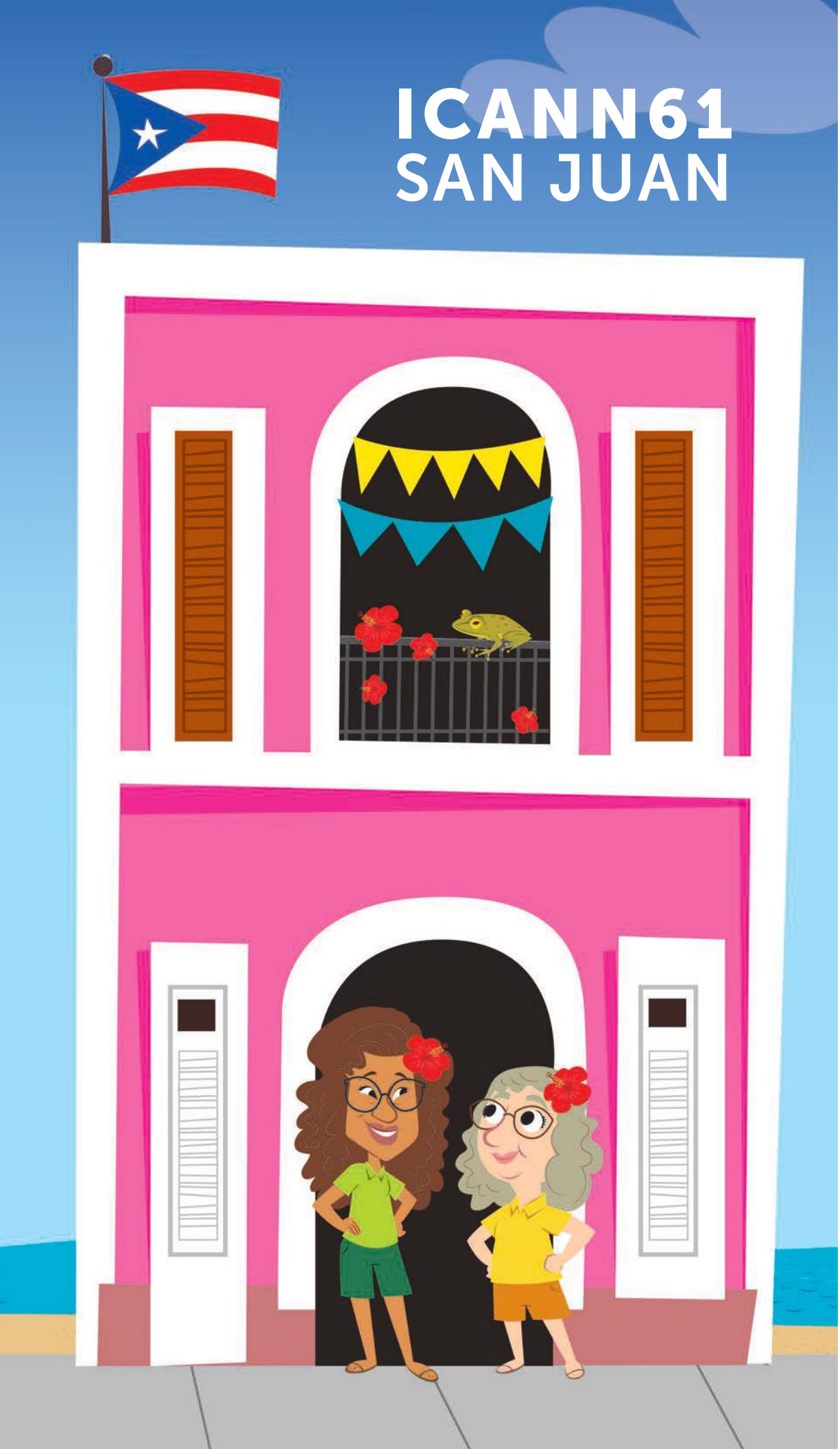
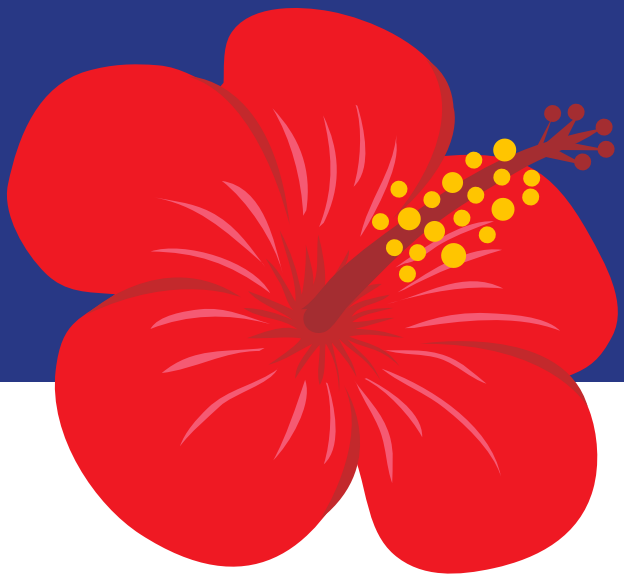
ICANN61
SAN JUAN



ICANNWiki QUICK GUIDE

ICANNWiki QUICK GUIDE

ICANN61 SAN JUAN



Welcome to ICANN61, in beautiful San Juan, Puerto Rico. It's no secret that Puerto Rico suffered greatly as a result of Hurricane Maria, yet the community is still working hard to rebuild their world, and refortification can be seen everywhere.

This issue of the ICANNWiki Quick Guide includes an with interview Pablo Rodriguez of NIC.PR, Primers on select topics, a special feature from the Geneva Internet Platform and much more!

2018 is a critical year for ICANNWiki—like much of the community, we are facing cuts in our funding. These cuts threaten our ability to carry out our work and continue to operate. In response to this, we are doing everything we can to keep the organization alive. We have benefited greatly from the time, energy and resources that the community has dedicated to ICANNWiki over the years and we will continue to keep you updated on how you can help us continue our work. We have been an integral part of the community for over a decade and we remain committed to bringing you the best information within the ICANN community.

Jackie Treiber and Dustin Phillips
Co-Executive Directors, ICANNWiki

TABLE OF CONTENTS

ABOUT ICANNWiki

ICANNWiki is a grassroots, community effort to create and curate articles describing the people, organizations, terms and topics within the ICANN community. We actively seek worldwide collaboration to increase understanding of how policy is created for the continued development of the Internet, a tool which we all use everyday. In particular we cover the Internet Corporation for Assigned Names and Numbers (ICANN) and related multistakeholder policy and management bodies.

FIND US ONLINE
@ICANNWIKI

GET INVOLVED!

Three times a year, ICANN's Multistakeholder Community gathers for meetings in different regions of the world. These meetings are free and open to all, including remote participants. With around thousands of participants, hundreds of sessions and various stakeholder groups, navigating ICANN as a newcomer can be difficult, but our ICANNWiki Primers are a helpful place to begin your ICANN journey.

LEARN

Learn how ICANN is structured and operates by taking a course on ICANN Learn, researching with ICANNWiki's multilingual encyclopedic resource, and exploring the vast amount of documents and information on icann.org.

FOLLOW

Follow the latest policy discussions by subscribing to some mailing lists or reading the archives. Many of the lists are publicly available, but some may be restricted to members of the Working Group.

BE HEARD

Comment on policy proposals through ICANN's public comment platform. Each proposal is open for a minimum of 40 days for community comments. At ICANN Meetings, you can also make comments at the Public Forums.

GET INVOLVED WITH ONE OF ICANN'S STRUCTURES

ICANN's Multistakeholder Community consists of seven structures, classified as Supporting Organizations (SO) and Advisory Committees (AC). Each of the seven structures have different compositions and criteria to join. Newcomers looking for a way to contribute to ICANN's multi-stakeholder, bottom-up, consensus driven model for policy development should start with the GNSO or ALAC.

SUPPORTING ORGANIZATIONS

GNSO
gnso.icann.org

The Generic Names Supporting Organization (GNSO) is the main policy-making body in ICANN. It brings together various stakeholder groups to develop and recommend policies to the ICANN Board concerning generic top-level domains (gTLDs).

ccNSO
ccnso.icann.org

The Country Code Names Supporting Organization (ccNSO) is open to and comprised of the managers responsible for operating country-code top-level domains (ccTLDs). It develops and recommends policies relating to ccTLDs.

