Legislative / Regulatory Report 3

This report is a limited list of some recent legislative and regulatory initiatives around the world that relate to data protection, cybersecurity issues and e-privacy/e-evidence that could impact ICANN's mission, operations or issues within ICANN's remit. This is the third such report in a periodic series of reports about potential legislative efforts so that ICANN and the community are better prepared for potential impacts.

The information has been updated and augmented based on new entries and the status reflects information as of 31 December 2018. While we try to track information in real time, occasionally it takes time for the existence of proposals, and/or the potential impact of those proposals on ICANN to become evident.

Recent and Pending Privacy/Data Protection and Cybersecurity Legislation and Regulation: Overview of Ongoing and Pending Initiatives

Privacy and Data Protection

AFRICA AND MIDDLE EAST

Benin
Code du Numérique : Digital Economy Law
The Code du Numérique of Benin addresses various issues pertaining to cybersecurity, security of information systems and the protection of privacy and personal data handling in Benin. Initially enacted in June 2017 the Digital Economy law in January 2018 began its implementation phase. Section 5 covers data protection and privacy. The Ministry in charge of digital economy is in the process of developing the regulations under the law.
No changes since the last report.

South Africa
The Protection of Personal information (POPI) Act
The Protection of Personal Information Act 4 of 2013 ("POPI") introduces an overarching regulatory framework for the processing of personal information. The Act was signed into law on 19 November 2013. Through POPI, the government intends to promote the protection of personal information processes by public and private entities. POPI also provides for the establishment of an information Regulator. POPI was signed into law in November 2013. Those provisions which deal with the establishment of the Information Regulator came into effect on 11 April 2014. The

process for appointing the Information Regulator began in April 2015 with a request from Parliament for the nomination of candidates. Since then the Portfolio Committee responsible for the nominations has held public consultations with relevant stakeholders regarding POPI and its relation to other legislation regarding access to and protection of information. Five candidates were nominated, and Parliament voted for the nominees to run the newly -formed office of the Information Regulator; three in a full-time capacity and two as part-time members. This recommendation has been referred to the Minister of Justice and Correctional Services.

No changes since the last report.

Kenya

The Data Protection Bill 2018

On 15 May 2018, Kenya published a draft data protection bill for public consultation Draft bill aims to harmonize existing legislation and provide an overarching regulatory framework for processing personal data in Kenya.

http://parliament.go.ke/the-senate/house-business/bills
http://parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf

Qatar

Law No.13 of 2016 Concerning Personal Data Protection (DPL)

In November 2016, Qatar enacted DPL (Personal Data Protection) a specific law relating to data protection. The law was supposed to be implemented around mid-2017 but the government has had to provide an extension to allow organizations more time for compliance.

No changes since the last report.

Bahrain

Personal Information Protection Law

Law 30/2018 on protection of personal data was published on 19 July 2018 and will come into effect on 1 August 2019. The law addresses the protection of personal and private information and applies to every individual and every legal person (corporation) having a place of business in the Kingdom of Bahrain. The law is pending implementation.

Turkey
Data Protection Law (DPL)
Similar in content to the GDPR the Turkish Data Protection Law (DPL) was enacted in April 2016. The Law was implemented during a two-year transitional period, whereby various provisions entered into force at different times. The DPL originates from the European Union Directive 95/46/EC. The Personal Data Protection Board is the national supervisory authority in Turkey and has published draft versions of the secondary legislation and booklets on implementation. The DPL deals with data processing grounds, purpose limitation, definitions of consent, and cross border transfers of data.
No changes since the last report.

Lebanon
e-transactions
Parliament has endorsed a e-transaction law governing digital documents and contracts for individuals and businesses including legal rights and penal provisions for the misuse of data, privacy, and modification. http://www.ict.pcm.gov.lb/ict/English/DocumentsDetails.aspx?pageid=859 Please see the Presidency of the Council of Ministers website www.ict.pcm.gov.lb

Morocco and Tunisia
Data Privacy Laws
Morocco and Tunisia have had public debates and discussions about updating existing data privacy laws to provide more protection of the processing of personal data and the possibility of bringing national frameworks closer to the EU General Data Protection Regulation while still reflecting local requirements.

ASIA PACIFIC

India
India Proposed Data Protection Framework

The Government of India plans to bring legislation which will define individual's right to privacy as per the Constitution of India. The key issues covered in a white paper that the Government of India issued seem to suggest conceptual reliance on the European GDPR process. The Government set up an expert committee in August 2017. In November 2017 the committee published a white paper - detailing all issues related to the subject and in the India context - for public comments. Open house discussions have been organized in several Indian cities. Based on inputs received, a draft law will be proposed. The Personal Data Protection Bill of 2018 had been expected to be placed for ratification in both houses of parliament during the Winter session of Parliament which ran from 11 December 2018 to 8 January 2019, but that did not happen. Now that Parliament is in recess and there are general elections in April 2019 it is not anticipated that the bill will be discussed until later in 2019.

