficult. In addition, sometimes the infringing offer is made through an ad serving agency and the contact information for the advertiser maybe be difficult or impossible to identify. If the infringer is identified, usually an attorney is retained to prepare and send the letter. This may result in quick success, a prolonged exchange of letters, or futility. Demand letters thus

have varied results in terms of effectiveness, efficiency, and cost. Lawsuits are typically the most reliable method for obtaining relief on meritorious complaints, but they are also the most time consuming and costly. A single trademark claim may take many years and multiple trials to resolve. Lawsuits are inefficient as they divert resources and introduce business uncertainty. Lawsuits are not often a feasible option for small businesses, and typically strain all but the most well-funded companies. They rarely provide final relief within less than a year and usually are contingent upon identifying the infringer and obtaining jurisdiction over it.

Domain Name Dispute mechanisms like the Uniform Domain-Name Dispute-Resolution Policy (UDRP) and Uniform Rapid Suspension (URS) are also useful tools. Envisioned as a quicker and less-expensive alternative to litigation concerning disputed domain names the UDRP allows trademark owners to have a disputed domain name canceled or transferred by an appointed panel. The UDRP offers a determination within 14 days of the panel's appointment, absent extraordinary circumstances. The base fees range between $500 and $7,100, depending on the location and service. (See References 12 and 13) The UDRP offers a relatively quick means of stopping domain name infringement for those are sophisticated enough to know about it and well-funded enough to move against multiple infringing domain names. The UDRP is an example for a well thought, negotiated compromise to solve a problem that transcends borders. The URS is another domain name dispute procedure, designed to be faster and cheaper than UDRP, offering a determination within 3 business days and no later than 5 business. However, the URS has a more limited scope than the URDP and a higher burden of proof. It also does not facilitate the transfer of an infringing domain name. It merely suspends it for a limite amount of time. The URS is also the result of community compromise but is not utilized as much as the UDRP given the limited scope of the remedy.

Other means of alternative dispute resolution may be used to address fraudulent uses other than in connection with domain names. These typically require an agreement between the parties to engage in the ADR and payment of private arbitrators. This mechanism can be effective, but because it requires a binding agreement with the infringer to participate in ADR, usually only large, sophisticated companies are in a position to use this as a viable alternative to litigation.

b) Who are the forgotten stakeholders in these mechanisms? How can we strengthen the voices of women, the youth, small enterprises, small island states and others who are often missing?

The enforcement mechanisms discussed above tend to best serve large, sophisticated global companies with ample resources to devote to monitoring and enforcement. It is difficult for small or unsophisticated enterprises without adequate legal counsel and financial resources to efficiently enforce their trademarks. This "enforcement gap" may diminish protection for the trademarks of the forgotten stakeholder trademark owner, as well as erode potential for growth, and possibly cause the enterprise to fail—as well as potentially resulting in consumer deception and fraud.

The rights of these forgotten stakeholders can best be protected by taking steps to ensure wide-spread access to low-cost and efficient enforcement mechanisms and educating the stakeholders about these mechanisms. These include global mechanisms that are not dependent on local governments to implement, such as:

1. Cooperative partnerships to provide low cost or pro bono services to emerging, small businesses especially in developing countries;

2. Providing legal publication and easy access to relevant domain name registration data so that trademark owners can take advantage of a ready means of identifying infringers and have the option of sending cease and desist letters;

3. Creating dispute resolution mechanisms for unlawful trademark uses on website pages and social media; and

4. Providing education about the availability of these systems and how to use them so that even small or unsophisticated companies can use them with minimal cost.

The other forgotten stakeholders tend to be consumers, those who are deceived and defrauded, especially the elderly and those with reduced access to, and fluency with, digital resources.

To ensure their voices are heard, easy-to-access systems (such as phone, text, and online forms) should be established and publicized for reporting digital fraud. The systems should funnel complaints to enforcement agencies for investigation and follow-up. Ideally, assistance to victims to help them restore their lost property or identifications would also be provided.

c) What new or innovative mechanisms might be devised for multi-stakeholder cooperation in the digital space?

Establish a unified, global system for reporting digital fraud. The systems should funnel complaints to enforcement agencies for investigation and follow-up. Publicly available information could be made about reported entities including notations for verified complaints.