ASO
aso.icann.org

The Address Supporting Organization (ASO) represents the Regional Internet Registries (RIRs). It is tasked with reviewing and developing Internet Protocol address policy and advise the Board accordingly. Membership is only available to RIRs.

ADVISORY COMMITTEES

ALAC

The At Large Advisory Committee (ALAC) functions as the voice for the individual Internet user as it relates to ICANN processes, policy and more and advises the Board accordingly. It is formed of smaller groups At-Large Structures that are part of Regional At-Large Organizations. **Learn more at atlarge.icann.org.**

GAC

The Governmental Advisory Committee (GAC) iscomprised of formally appointed governmental representatives and is responsible for providing advice to the Board relating to the concerns of governments, including how ICANN policies interact with laws and international agreements. **Learn more at gac.icann.org.**

SSAC

The Security and Stability Advisory Committee is composed of technical experts from industry and academia that advise the Board on the security and integrity of the Internet's naming and address allocation systems. The SSAC is an invite-only organization. **Learn more at ssac.icann.org.**

RSSAC

The Root Server System Advisory Committee is made up of representatives from the organization responsible for operating the 13 root name servers and advises the Board on issues related to the operation, administration, security, and integrity of the Internet's Root Server. **Learn more at rssac.icann.org.**

PDP Review of All Rights Protection Mechanisms in All gTLDs

Disputes and questions around the legal rights and legitimate ownership of domain names is nothing new. In 1999, the Uniform Domain-Name Dispute-Resolution Policy (UDRP) was established to resolve disputes relating to the registration of domain names. Ahead of the 2012 round of the New gTLD Program, additional Rights Protection Mechanisms (RPMs) were developed and adopted to mitigate the risks and costs to trademark rights holders. The PDP Review of RPMs in all gTLDs was spun out of the Final Issue Report on the current state of the UDRP in 2011 and the subsequent Issue Report on the current state of all RPMs in 2016.

The PDP was initiated in February 2016 to review all RPMs in two phases:

PHASE 1: All RPMs applicable to New gTLDs (2012 Program)

Trademark Post-Delegation Dispute Resolution Procedures (TM-PDDRPs)
Completed in late 2016

Trademark Clearinghouse (TMCH)
Sunrise periods
Trademark Claims notification service

Uniform Rapid Suspension Dispute Resolution Procedure (URS)

PHASE 2: Uniform Domain Name Dispute Resolution Policy (UDRP)

The Working Group (WG) is currently in the midst of Phase One. It has already completed its review of the TM-PDDRP and has carried out an initial review of structure and scope of TMCH, but is awaiting the results of a survey to collect quantitative data and anecdotal evidence to better assess the services provided by TMCH. With this survey ongoing, the WG is currently focused on organizing and refining the charter questions related to URS and determining what, if any, data will need to be collected to address the questions.

Completion of Phase One is estimated for early 2019, at which point the WG will publish a Preliminary Report. During this process timelines will continue to be coordinated with related efforts, including the New gTLD Subsequent Procedures PDP and Competition, Consumer Choice, and Consumer Trust (CCT) Review.

ICANN61 SESSIONS

Rights Protection Mechanism (RPM)
GNSO RPM Review Working Group Meetings

Saturday, March 10	15:15 – 16:45
Saturday, March 10	17:00 – 18:30
Sunday, March 11	17:00 – 18:30
Wednesday, March 14	8:30 – 10:15

Registration Directory Services (RDS)
GNSO RDS PDP Working Group Meetings

Saturday, March 10	8:30 am – 12:00
Wednesday, March 14	15:15 – 16:30

General Data Protection Regulation (GDPR)
Cross-Community Session: GDPR and WHOIS Compliance Models

Monday, March 12	10:30 – 12:00

GAC and GAC Public Safety Working Group (PSWG) Discussion: GDPR & WHOIS

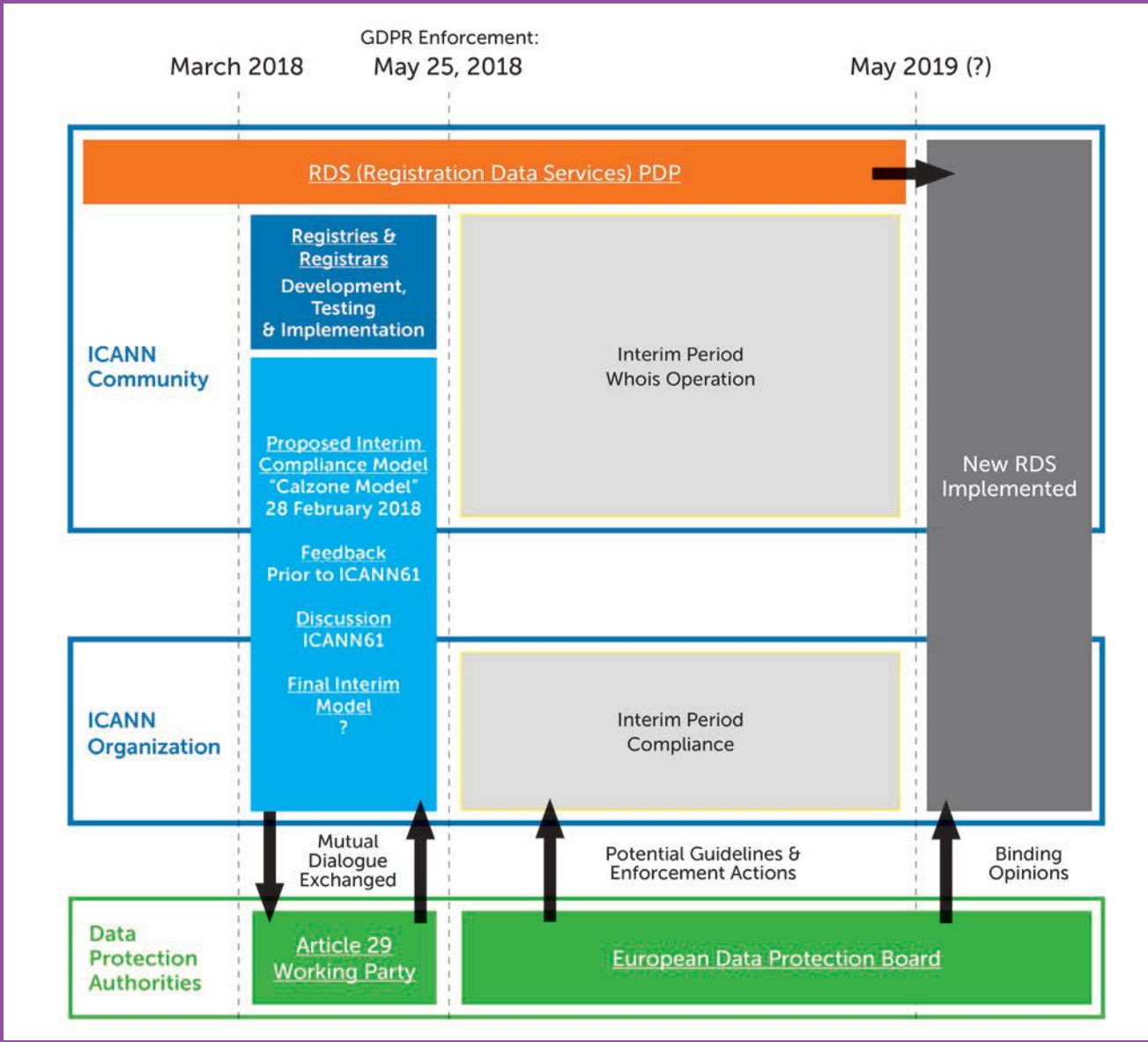
Tuesday, March 13, 9:30	9:30 - 10:15

GAC Discussion: GDPR & WHOIS Compliance Models

Tuesday, March 13	10:30 – 11:00

The WHOISteria of GDPR

With May 25th and GDPR enforcement looming, an Interim compliance model is being developed by ICANN to replace the current model until the outcome of the Next Generation gTLD RDS to Replace WHOIS PDP is implemented. During this process, there have been several food metaphors invoked. It began with comparing the potential Interim model to a hawaiian pizza, creating controversy around the validity of pineapple as a pizza topping. Most recently, ICANN released its "Calzone Model" proposal on the 28th of February, seeking a balance between competing elements included in the community-submitted models and the comments on the ICANN-proposed models. However, at this point an egg-based metaphor could be more apt, because no matter what's included it's going to be a scramble.



