



IN THIS ISSUE:

UAE Marks New Milestone with Launch of New IP Ecosystem

Registry service provider evaluation handbook published

WebUnited Inks Deal to “Mirror” Country’s TLD in the Blockchain

UN Cybercrime Convention: Time Is Running Out to Address Draft’s Urgent Risks to Human Rights

THNIC Launches 2nd level .TH Domain Names

UAE Marks New Milestone with Launch of New IP Ecosystem

DUBAI - The Ministry of Economy of the United Arab Emirates announced the launch of its new Intellectual Property Ecosystem, which will help inventors and creators protect their concepts, attract more foreign direct investment to the country, and enhance the country’s transition into a knowledge and innovation economy and develop an incubating national environment for Intellectual Property.

The newly launched IP system is aligned with the UAE’s vision to become a global hub for the new economy and the most prosperous society globally. The IP Ecosystem program is anchored by 11 initiatives, covering key economic and creative sectors of the UAE, including support for new technologies and student awareness programs.

Considered one of the biggest supporters and impactful in the field of Intellectual Property in the UAE, Abu-Ghazaleh Intellectual Property (AGIP) was invited by the Ministry of Economy to attend the launch of the IP Ecosystem, held on February 7, 2024.

It is worth mentioning that the UAE spares no effort in developing its IP sector in accordance with global best standards, to ensure better IP practices, laws and regulations in the country, and to maintain an attractive business environment for all entities and businesses.

Libya: Online Publication of Trademark Applications

TRIPOLI – According to Chapter Ten regarding trademarks of Law No. 23 of 2010, and its executive regulations issued in 2024, the Libyan Trademarks Office announced that the trademark applications accepted by the Registrar will be published on the Official website of the Trademarks Office, starting from February 1, 2024. The Trademarks Office will publish the trademark applications that have been filed from April 2013 to April 2015, holding the filing numbers from 22,100 to 28,699.

For more information in this regard, please contact AGIP Libya office at: libya@agip.com

Registry service provider evaluation handbook published

ICANN has released the first draft of its RSP Handbook, the guidelines and questionnaire for registry service providers that want to get pre-approved by the Org ahead of the next new gTLD application round. The Handbook is aimed at the few dozen companies that offer back-end services to gTLD registries — companies such as GoDaddy, Identity Digital and CentralNic — to guide them through the process of getting approved under the new Registry Service Provider Evaluation Program.

The program was called for by the GNSO community in order to minimize the amount of time-consuming, expensive evaluation work required for each new gTLD application. If a gTLD applicant's selected RSP has been pre-approved by ICANN, it's an automatic pass on the technical part of the application.

The new Handbook 1.0 envisages four types of RSP. A "Main RSP" is a full-service provider that looks after all technical aspects of a registry back-end. There are also categories for companies that provide DNS resolution only and DNSSEC services.

A fourth type, the "Proxy RSP", is aimed

primarily at companies that provide secondary registry services in countries that have very restrictive domain licensing rules. That basically means China, and proxies such as ZDNS. Incumbent gTLD RSPs have a distinct advantage in the Handbook process. If they're in good standing with ICANN and have complied with their service level agreements for the last six months, they can skip the second, technical part of the evaluation.

Incumbents also get a streamlined process for additional registry services - stuff like name-blocking and registry locks - they wish to offer. If they already offer them in an existing gTLD, they get to skip the full Registry Services Evaluation Process.

The Handbook is a first draft and does not currently include things like fees and dates. ICANN expects to launch the pre-evaluation program 18 months before it starts accepting new gTLD applications, so applicants have a list of approved RSPs to choose from. With a Q2 2026 target date for the next application window, that means the RSP program could launch later this year.

Source: Domain Incite

WebUnited Inks Deal to “Mirror” Country’s TLD in the Blockchain

Blockchain domains startup WebUnited says it has signed up its first registry client to a service that allows domain names to be “mirrored” on a blockchain naming service.

The company has inked a deal with Global Domains International, the registry for Samoa’s .ws ccTLD (sometimes marketed as a generic for “web site”), that will let its registrars up-sell matching .ws names on the Polygon blockchain.

WebUnited, a Swiss-based joint venture of domain registry ShortDot and “Web3” naming player Freename, says registrants will be able to use their mirrored .ws names to address cryptocurrency wallets, for example.

The company essentially acts as a registry service provider for its registry clients in much the same way as regular RSPs do now, except instead of putting domains into EPP databases and the consensus DNS, it adds them to a blockchain.

Registrars that choose to sign up to the service will use an “EPP-like” API to access the

registry, ShortDot COO Kevin Kopas said. He expects .ws to charge about five bucks a year for the blockchain add-on domains.

Kopas said WebUnited is also mirroring policies found in regular domain names, so if somebody loses their domain in a UDRP case, for example, they also lose their matching blockchain name.

After .ws, ShortDot’s own TLDs - .bond, .sbs, .icu, .cyo and .cfd - are also expected to offer the mirroring service. Because these are gTLDs governed by ICANN contracts, ShortDot first has to go through the Registry Service Evaluation Process for approval.