III. Illustrative Action Areas

The Panel plans to explore, among others, the following areas where greater digital cooperation is required:

- **inclusive development and closing the digital gap**
- **inclusive participation in the digital economy**
- **data**
- **protection of human rights online, particularly of children, women and marginalized communities**
- **human voice and participation in shaping technological choices and architecture**

- **digital trust and security**
- **building the capacity of individuals, institutions and governments for the digital transformation.**

a) What are the challenges faced by stakeholders (e.g. individuals, Governments, the private sector, civil society, international organizations, the technical and academic communities) in these areas?

Digital trust and security in economic transactions requires the transparent identification of vendors and a means of contacting them. A current challenge is the debate surrounding the appropriate level of information gathering and access related to the Registrants Directory Serviced known as WHOIS as ICANN. The European Union has adopted an approach to privacy rights that ICANN has interpreted to require the effective masking of the WHOIS system. The sudden redaction of information necessary for trademark enforcement has not been balanced with a concurrent system of access for legitimate purposes. A resolution to the issue is being negotiated through ICANN's multistakeholder process but an efficient, reliable means of access is not in place nor is there an estimated time frame for such access may be implemented.

Stakeholders must to work together and in a spirit of compromise make sure that identities of those involved in commercial transactions can be sufficiently known and subject them to enforcement remedies as necessary. Restoring the publication of critical WHOIS information, negotiating access to nonpublished information and requiring registries to obtain, as a condition of name domain registration, a valid email address to reach the domain owner are important steps in the direction. This minimal level of transparency for economic transactions will increase the efficiency of and reduce the cost of consumer protection especially by public and private entities as neither have easy, affordable access to WHOIS data at the moment. Doing so helps protect human rights online by reducing exposure to fraud and deception, and the counterfeiting activities that go hand in hand with criminal and destabilizing activity around the globe, and by enabling small business owners to grow their brands and reach more people, can increase inclusion in the digital economy and build capacity for economic self-determination.

b) What are successful examples of cooperation among stakeholders in these areas? Where is further cooperation needed?

Under stewardship of ICANN's multistakeholder process, the WHOIS database and the UDRP are examples of successful cooperation among stakeholders. However, as described above, the masking of vital information in WHOIS database has made both of those mechanisms more expensive and cumbersome to use. There are deep disagreements within the multistakeholder community as to how far ICANN's measures should go in terms of publication and access to WHOIS data. We applaud ICANN for creating an expedited process to resolve some of the issues. However, the effects of ICANN policy can reach well beyond ICANN. It is important to analyze how mechanisms work together inside and outside of ICANN's multistakeholder process in order to prevent unintended policy consequences in terms of how to balance privacy interests online with legitimate law enforcement, consumer protection and IP interests. Further

cooperation is needed to restore the WHOIS database to the right balance. In addition, stakeholders should work to create a unified access model for domain name ADR and enforcement. (See Reference 14)

c) What form might cooperation among stakeholders in these areas take? What values and principles should underpin it?

Stakeholders are currently cooperating through ICANN's multistakeholder process and the Internet Governance Forum (IGF) and the World Summit on the Information Society (WSIS). There should be much more attention paid to bolstering awareness of the missions of ICANN, IGF and WSIS and creating mechanisms that allow for engagement that goes beyond those who are entrenched in the circle of policy professionals who frequent these meetings. The policy discussions inside and outside of ICANN, IGF and WSIS should be meshed in some way so that these organizations are not operating in silos.

Although ICANN's functions are technical, as described in the question above, ICANN's policy ramifications are global and overreaching. ICANN policies can have an unintended global effect as we have seen with GDPR implementation and the WHOIS system. We need to develop a better understanding of how ICANN fits into the Internet Governance picture and vice versa.

The Internet Governance Forum (IGF) has also played a key role in fostering debate about the correct ways to approach the myriad issues presented by internet governance. There is a call for the IGF to become more outcome oriented. INTA supports that drive but also understands that having a safe space for debate is also important to the growth of ideas and solutions. While the IGF has provided such a space, areas that are vital to the private sector, like intellectual property protection, do not appear to be given the same weight as other topics. Expanding the diversity of topics and formulating an agenda for executable outcomes at the national and international level would be welcomed.