Under this proposed model, the collection, transfer and retention of full Thick WHOIS remains largely unchanged. However, public access would be limited to registrant organization (if provided), state/province, and country, in addition to "thin data," or technical data related to the domain name itself. While registrant email addresses would not be publicly available, it is being proposed that the anonymized email addresses or web forms could replace the email address as a means for contacting the owner of a domain name. Access to the full set of data would be available through a yet-to-determined accreditation process. These changes apply to the collection and processing of the data of both natural and legal persons linked to the European Economic Area (EEA) with the option of applying changes globally.

When an interim model of compliance goes into effect it will mark the first substantial change to the WHOIS system since its inception in 1982. The community is hard at work developing a permanent solution, but until then the interim model will reign, making the decision critical to the ICANN community.

Next-Generation gTLD Registration Directory Services

WHOIS launched in 1982 as a directory service for users transmitting data across the ARPANET. It is currently used for registration data on all gTLDs, serving the needs of domain name registrants, law enforcement agencies, intellectual property interests, businesses, individual users, as well as some who misuse it for malicious purposes. Despite this evolution, the WHOIS protocol has remained largely unchanged.

Comprehensive reform has been a long-running source of debate with nearly 15 years of history, dating back to the formation of the WHOIS Privacy Steering Group in 2003. This effort by the Steering Group, and later, the "Preliminary Task Force on the Purpose of Whois and of the Whois Contacts" were ultimately unsuccessful in bringing forth new policy to reform WHOIS.

In 2009, when ICANN signed the Affirmation of Commitments with the US Department of Commerce, it committed to conduct a number of high level reviews. As a result, the WHOIS Policy Review Team was formed in 2010 and released its final report in 2012, outlining a set of recommendations to ensure that WHOIS policy is effective, meets the legitimate needs of law enforcement and promotes consumer trust. Shortly after this final report, the SSAC issued a response that stressed the importance of "understanding the purpose of domain name registration data" before any meaningful, comprehensive solution can be reached.

On 8 November 2012, the ICANN Board passed a resolution for a board-initiated PDP and the Expert Working Group on gTLD Registration Directory Services (EWG) was launched to consider the purpose of registration data and how to safeguard it, and propose a new model that addresses the issues of accuracy, privacy, and access. The EWG released its final report in 2014, leading to the development of a Process Framework for the PDP, which was adopted in May 2015 by the ICANN Board, reaffirming its request for a Board-initiated PDP. In November 2015, the GNSO Council approved the charter for the Next-Generation gTLD Registration Directory Services to Replace Whois Policy Development Process Working Group (RDS PDP WG).

The RDS PDP is a 3-phase process:

PHASE 1: Policy - Requirements (Current Status)	***PHASE 2:*** Policy - Functional Design	***PHASE 3:*** Implementation & Coexistence Guide

In Phase 1, the WG seeks to reach consensus on providing recommendations to two questions:

1) What are the fundamental requirements for gTLD registration data and directory services?

FIVE FUNDAMENTAL CHARTER QUESTIONS

USERS & PURPOSES: Who should have access to gTLD registration data and why?
GATED ACCESS: What steps should be taken to control data access for each user/purpose?
REGISTRATION DATA ACCURACY: What steps should be taken to improve data accuracy?
PRIVACY: What steps are needed to protect privacy and data?
REGISTRATION DATA ELEMENTS: What data should be collected, stored, disclosed?

The WG is continuing its work on developing initial rough consensus on key concepts related to these questions. As of February 2018, they had reached rough consensus 49 key concepts. Seven drafting teams were formed to better understand and define each purpose of gTLD Registration Data, starting with those outlined in the EWG Final Report. Thus far, 12 potentially legitimate purposes have been drafted for deliberation of the WG as a whole.

Deliberations will continue around which purposes and data elements need to be supported by the RDS and the requirements for collection of those data elements. Once there is consensus on this, the WG will turn to the other fundamental charter questions. These deliberations will take input from independent legal counsel and senior EU privacy experts.

The drafting of the first of two initial reports is planned to begin in the first half of 2018 and aims to include responses to the first five Phase 1 questions.

2) Is a new policy framework and next-generation RDS needed to address these requirements?

The agreements on the fundamental requirements will be used to determine if a new RDS is needed or if WHOIS meets the requirements. If a next-gen RDS is needed, the WG will recommend "cross-cutting requirements" that it must address. If not, the WG will determine what changes, if any, need to be made to the current WHOIS policy framework. Depending on the outcome of these deliberations, the PDP will transition into Phase 2 to design policies to satisfy the requirements from Phase 1.

All deliberations and initial agreements have been guided by the following:

DRAFT REGISTRATION DATA AND DIRECTORY SERVICE STATEMENT OF PURPOSES

1. A purpose of gTLD registration data is to provide info about the lifecycle of a domain name and its resolution on the Internet.
2. A purpose of RDS is to facilitate dissemination of gTLD registration data of record, such as domain names and their domain contacts and nameservers in accordance with applicable policy.
3. A purpose of RDS is to identify domain contacts and facilitate communication with domain contacts associated with generic top-level domain names, [based on approved policy].
4. A purpose of gTLD registration data is to provide a record of domain name registrations.

Connectivity and Domain Names in the Wake of Natural Disaster

In February, we had a conversation with Pablo Rodriguez, Executive Vice-President of NIC.PR, about his experience with Hurricane Maria and the state of connectivity and domain names in the storm's aftermath.

There are many concerns during and in the wake of a natural disasters and other catastrophic events. With the potential for loss of life, homes and livelihoods, the renewal of domain names is likely not the first priority for those affected. In some cases, renewal might not even be possible due to the failure to power grids, telecommunication infrastructure, or both, as was the case in the Caribbean during the 2017 Atlantic hurricane season.

During our interview, Pablo Rodriguez told us that NIC.PR protected their customers' assets by renewing all of the domain names tied to registrant countries affected by Hurricane Irma or Maria. This service was provided free of charge, with the request that customers paid their bills when they were able to.

ICANN also took steps to protect registrants by approving Hurricane Maria and other similar natural disasters as extenuating circumstances under the Registrar Accreditation Agreement (RAA). By doing so, they gave registrars the flexibility to extend registration renewal periods for any individuals in affected regions.

ICANN's statement also stated, "The devastating impact of Hurricane Maria also highlights the need for a broader policy to protect registrants when they are unable to renew their domains as a result of natural disasters or other extraordinary circumstances. We encourage the community to consider this topic during policy development discussions."

There will inevitably be more situations in which regions are disconnected from the Internet for extended periods of time, placing various digital assets in jeopardy and the community should consider discussing practices or policies that can protect domain names in the event of catastrophic events.

"NIC.PR was operational prior to, during, and after the [hurricane]. We never went down... obviously we are very proud of that, but it took a lot from us to make sure that those services were protected."

- Pablo Rodriguez, Executive Vice-President of NIC.PR

An Interview with Pablo Rodriguez

(The following content has been edited for brevity and clarity.)

"NIC.PR continues to work very closely with the government in making sure that we have cemented the websites that the government is using to provide statistics, such as status.pr, which is the official website that has been providing statistics on our recuperation globally."

What were the impacts of Hurricane Maria on Internet connectivity and Infrastructure in Puerto Rico?

On September 20th, we were impacted by a category 5 hurricane that destroyed most of our electrical grid, in addition to the telecommunication towers. At least 80 percent or more of our telecommunication towers were destroyed, rendering the island in a blackout for days on end and without communication for weeks. We had not seen an event like this for at least 85 years. With the help of the army corps and various telecommunications companies, they began the reconstruction of the cell towers' telephone poles that would allow the electrical grid to get reestablished. It has taken a tremendous amount of effort and energy from various groups, whether it local, federal, or at a state level. To answer your question, the grid was destroyed, telecommunications were destroyed, and it has taken us a long time to reestablish all of that system.