Kopas said that once ShortDot has completed its RSEP it will be able to supply gTLD clients with template language to get their own RSEPs approved. He said WebUnited has a pipeline of potential ccTLD and gTLD registries that have expressed an interest in the service.

Source: Domain Incite

UN Cybercrime Convention: Time Is Running Out to Address Draft's Urgent Risks to Human Rights

Co-authored by Maria Paz Canales, Head of Legal, Policy and Research at GPD and Ellie McDonald, Global Engagement and Advocacy Lead at Global Partners Digital.

In two weeks, final negotiations will begin on the UN's proposed Cybercrime Convention, a document which has elicited widespread concern from civil society, industry groups, and some states due to the serious risks it poses to human rights, including privacy and freedom of expression.

Since 2022, GPD and other groups, including EFF, Human Rights Watch and Privacy International, have sought to alert stakeholders within the process to the need for substantial revisions to the treaty's text to avoid it becoming an instrument of surveillance and repression. As we enter crunch time in the discussions, we present below a rundown of the most pressing issues within the most recent draft (published in November last year), in the hopes that policymakers will mobilize to address them.

It criminalizes an overly broad range of offences (including those which only incidentally involve digital technologies)

As drafted, the Convention's chapter on criminalization is vastly overbroad. Instead of just covering the traditionally understood range of cybercrimes like illegal access or interference with computer systems, it goes

significantly beyond this to capture a range of cyber-enabled crimes—which includes misuse of devices and computer fraud. Troublingly, it also captures content-based offences like intimate image sharing and grooming due to overly broad definitions that risk clashing with the exercise of human rights, notably freedom of expression and access to information, privacy, non-discrimination, and the rights of the child.

We've already seen how vaguely drafted cybercrime laws have been used to restrict online activity and violate human rights. Recent research by APC and Derechos Digitales maps where cybercrime laws have been used to stifle dissenting voices and criminalize those advocating on behalf of women and LGBTQIA+ people: from a trans influencer in Nicaragua forced into exile for social media posts, to an Egyptian human rights activist sentenced to two years in prison for a video on sexual harassment.

If exercised through a global, binding treaty, this would have disastrous outcomes for the freedom and security of all internet users globally.

It puts security researchers, activists and whistleblowers at increased risk

The draft's criminalization chapter fails to account for the protection of security research and other public interest activities that could be prosecuted according to the current

provisions, harming both cybersecurity and the right to seek and receive information by whistleblowers and journalists. The effect of these drafting flaws is a Convention which will make us less secure: chilling the work of cybersecurity researchers and others by exposing them to excessive criminalization of actions executed to improve digital security and benefit the public interest. This is the opposite of what a global Convention purporting to fight cybercrime should seek to achieve.

It lacks meaningful human rights safeguards

While the scope of the treaty has been consistently enlarged throughout the drafting process, this has not been accompanied by the required and necessary human rights safeguards, despite repeated calls from GPD and other groups. In the present draft, they are entirely insufficient to prevent the abuses that the current wide scope facilitates.

We are concerned with the latest draft's deletion of a reference to the right to effective remedy regarding the proposed safeguards, and we continue to recommend more granular guidance on conditions and safeguards, such as the principle of prior authorization for the accessing or sharing of data, and a guarantee that the investigatory powers provided for cannot be used to compromise the security of digital communications and services.

Even the fragile safeguards included in

the text risk being undermined if certain proposals are enacted. The current draft text limits the safeguards already established to the procedural measures chapter, which means there are no proper human rights protections for the activities pursued under the international cooperation and preventive measures chapters. This absence of robust safeguards is antithetical to the UN's responsibility to ensure compliance with international human rights law.

We are particularly concerned by the inclusion in this draft (in the international cooperation chapter) of language referring to the possibility of preserving, accessing, or collecting data “where the data are in the possession or control of a service provider located or established in that other State Party.” Without proper safeguards, this phrase creates the risk of mass extraterritorial surveillance, enabling states to secretly surveil individuals located in third states via service providers. With the current weak safeguards, nothing will prevent this from happening in total secrecy, without users whose data is impacted being notified.

Many of the issues highlighted above are still italicized in the text, meaning that they are currently subject to informal and opaque negotiations. It is concerning that some of the proposals that would positively strengthen safeguards or limit the scope of the Convention are not reflected in the draft at this point, even those which seem to have wide support from states and other stakeholders in the process.

It has an uncertain (possibility limitless) remit

All the issues raised above are serious and troubling enough on their own terms. But the looseness of certain parts of the present draft raises the possibility that the scope and criminalization of the treaty could be expanded even further in the future: raising the spectre of an limitlessly expanding, increasingly punitive framework.

The key provision here is the current draft's inclusion of an open-ended reference to "applicable international conventions and protocols". This is significant, because it opens the door to expanding without clear limits the offences that could be enforced through the treaty, transforming it from a cybercrime treaty to a general-purpose one.