In terms of the WSIS, it appears that WSIS is organized more around a reporting structure. Governments and organizations report on the progress of national and international programs. As such, the format may not foster collaboration as it tends to be oriented toward governmental and NGO panels and does not appear to have robust private sector engagement. Moving WSIS toward collaborative, multistakeholder dialogues could be a constructive improvement.

The underpinning values to these suggestions are transparency and inclusiveness.

IV. Do you have any other ideas you would like to share with the Panel?

Engaging business entities at all levels of discussion will be important to any cooperative effort, whether in a forum like ICANN, IGF or WSIS. This is a tough assignment as many policy development efforts have sought solutions to building public awareness and capacity for small and medium enterprises (SMEs), but have not found the key to success. The typically limited resources of SMEs make it difficult for them to focus on issues like internet governance, even though it may be important to them. This is also true for areas of intellectual property protection, like trademarks, where SMEs may not know that they need help or protection until it is too late.

Partnering with trade associations and local chambers of commerce should be a key component for planning full engagement and creating networks for digital cooperation. From a values perspective, protection of intellectual property can be perceived as an inhibitor to development and growth when, in fact, it may be the only means to protect a growing online business. Economic growth and sustainability are key factors underlying some of the more pressing digital issues. Recognizing intellectual property as a driver rather than an obstacle to growth could attract more private sector involvement in policymaking in the digital space.

Many private sector entities are not familiar with nor understand domain name system terminology nor do they understand the Strategic Development Goals (SDGs). As ICANN has its own language, so does IGF and WSIS in terms of their relationship to SDG's. The discussions around digital cooperation should be conducted in as accessible language as possible without acronyms or insider terms that go beyond what is understood outside the walls of particular policy models. The underpinning values are transparency and inclusiveness.

V. Please provide your numbered references or links to additional reports/documents here.

1. FBI, 2017 Internet Crime Report, available at https://pdf.ic3.gov/2017_IC3Report.pdf)
2. FBI Alert https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams.
3. FIT, 2018 Typologies (https://www.fic.gov.za/Documents/TYPOLOGIES%20-%20September%202018.pdf)
4. INTA Submission On The Request For Public Comment Regarding The Fourth Joint Strategic Plan For Intellectual Property Enforcement for the Office of the Intellectual Property Enforcement Coordinator (IPEC) through the Office of Management and Budget, Nov. 13, 2018, available at https://www.inta.org/Advocacy/Documents/2018/INTA%20Comments%20to%20IPEC%20Joint%20Strategic%20Plan.pdf)
5. February 2017, INTA & ICC- BASCAP report from Frontier Economics entitled "The Economic Impacts of Counterfeiting and Piracy" available at https://iccwbo.org/publication/economic-impacts-counterfeiting-piracy-report-prepared-bascap-inta/
6. Organisation for Economic Co-operation and Development/European Intellectual Property Office (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris, at 68 available at https://read.oecd-ilibrary.org/governance/trade-in-counterfeit-and-pirated-goods_9789264252653-en#page1
7. United Nations Office of Drugs and Crime, The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime, 2014, available at https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf.
8. Polaris Project, 2017 Statics from the National Human Trafficking Hotline and BeFree Textline, available at http://polarisproject.org/sites/default/files/2017NHTHStats%20%281%29.pdf

9. INTA, Unfair Competition Survey Report 2016/2017, available at https://www.inta.org/Advocacy/Documents/2018/Unfair%20Competition%20Survey%20Report.pdf
10. INTA, Trademarks Basics for Business, available at http://www.inta.org/Media/Documents/2012_TMBasicsBusiness.pdf
11. http://www.wipo.int/madrid/en/index.html
12. ICANN, URDP Information https://www.icann.org/resources/pages/help/dndr/udrp-en
13. WIPO, The UDRP and WIPO - INTA Conference Paper: The Uniform Domain Name Dispute Resolution Policy and WIPO (2011) available at http://www.wipo.int/export/sites/www/amc/en/docs/wipointaudrp.pdf
14. Sept. 2018 Interview with B. Beckham of WIPO available at http://www.ipprotheinternet.com/interviews/interview.php?interview_id=128