I would dare to say that 90 percent or more of the metropolitan area is operational, but NIC.PR continues to work very closely with the government in making sure that we have cemented the websites that the government is using to provide statistics, such as status.pr, which is the official website that has been providing statistics on our recuperation globally.

What is the situation outside of the metropolitan area?

The center of the island, the mountains region, is struggling the most in getting reestablished. The metropolitan area, with a stronger infrastructure and newer buildings, was able to resist the brunt of the hurricane's punishment. However, the outskirts of the metropolitan area continue to suffer greatly, either without water or electricity. The electrical grid is being replaced in the majority of metropolitan areas. There are some pockets within that area that may not have services, but efforts are being made to reestablish the services there.

What has NIC.PR been doing as things recover?

In 2011, Japan suffered an earthquake and a tsunami, and their infrastructure suffered to a point where they were unable to communicate with their providers and renew their domain names. So, we took advantage of that experience and we thought of the same thing for us. What about our customers on the island? Can they communicate with us? They have no electricity, no power, and they are literally concerned about protecting themselves.

Since domain names were most likely not first [priority] on their list, we went ahead and did a search in our databases for all of those domain names whose country of origin was Puerto Rico, and other countries that were in the Caribbean. After this search, we went ahead and renewed all of those domain names and began to contact them and inform them that their domain names had been protected, and that they didn't have to pay extra money for that. All they had to was pay their bill as soon as they could, and, in the meantime, we would protect their domain names. In fact, that initiative has brought a lot of attention within the GNSO and other constituencies within ICANN, and they are now considering adopting this in the wake of natural disasters.

Do you think there is potential to create new policies or best practices within ICANN?

At ICANN61, we have scheduled a number of opportunities to speak to different constituencies about our process. For example, I have been invited by the GAC to explain our experience to them. Additionally, they want to hear more about our initiative to protect domain names. ALAC has also approached us to hear the same.

NIC.PR was operational prior to, during, and after the event. We never went down. So, obviously we are very proud of that, but it took a lot from us to make sure that those services were protected.

What are other major companies going to do? Are

the major registrars aware that a portion of their users live in those areas? When natural disasters do occur, what will they do about it? Will they develop a protocol that leads to better policy, that at a minimum asks [registrars] to look into their databases to see if people from that particular area are their customers? And what they will do to protect their domain name real estate?

So, we learned a lesson with Japan in 2011 and little did we know that the lesson was going to be what helped us and our users to protect their own domain name real estate.

What did you do to keep your back-end services up and running?

We had two colos (colocation centers); one of the colos ran out of diesel within three days. The other colo remained strong, and that kept us on top of our game. We were still scared because they were not getting any fuel either, but they had bigger reserves. The governor of Puerto Rico made it a point that hospitals and telecommunications were a priority and began sending fuel to hospitals and telecommunication companies to maintain those services.

It was very scary. We had no idea how long we were going to maintain our services. Thankfully, [the colo] was able to get the fuel that was needed to provide us with the services that we required.

Have you made any improvements to increase the resiliency of NIC.PR since Hurricane Maria?

We are working on that. We are making sure that we are putting our money into every single detail to ensure that we have connectivity. Also, escrow services became very relevant, right? Many people don't talk about escrow services, but all of a sudden, when a hurricane passes by and demolishes your country, escrow services are instrumental. It immediately puts things into perspective: do you have a risk management plan? Do you have a disaster recovery plan? And for those people that don't have an answer to that, now they know that this is very real. Sometimes people think that to have a risk management plan, or a disaster recovery plan, has to do with cyber attacks, DDoS, etc, but at the end of the day, mother nature can come and everything you knew no longer exists. And it only takes a couple of seconds. You need to be prepared for that.

We've done a lot to combat this. Our offices right now are partially being used as storage. We have water, Pampers, milk, and we have groups of people that come pick them up and take them to various areas. This process continues to be important to us, but what we have done to protect the domain name real estate is going to make a big difference.

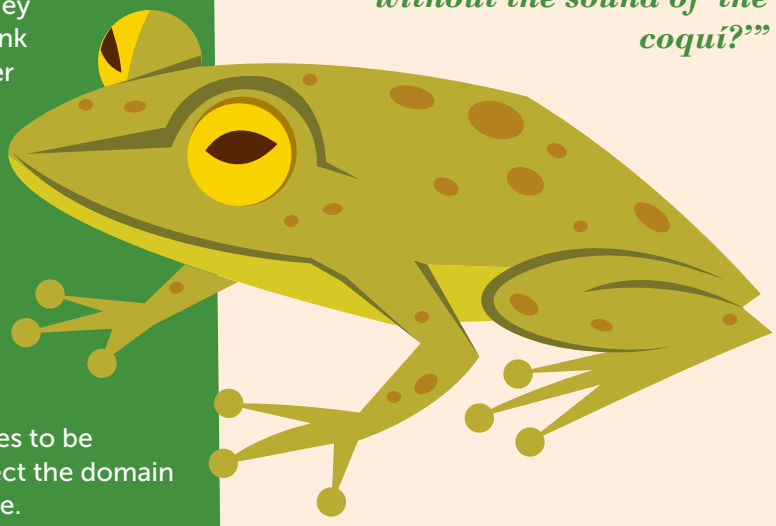
While wrapping up our Interview, ICANNWiki learned that the Puerto Rican resiliency and sense of family extends far beyond the Domain Name System. These sentiments are perfectly captured in Pablo's closing remarks, which recount the storm and its aftermath:

"There's nothing more Puerto Rican than the coqui [frog]. We love them. They sing all night long. Thousands of them. Every night, we have an orchestra...

After the hurricane, we heard nothing... silence. Wildlife's habitat had been destroyed. They didn't know what to do.

So we had to protect our wildlife. We had to protect our birds. We had to protect our bees. We had to protect our coqui. We cannot lose them. They're a part of us; they're family.

There is a Puerto Rican song that says: 'Ay que fuera de mí sin ti? Que fueran de mis noches si no canta el coquí' – or, 'What would I be without you? What would my nights be without the sound of the coquí?'"



ACRONYM ABC's

AC Advisory Committee

AFRALO African Regional At-Large Organization

AGB Applicant Guidebook

ALAC At-Large Advisory Committee

ALS At-Large Structure

APRALO Asian, Australasian and Pacific Islands Regional At-Large Organization

ASO Address Supporting Organization

BC Business Constituency

ccNSO Country Code Names Supporting Organization

ccTLD Country Code Top-Level Domain

CCWG Cross Community Working Group

CSG Commercial Stakeholder Group

DNS Domain Name System

DNSSEC Domain Name System Security Extensions

EURALO European Regional At-Large Organization

F2F Face-to-Face

GAC Governmental Advisory Committee

GDD Global Domains Division

GDPR General Data Protection Regulation

GNSO Generic Names Supporting Organization

gTLD Generic Top-Level Domain

HRIL WG Human Rights and International Law Working Group (GAC)

IANA Internet Assigned Numbers Authority

ICANN Internet Corporation of Assigned Names and Numbers

IDN Internationalized Domain Name

IETF Internet Engineering Task Force

IPC Intellectual Property Constituency

IRP Independent Review Process

ISPCP Internet Service Providers and Connectivity Providers Constituency

IPv4 Internet Protocol Version 4

IPv6 Internet Protocol Version 6

KSK Key Signing Key

LACRALO Latin American and Caribbean Islands Regional At-Large Organization

NARALO North American Regional At-Large Organization

NCSG Non-Commercial Stakeholder Group

NCUC Non-Commercial Users Constituency

NOMCOM Nomination Committee

NPOC Not-for-Profit Operational Concerns Constituency

PDP Policy Development Process

PTI Public Technical Identifier

RDS Registration Directory Service

RIR Regional Internet Registry

RrSG Registrar Stakeholder Group

RT Review Team

RySG Registry Stakeholder Group

RSSAC Root Server System Advisory Committee

RZERC Root Zone Evaluation Review Committee

SO Supporting Organization

SSAC Security, Stability and Resilience Advisory Committee

TF Task Force

UDRP Uniform Dispute Resolution Process

URS Uniform Rapid Suspension

WG Working Group

Geneva Internet Platform
DigitalWatch
NEWSLETTER

You receive hundreds of pieces of information on digital policy. We receive them, too. We decode, contextualise, and analyse them. Then we summarise them for you.