States are continuing to discuss different approaches to this provision, including placing it within the criminalization chapter or the international cooperation chapter (which could mitigate some of the risk), or removing it entirely. We are concerned by signals that the provision is likely to remain in some form despite the uncertainty it introduces and the clear human rights risks this poses. We urge states to entirely remove this provision.

The cumulative effect of this provision and the aspects described above is that, in its current form, the draft Convention has a potentially limitless scope. This is an issue

which has been rightly acknowledged by Canada alongside 39 other states and the EU, who have referred to a "continuous push" to widen the draft Convention's remit.

Next steps

These fundamental flaws in the draft must be corrected. Otherwise, due to the risks it poses to human rights, the Convention should not be moved forward for adoption.

In concrete terms, addressing these flaws would mean:

- Narrowing the scope of the treaty to cyber-dependent crimes;
- Ensuring that security researchers, whistleblowers and journalists are not prosecuted for their legitimate activities;
- Including strong human rights safeguards applicable to the whole treaty;
- Avoiding ambiguities by deleting reference to offences established by other undetermined international treaties; and,
- Avoiding the use of the treaty as an instrument for state surveillance—by limiting the application of its procedural measures and international cooperation chapters to cyber-dependent offences established in the treaty.

For more detail on these suggested changes, read our full submission to the AHC on the latest draft.

Source: circleID

THNIC Launches 2nd level .TH Domain Names

The Thai Network Information Center Foundation (THNIC Foundation) announced that it is re-launching 2nd level .TH domain names beginning February 1, 2024, through March 31, 2024. Previously, the .TH extension was restricted to IDN characters only. THNIC is now allowing ASCII characters for .TH domain names during this launch.

Sunrise Registration: Domain names will be registered in one of the below categories.

Category 1: Trademark name

- Trademark name registered with the Department of Intellectual Property. Ministry of Commerce. of Thailand

Category 2: Foreign Trademark

- Foreign trademark owner registers domain by a local Thai company.



Sunrise Phase - February 1, 2024 through March 31, 2024

To be included in the Sunrise phase, orders must be received before March 29, 2024 (noon MST).

- * Restricted
- * 1-year min term
- * Min/Max Characters: 2 - 63 Characters
- * DNS Requirements: 2 - 8 Configured DNS
- * Domain Masking Available: No

Documents Required:

- Thai trademark, fully registered and an exact match to the domain name requested.
- Thai company business registration document.
- Documents must be signed and stamped by an authorized person. The authorized signatory must provide a valid photo ID.
- Foreign trademark exact match to the domain, with Thai Company registration document.



Please feel free to contact us at:
info@tag-domains.com
Tel.: +962 6 5100 900 ext. 2743
Fax: +962 6 5100 901



TAGTech

PRODUCTS



**Intel Core i5
8th Generation**



**8 GB RAM
DDR4**



256 GB SSD



FLIP



**Intel® Core i7
10th Generation 1065G7**



**8 GB RAM
DDR4**



**128 GB SSD
+ 512 GB SSD**



PRO



Intel Celeron N4100



4 GB LPDDR3



**256GB SSD
+ 64GB EMMC**



UNI C



**Intel® Core i3
10th Generation 1005G1**



**4 GB RAM
DDR4**



128 GB SSD



EDU



**Intel® Core i7 10th
Generation 10510U**



**8 GB RAM
DDR4**



**128 GB SSD
+ 1 TB HDD**



PLUS I



**Intel® Core i7 10th
Generation 10510U**



**8 GB RAM
DDR4**



**128 GB SSD
+ 512GB HDD**



PLUS II



**Intel® Core™ i7
1255U**



**8 GB RAM
DDR4**



**256 GB SSD
+ 1 TB HDD**



**Intel® Iris®
Xe Graphics**



4500 mAh



AX (wifi 6) BT 5.1

PLUS III

7022

New





Intel® Core™ i5
1235U



8 GB RAM
DDR4



256 GB SSD
+ 1 TB HDD



Intel® Iris®
Xe Graphics



5000 mAh



AC WIFI
BT 4.2

PLUS III

5022

New



Spreadtrum
SC7731E Quad-core



2 GB



32 GB



TAG-TAB Kids II



MediaTek MTK
8788 octa-core



8 GB



128 GB



TAG-TAB III



Front: 16 MP
Rear: 20 MP



6 GB



128 GB



TAG-PHONE
Special



Spreadtrum
SC9863 Octa-core



4 GB



64 GB



TAG-DC



Front: 8 MP
Rear: 16 MP



4 GB



128 GB



TAG-PHONE
Plus



Front: 16 MP
Rear: 16 MP



6 GB



128 GB



TAG-PHONE
Advanced

TAGTech.Global Building 7, Abdel Rahim Al-Waked Street, Shmeisani, Amman, Jordan
TAGUCI Building 104 Mecca Street, Um-Uthaina, Amman, Jordan

+962 65100 250 **info@tagtech.global** **For More Information: www.tagtech.global**