DIGITAL POLICY TRENDS IN FEBRUARY

1. Renewed calls for cyber norms

The debate on cyber norms has picked up after renewed calls for adopting rules to tackle cybercrime and cyber conflict were made this month.

Referring to the use of warfare among states, UN Secretary General António Guterres warned that cyber-attacks against military targets and critical infrastructure will likely initiate future wars, and called to minimise the impact of electronic warfare on civilians.

During his address at the University of Lisbon, Guterres said that it is not clear how existing international humanitarian law, including the Geneva Conventions, apply to cyberwarfare. He said the UN could serve as a platform for various stakeholders to work on rules that can ensure 'a more humane character' to cyber conflicts.

Addressing also the Munich Security Conference, he called for discussions on the related international legal framework using the competence of the First Committee of the UN General Assembly. 'I don't intend that the United Nations has a leadership role on this, but I can guarantee that the United Nations would be ready to be a platform in which different actors could come together and discuss the way forward.'

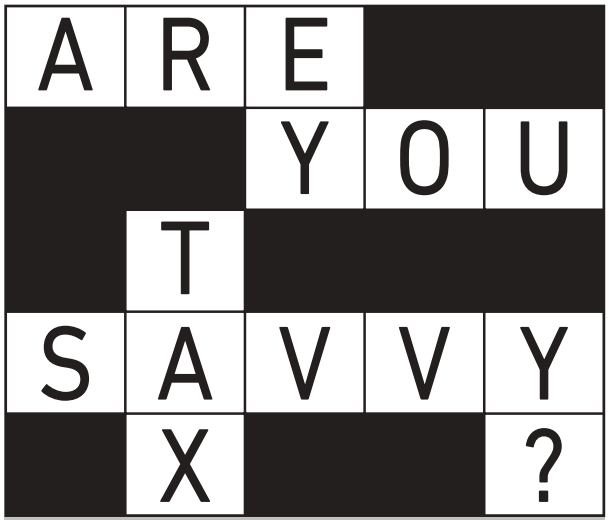
During the conference, several leading global IT companies presented their joint Charter of Trust for a Secure Digital World, calling for shared ownership of IT security by governments and industry.

Meanwhile, top Russian and Indian officials also called for the adoption of regulations, norms, and principles of state behaviour in cyberspace, under the UN's role as a coordinator. They also called for the continuation of the UN GGE activities in drafting the rules.

2. Are countries and companies GDPR-ready?

With three months to go until the EU's General Data Protection Regulation (GDPR) comes into effect, experts are assessing the GDPR-readiness of companies and countries.

Continued on page 3



The taxation of the digital economy continues to generate heated debates, as new tax rules are in the making. Test your knowledge on the main issues and developments regarding taxation policy, with our crossword on page 8.

IN THIS ISSUE

Issue no. 28 of the *Digital Watch* newsletter, published on 28 February 2018, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Stephanie Borg Psaila, Stefania Pia Grottola, Jovan Kurbalija, Marco Lotti, Clément Perarnaud, Roxana Radu, Barbara Rosen Jacobson, Sorina Teleanu | Design by Viktor Mijatović, layout by Aleksandar Nedeljkov, Diplo's CreativeLab | In addition to the *Digital Watch* newsletter, you can find in-depth coverage of developments on the *GIP Digital Watch* observatory (https://dig.watch) and join discussions on the last Tuesday of every month online, or at the GIP (https://dig.watch/briefings) | Send your comments to digitalwatch@diplomacy.edu | Download your copy at https://dig.watch/newsletter/february2018

DIGITAL DEVELOPMENTS IN GENEVA

Many policy discussions take place in Geneva every month. The following updates cover the main events of the month. For event reports, visit the Past Events section on the GIP *Digital Watch* observatory.

Launch of the *Data Diplomacy* report

The GIP hosted the launch of the report *Data Diplomacy: Updating Diplomacy to the Big Data Era*, on 8 February, prepared by DiploFoundation and commissioned by the Ministry of Foreign Affairs of Finland. The report maps the main opportunities of big data in different areas of diplomacy, proposing ways for ministries of foreign affairs to capture its potential, while describing the key considerations to take into account for big data to flourish. The event was attended by diplomatic representations, international organisations, and civil society in Geneva.

Global Commission on the Future of Work: Second Meeting

The second meeting of the International Labour Organization's Global Commission on the Future of Work, on 15–17 February, focused on the main themes to be addressed in the 2019 report, prepared for the ILO centenary. The work of the high-level Global Commission is part of the ILO Future of Work Initiative launched by the ILO Director-General, Guy Ryder, in 2013. In its discussions, the 28-member Commission focused, among others, on the platform economy, skill building, the situation of youth, and universal social protection. The Commission agreed to seek outreach opportunities via technical meetings, collaboration with international organisations, and an information session with member states later this year. The next meeting of the Global Commission will take place in Geneva on 15–17 May.

WSIS Forum: Final Brief

The 2018 edition of the World Summit on the Information Society Forum (WSIS Forum) will be held on 19–23 March in Geneva on the theme 'Leveraging ICTs to Build Information and Knowledge Societies for Achieving the Sustainable Development Goals (SDGs)'. The consultation process for the WSIS Forum finalised on 19 February with a brief on preparations for the event, workshop submission information, and innovations in this year's programme. More than 250 submissions were received from different stakeholder groups, proportionally distributed as follows: 22% government, 22% civil society, 20% international organisations, 19% private sector, and 17% academia. As in previous editions, the week-long event will feature a high-level track (consisting of a moderated policy session, high-level dialogues, the WSIS Prize 2018, and a ministerial roundtable) and a forum track (consisting of thematic and country workshops, interactive sessions, facilitation meetings, knowledge cafés etc.). The 15-year celebration of the Geneva Plan of Action is the highlight of this year's event.

Expert Workshop on the Right to Privacy in the Digital Age

The expert workshop, organised by the Office of the High Commissioner for Human Rights (OHCHR) on 19–20 February, focused on the identification of principles, standards, and best practices regarding the promotion and protection of the right to privacy. The two-day discussion comprised six different thematic panels ranging from the existing legal framework regulating the right to privacy to the role of individuals, governments, business enterprises, and private organisations in the processing of data. Both the panellists and the participants stressed repeatedly the importance of focusing on the collective dimension of rights while addressing data protection. The discussion concluded that further guidance is needed to unpack the available legal framework for the protection of privacy. In addition to developing the principles, greater effort is needed to ensure adequate implementation of existing provisions as there is still a lack of adequate legal and procedural guidance at national level. Furthermore, the emergence of powerful data-driven technology brings both opportunities and challenges – especially considering that there is an increasing reliance on extraterritoriality and demand for access to data stored abroad. The protection of children's rights in the digital space also emerged as a new and important discussion point in the near future.

Roundtable on data partnerships in international organisations

As part of the GIP's Data Talks series, representatives of international organisations gathered on 22 February to discuss how they could best engage in sustainable partnerships with the private sector to obtain new forms of data that could better inform their activities. The session zoomed in on three case studies of such cooperation between international organisations and the Internet industry, focusing on social media firms Facebook and Twitter, and e-commerce giant Alibaba. While it became clear that these kinds of partnerships need a tailored approach, some common lessons appeared, such as the importance of trust-building between organisations, and the need to set clear objectives, roles, and deliverables from the outset.

DIGITAL POLICY TRENDS IN FEBRUARY

Continued from page 1

Although the GDPR is directly applicable in the EU without the need to be transposed into national law, the regulation provides for several areas which allow the member states to regulate within their respective jurisdictions. Over 50 provisions in the GDPR allow for such flexibility.

Countries have been preparing draft legislation to introduce more specific provisions where the GDPR allows for this. An ongoing survey indicates that only one-fifth of EU countries still have to introduce draft bills.

GDPR-readiness is a tougher challenge for companies. A Forrester Research survey found that half of European companies are or expect to be compliant soon. An EY survey found that fewer companies in other markets were GDPR-ready: 27% of companies surveyed in Africa and the Middle East, 13% in the Americas, and 12% in the Asia-Pacific region.

3. New details about proposed EU tax reforms emerge, as pressure mounts

Internet companies are no doubt waiting to see the tax reforms which the EU will propose by the end of March.

This month, new details have emerged. As revealed by Bloomberg, the European Commission is planning two new taxes: (a) a temporary tax on the advertising revenue of large Internet companies such as Facebook and Google – considered to be a 'politically palatable' solution, and (b) a separate tax aimed at online platforms such as Amazon, Ebay, and Airbnb.

The proposals will also introduce the concept of the virtual permanent establishment. In a letter sent to the US Secretary of Treasury, Internet companies have expressed concerns over the impact of these plans on the 'global business climate', and asked the US to 'engage directly and forcefully' in the debate.

Currently, EU member states are split. There are those in favour of tax reforms, such as France and Germany, and smaller countries like Ireland that believe the EU should wait for the OECD's taxation proposals, arguing that tax reform should be tackled on a global level.

The OECD is in fact reviewing options for tackling the tax challenges raised by the digitalisation of the economy. Some EU countries, however, have expressed concern that the process is too slow, and said that the EU should move ahead on its own. Both the EU's proposal and the OECD's interim report are expected in the next few weeks.

4. Computer systems and websites exploited to mine cryptocurrency

In the latest cybercrime trend to have hit the Internet, systems and websites are being exploited to mine cryptocurrency.

Researchers discovered that cryptocurrency mining scripts were operating on Tesla's cloud system, and on thousand of websites around the world. Scientists working at one of Russia's nuclear facilities were arrested for allegedly trying to use the site's powerful computers to mine cryptocurrencies.

The so-called cryptojacking is a relatively new trend in cybercrime. Users are tricked into clicking a link, or visit an infected site, and a script is automatically executed. The script, which taps into the user's computing power, carries out 'accounting' services for the currency, in return for a fee. Cryptocurrency mining is in itself a legitimate way of raising cryptocurrency; exploiting a user's computer without the user's consent is a crime.

If governments are concerned about the use of cryptocurrency for fraudulent purposes, cryptojacking practices will add to those concerns.

5. Child online sexual abuse increasing

This year's Safer Internet Day, on 6 February, served to highlight the growing abuse against children, and the need for stronger cooperation among stakeholders to protect children online. UNICEF estimates that a child goes online for the first time every half a second, every day. The organisation said that children tap into the opportunities offered by the Internet, but also face grave risks.

Child sexual online abuse is on the increase, the WeProtect alliance has revealed. Cybersex trafficking has become a 'brutal form of modern-day slavery'. The alliance believes that authorities should have access, under due process, to the necessary data to protect children, to ensure effective investigation, and support prosecution of offenders.

The Council of Europe's Lanzarote Committee, which monitors the implementation of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, has recommended that countries specifically address the issue of sexual abuse in the circle of trust through dedicated subjects at school.

A new trend is emerging in cybercrime – cryptojacking. This month saw websites and systems exploited to mine cryptocurrency. These include a Russian supercomputer for nuclear research, Tesla's cloud system, and thousands of websites worldwide.

Geneva Internet Platform
DigitalWatch NEWSLETTER

Issue 28: February 2018

OBSERVATORY

DIGITAL POLICY: DEVELOPMENTS IN FEBRUARY

The monthly Internet Governance Barometer tracks specific Internet governance (IG) issues in the public policy debate, and reveals focal trends by comparing issues every month. The barometer determines the presence of specific IG issues in comparison to the previous month. *Read more about each update.*

Global IG architecture

decreasing relevance

The Internet Society launched a Collaborative Governance Project to 'expand the global knowledge and use of collaborative governance processes to solve problems and develop norms'.

Several global companies, including Airbus, IBM, Siemens, and Deutsche Telekom, signed a Charter of Trust for a Secure Digital World.

Sustainable development

same relevance

The Food and Agriculture Organization and Telefonica have concluded an agreement to work together on leveraging the use of digital technologies such as the Internet of Things (IoT) and big data for agricultural development, food security, and nutrition. The World Bank Group and the GSMA also announced a partnership on harnessing big data from the IoT for growth and development.

Security

increasing relevance

Speaking at the Munich Security Conference, UN Secretary General António Guterres called for 'a serious discussion about the international legal framework in which cyberwars take place'.

India and Russia agreed to broaden cooperation on cybersecurity. They also called for norms to govern state behaviour in cyberspace, and for the continuation of the UN GGE. The UK and the USA have publicly accused Russia of being behind the NotPetya ransomware attack in June 2017. Russia denied the accusations as groundless.

The *Worldwide Threat Assessment of the US Intelligence Community*, presented by the US Director of National Intelligence, sees cyberthreats among top global threats in 2018.

A Russian supercomputer for nuclear research, Tesla's cloud system, and thousands of websites worldwide have been exploited to mine cryptocurrencies.

E-commerce & Internet economy

increasing relevance

More than five years after Amazon was given a tax bill of almost €200 million by French tax authorities, the two parties have reached a 'comprehensive settlement agreement' for an undisclosed amount. The European Commission will present its plan for tax reforms for Internet giants by the end of March. According to EU Economic Affairs Commissioner, Pierre Moscovici, 'digital taxation is no longer a question of if', but rather of how.

In a case brought by an Uber driver, the labour tribunal in Paris, France ruled that Uber's 'business is intermediation rather than transportation', and that the driver was self-employed. In Morocco, Uber suspended its activity, due to regulatory uncertainty. The US State Secretary proposes the creation of a Bureau for Cyberspace and the Digital Economy, 'to formulate and coordinate a strategic approach necessary to address current and emerging cyber security and digital economic challenges'.

The European Commission launched the EU Blockchain Observatory and Forum, to help the EU stay at the forefront of blockchain developments. The Indian government announced that it does not recognise bitcoin as a legal tender for payment, and that it will seek for a thorough regulation of the cryptocurrency industry. The General Manager of the Bank for International Settlements warned that cryptocurrencies could become a threat to financial stability. The Swiss Financial Market Supervisory Authority published a set of Guidelines on Initial Coin Offerings (ICOs). Venezuela launched the world's first sovereign cryptocurrency, the petro.

Digital rights

increasing relevance

The Article 29 Working Party released revised guidelines concerning the implementation of the EU GDPR. The European Commission has sent a second letter to the Internet Corporation for Assigned Names and Numbers (ICANN), expressing concerns over the organisation's proposed models for ensuring compliance between its WHOIS policy and the GDPR.

A Belgian court decided that Facebook has been in breach of privacy laws by tracking users on third-party sites. Facebook intends to appeal the ruling.

Jurisdiction & legal issues

increasing relevance

A Clarifying Lawful Overseas Use of Data Act (CLOUD Act) bill introduced in the US Congress seeks to clarify the conditions under which US authorities can access data stored by US companies outside national borders. The bill was welcome by the Internet industry, and received with reticence by human rights organisations.

The European Parliament voted in favour of a new regulation on geoblocking, aimed to facilitate cross-border access to online services, within the EU, preventing the restriction or discrimination of content in particular locations. An exception for copyrighted materials has drawn criticism from consumer rights group.

Infrastructure

same relevance

ICANN decided not to delegate the .corp, .home, and .mail generic top-level domains (gTLDs) because of concerns over collisions with name labels used in private networks.

Foreign affairs ministers of ASEAN countries expressed support for a proposal to build an ASEAN Smart Cities Network.

The Telecom Regulatory Authority of India recommended the adoption of policies to encourage the development of networks especially suited to IoT.

Net neutrality

increasing relevance

In the USA, states are taking measures to preserve net neutrality after the Federal Communications Commission (FCC) adopted the *Restoring Internet Freedom Order* last December. The Internet Association expressed support for the Senate Congressional Review Act resolution, put forward to invalidate the FCC order. Attorneys-general in 22 states and Washington DC re-filed a lawsuit challenging the order.

The Netherlands' Authority for Consumers and Markets denied a request to take action against T-Mobile's alleged breach of net neutrality rules through its zero-rated music streaming offer.

In a report on 'Open Internet and Devices', the French regulator ARCEP noted that neutrality rules should also apply to devices, and not only to networks.

New technologies (IoT, AI, etc.)

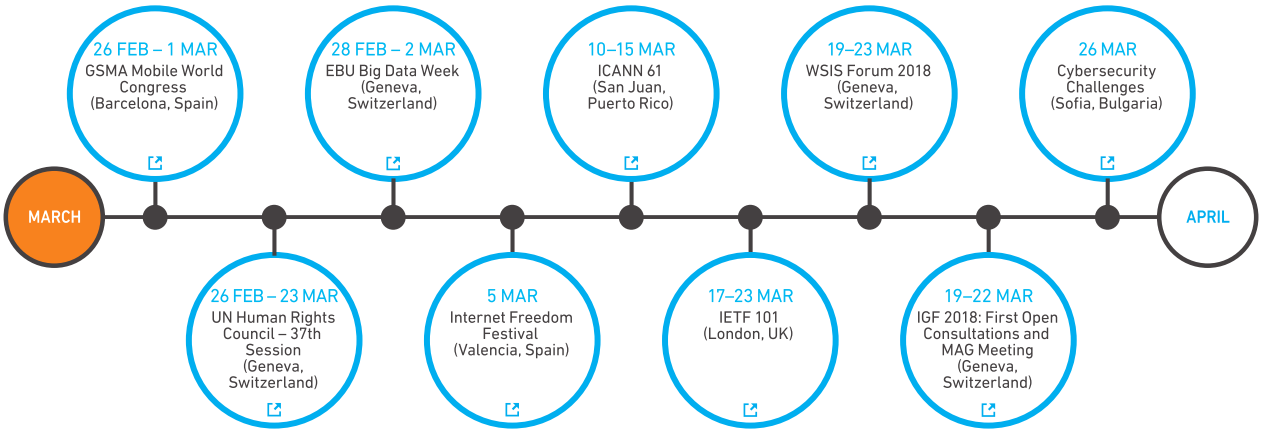
increasing relevance

India is setting up its first artificial intelligence (AI) institute, and has created four committees tasked with preparing a national roadmap on AI.

Germany does not have any intention to procure autonomous weapons systems.

The *Worldwide threat assessment of the US Intelligence Community* lists AI, the IoT, and big data among areas that could generate national security concerns. A report released by academic and civil society organisations outlines security threats that could be generated by the malicious use of AI systems, and makes recommendations on how to better forecast, prevent, and mitigate such threats.

AHEAD IN MARCH



For more information on upcoming events, visit https://dig.watch/events

US CLOUD ACT: IMPLICATIONS AND REACTIONS

In the USA, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) is proposing to establish a new framework for authorities to access data stored abroad and thus amend the Stored Communications Act (SCA). We look at the salient features of the bill, and its implications.

The draft bill, introduced to the US Congress on 6 February 2018, highlights electronic data held by companies as essential for authorities to investigate crime and prevent threats. Currently, authorities claim they are largely unable to access data stored outside the USA in an effective way; companies are also facing conflicting legal obligations across various jurisdictions. The proposed bill therefore aims 'to improve law enforcement access to data stored across borders'.

Preservation and disclosure of communications and records

One of the key parts of the proposed bill introduces a new provision in Chapter 121 of the SCA:

> *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.*

Chapter 121 regulates how and to what extent a public authority can request US providers to disclose data and communications stored online. The amendment would authorise governmental authorities to force US companies to disclose information, even if held in another country.

If approved, this bill could be seen as an exercise of extraordinary jurisdiction, though remaining consistent with long-standing notion of state authority to legislate in areas that have domestic effects. However, the proposed bill would give providers a 'statutory right' to challenge warrants or other legal processes and establish international comities that could limit their reach.

Finally, the CLOUD Act would give the right to providers to notify foreign governments when they receive a legal data request from US authorities about one of their nationals/residents, provided that these foreign governments have entered into agreements with the US government.

Support and criticism

Reactions to the bill have been mixed. Among the actors favouring this bill are the tech companies; human rights organisations and NGOs are strongly opposed to it. Tech companies, including Apple, Facebook, Google, Microsoft, and Oath, signed a letter supporting the bill, stating that it 'reflects a growing consensus in favor of protecting Internet users around the world and provides a logical solution for governing cross-border access to data.'

However, the Electronic Frontier Foundation (EFF) argues that the draft bill constitutes 'a dangerous expansion of police snooping on cross-border data'. In EFF's view, the bill would provide US law enforcement agencies with access to content about individuals wherever they live or where the information is stored.

The bill would offer to the US President the possibility to enter into 'executive agreements' with foreign governments, and thus provide them with data on users regardless of the respective privacy laws of these countries. It would also lead to the failure of Mutual Legal Assistance Treaties (MLATs), which would better guarantee data protection.

Other privacy groups such as the Open Technology Institute (OTI) and Access Now also oppose the bill, claiming that sufficient safeguards for privacy, civic liberties, and human rights are lacking.

CLOUD Act in context: the Microsoft Ireland case

The CLOUD Act needs to be understood in the light of past legal cases that have shone a spotlight on the issue of the extraterritorial application of US law.

The dispute in the Microsoft Ireland case emerged when the US Department of Justice issued a warrant requesting Microsoft to hand over the details and content of an e-mail account – related to a suspected drug trafficker ¬– stored in Ireland. Initially, Microsoft denied to comply: Since the data and communication requested was located in Microsoft's Dublin datacentre, Microsoft has argued that US authorities should have used their legal international channel with Irish authorities in order to obtain these communications. A federal judge initially upheld the warrant, but then the Second Circuit determined that 'that execution of the warrant would constitute an unlawful extraterritorial application of the Act'. The US authorities, however, considered the warrant valid, since it had international reach, and counter-appealed the Second Circuit decision to the Supreme Court.

The decision of the Supreme Court will have profound implications for US laws regarding data requests, and in all likelihood for the CLOUD Act.

CLOUD Act and the GDPR

Though the CLOUD Act and the GDPR are essentially different in their aim and scope, the CLOUD Act may enter into conflict with certain provisions of the GDPR. Experts believe that the GDPR (article 48) addresses foreign – including US – investigations and prohibits the transfer or disclosure of personal data unless pursuant to an MLAT or other international agreement. This example tends to illustrate the seemingly diverging dynamics of Europe and the USA in dealing with privacy and data requests.

The CLOUD Act will likely be the subject of further discussions at national and international levels. It constitutes a strong stance by the US government and also reflects the partial obsolescence of current national legal frameworks and the challenges of international regulations in the digital era.

THE FUTURE OF WORK: PREPARING FOR AUTOMATION AND THE GIG ECONOMY

The increasingly digitalised world, the sharing economy, and the ongoing developments in automation and AI bring changes to the world of work. Several reports and studies released this month shed light on how these changes could look, how employers and employees perceive them, and what stakeholders can do to better prepare for the new world of work.

UK to adapt legislation to the 'gig economy'

The so-called gig economy (or sharing economy) has brought new jobs, but also concerns about the rights and protection of people working in these new business models. Governments have started to pay more attention to these concerns, the most recent example coming from the UK.

In July 2017, a report commissioned by the UK government stated that the gig economy brings benefits to individuals (such as flexibility and control over how they work), but the employment legal framework needs to better protect them. The *Good Work* plan released this month proposes several measures for ensuring a balance between protecting the opportunities offered by 'platform-based working', and ensuring fairness for 'those who work through these platforms and those who compete with them'. Among them is the introduction of the concept of 'dependent contractors' for gig-economy workers, and legal clarifications and practical tools to easily distinguish between employees and dependent contractors.

New insights into the impact of automation on jobs

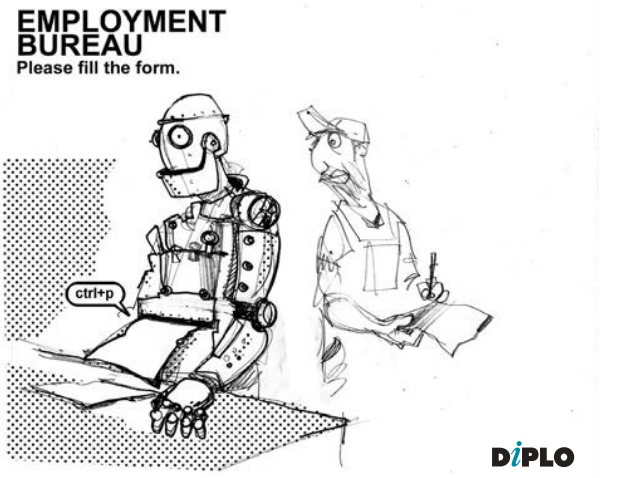
Concerns about the future of work also come from ongoing technological advancements in automation and AI. Some worry that job automation will lead to significant unemployment rates. Others argue that technological progress will also generate new jobs, compensating for those lost, without significantly affecting employment rates.

PricewaterhouseCoopers' latest study foresees three waves of automation in the next 20 years:

- Wave 1 – algorithmic (to early 2020s). Based on automation of simple computational tasks, this wave would see low displacement of jobs – around 3%.
- Wave 2 – augmentation (to late 2020s). A 'dynamic interaction with technology for clerical support and decision making' will affect more jobs.
- Wave 3 – autonomy (to mid-2030s). Up to 30% of jobs could be automatable.

Throughout all three waves, jobs automation is expected to vary significantly by industry sector, country, and type of worker. Overall, only around 20–25% of jobs in East Asian and Nordic economies are likely to be automated by the mid-2030s, while the percentage rises to over 40% in Eastern European countries. While transportation, manufacturing, and construction jobs are expected to be automated in a proportion of 40–50% by the mid-2030s, human health, social work, and education are less exposed. Highly educated workers will be faced with a lower potential of job automation, and women are likely to be more strongly affected by automation than men in the first two waves.

The report suggests several measures to 'help people adjust to the new technologies': education and (re)training, supporting job creation, protecting workers' rights, and strengthening social safety nets. And, despite concerns about jobs being lost due to technological progress, governments and companies should support and invest in these new technologies. Otherwise, they will miss the opportunity to be at the forefront of technological progress, with negative social and economic consequences in the long run.



What do employers and employees think about AI at the workplace?

While many studies focus on predictions about the impact of automation and AI on jobs, there seems to be less insight into how this impact is perceived by companies and workers. Two studies published this month shed some light on this area.

According to a survey conducted by Willis Towers Watson in 38 countries, over half of the surveyed employers (57%) consider that the main goal of automation is to augment human performance and productivity (as opposed to replace humans to save costs). However, 38% of the employers surveyed declared themselves unprepared to identify reskilling pathways for people whose work is being affected by automation.

Employees seem to be 'cautiously optimistic' about the impact of AI on their work. A survey conducted by the Workforce Institute and Coleman Parkes Research in 8 countries found that only 34% of employees are concerned that AI would replace them at some point, while two-thirds would be more comfortable if employers were more transparent about how they plan to use AI in the workplace.

What next?

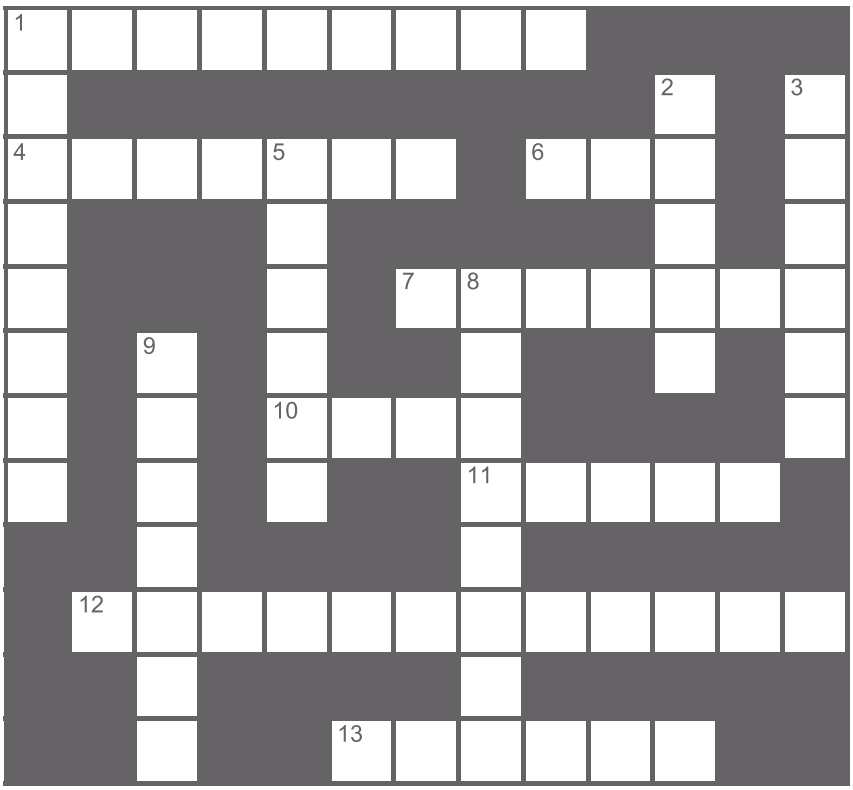
It is clear that digitalisation, automation, and AI will impact the world of work. So what measures should be taken, and by who, to ensure the future of work is a future we all want and can benefit from? The Global Commission on the Future of Work, established by the ILO, is one of the venues where such questions are being explored. It is likely that these issues will remain in focus for the years to come.

CROSSWORD

TEST YOUR KNOWLEDGE ON INTERNET TAXATION ISSUES

The taxation of Internet companies is one of the heated debates of the moment. Proposals from the European Commission and the OECD, expected in the weeks to come, and the introduction of new taxes in other countries worldwide are two of the signs that the taxation of the digital economy will remain high on public policy agendas this year.

Test your knowledge on the main issues and updates regarding taxation issues. Consult our dedicated space on the *Digital Watch* observatory to find answers to most of the clues.



Across

1 Asian country that has recently announced the introduction of a goods and services tax on imported digital services starting January 2020. (9)

4 The name of the country involved In the famous 'sweetheart tax' ruling in 2016; the European Commission ordered Apple to pay this country up to €13 billion in taxes. (7)

6 Acronym of the intergovernmental organisation dealing with trade, which in 1998 introduced a moratorium which rendered all electronic transmissions free of custom duties among member states. (3)

7 Tax authorities are concerned that _____ and other virtual currencies are increasingly being used for money laundering and tax evasion. (7)

10 Acronym of the intergovernmental organisation which is expected to present an interim report on the issue of taxation in the digital economy in the coming weeks. (4)

11 The 'Double _____' and the 'Dutch Sandwich' arrangements are some of the approaches used by Internet companies to shift revenues to different jurisdictions. (5)

12 High judicial body in the USA which is revisiting a tax ruling from 1992 that allowed the Internet to be a largely 'tax-free zone'. (7,5)

13 In 1998, the _____ Principles adopted by the Organisation for Economic Co-operation and Development (OECD) stated that taxation of e-commerce should be based on the same principles as taxation for traditional commercial activities. (6)

Down

1 The strategy which companies use to move profits to low-tax or no-tax jurisdictions is called profit _____. (8)

2 At the World Economic Forum annual meeting in January 2018, philanthropist George _____ criticised major IT companies for their 'monopolistic behaviour' and stated that regulation and taxation pressures could break their global dominance. (5)

3 European country which presented one of the first comprehensive reports on Internet taxation, back in 2013. (6)

5 Internet company which this month reached a settlement agreement with France after receiving a tax bill of almost €200 million. (6)

8 Sales tax, value added tax, and goods and services tax are examples of the so-called _____ taxation. (8)

9 Under the concept of _____ permanent establishment proposed by some EU countries, Internet companies would be taxed where value is created, rather than where the companies are registered. (7)

Across: **1** Singapore, **4** Ireland, **6** WTO, **7** Bitcoin, **10** OECD, **11** Irish, **12** Supreme Court, **13** Ottawa.
Down: **1** Shifting, **2** Soros, **3** France, **6** Amazon, **8** Indirect, **9** Virtual

ICANNWIKI.ORG

giving everyone a voice in the future of the internet

BACK COVER
CLOCKWISE

Javier Rua-Jovet
Susannah Gray
Klaus Stoll
Pablo Rodriguez

FRONT COVER
LEFT TO RIGHT

Ashley Clemente
Avri Doria