White paper: http://bit.ly/2n22joJ

National Digital Communications Policy 2018

First released for public comment 1 May 2018, the National Digital Communications Policy was approved by the Cabinet of Ministers on 26 September and notified by the Government on 22 October 2018 and the policy is now in force. Among other provisions it establishes a Data Protection Regime by harmonizing communication law and insuring data protection and security principles are applied and enforced. This includes assuring security of digital communications

China

Cybersecurity Law Implementation

To implement the Cybersecurity Law referenced below in the Cybersecurity section of this report, three documents have been released, with final versions still to be determined:

- The Cyberspace Administration of China (CAC) released the first draft of Measures for the Security Assessment of Transborder Transfer of Personal Information and Important Data on 11 April 2017. The draft measures specify the content and criteria of conducting the security assessment. Network operators will undergo governmental assessment if they transfer more than 1000 GB of data or data on more than 500,000 people from China to abroad. For data transfers below that threshold self-assessment will apply.

- The National Information Security Standardization Technical Committee released a second draft of Guidelines for Trans border Data Transfer Security Assessment on 30 August 2017. It further clarified the definition of cross-border data transfer and the conditions that initiate government security assessment.

- CAC released the first draft of Regulation on the Protection of Critical Information Infrastructure (CII) on 10 July 2017. The draft regulation clarified the scope of CII and elaborated on how CII operators should protect their networks against cybersecurity threats. It also set out additional obligations for CII operators, including cooperating with the relevant government agencies to conduct spot inspections.

EUROPE

European Union
General Data Protection Regulation (GDPR)
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. It came into force on 25 May 2018.
No changes since the last report.
e-Privacy Regulation
Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Main elements of the proposal: • It provides updated privacy rules in light of the revision of the GDPR & tries to ensure consistency between both instruments. • It extends scope to cover Over-The-Top (OTT) media services and protects the confidentiality of the device. • It sets Do Not Track (DNT) as an option in browser settings; websites may still obtain the consent of the user at website level • It aims to achieve greater harmonization among Member States by transforming this Directive into a Regulation applicable uniformly across EU Member states. The proposed Regulation is under negotiation at the EU co-legislators' level (the European Parliament and the Council). Proposed text of the Regulation: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en
No changes since the last report.

Regulation on a framework for the free flow of non-personal data in the European Union
Policy objective – to support the free-flow of non-personal data as a pre-requisite for a competitive data economy within the Digital Single Market. To ensure the free flow of data this regulation is intended to allow companies and public administrations to store and process non-personal data wherever they choose in the EU. To achieve this, the proposed regulation restricts data location restrictions imposed by Member States' legislation. The proposed Regulation is under negotiation at the EU co-legislators' level. Background to the proposal and the proposed regulation is at: https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data and https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data

Russia
"Yarovaya Law" (Anti-terrorism amendments)
Originally signed into law 6 July 2016, the laws had a partial compliance deadline of 1 July 2018, with a full implementation deadline of 1 October 2018. The amendments affect telecom operators and Internet providers included in the register of information disseminators on the Internet, a Russian registry maintained by Internet watchdog Roskomnadozr. Large foreign service providers not in the register, do not currently fall under the law. The register-listed service providers are required to store text messages, voice information, images, sounds, video, and other electronic messages of users, including user correspondence for six months, and metadata for three years. In addition, cellular operators and Internet providers must provide information to law enforcement agencies upon request and without a court order and provide encryption keys to relevant security agencies
No changes since the last report.

LATIN AMERICA - CARIBBEAN

Brazil
General Data Protection Regulation (LGPD)
The General Data Protection Regulation (LGPD) requires that any company that gathers, and processes personal data, (such as name, address, email, among others) obtained by electronic or physical means, needs the consent of the owner of such information. The Bill grants the data owner the right to access his collected information and correct it and obligates companies to inform data owners immediately if any data leaks occur. The LGPD also provides for the creation of a regulatory body to manage

these issues. The draft of the LGPD was approved by the Senate and sent to the President on 10 July 2018.

Chile
Personal Data Protection Law No. 19628
A consolidated bill to amend the Personal Data Protection Law was approved by the Senate in April 2018. The amendments establish general provisions regarding personal data processed by third parties including informing data subjects of the purpose for which the data will be stored and securing written consent. The amended law also designs the new Chilean Personal Data Protection Agency. Lawmakers have been working on a reform of the law for several years and that legislative process is still underway.

To date, Privacy, Data Protection and Data Retention legislations have been passed or are in discussion in Columbia, Mexico, and Peru.

NORTH AMERICA

United States
Clarifying Lawful Overseas Use of Data Act (CLOUD). Enacted March 23, 2018
The Clarifying Lawful Overseas Use of Data (CLOUD) Act amended the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel US-based tech companies via warrant or subpoena to provide requested data stored on servers regardless of the location of the servers (whether or not the data is stored on US or on foreign soil). The CLOUD Act expanded the geographic reach of the SCA but does not change who is subject to the SCA (providers of electronic communications services and remote computing services) or what type of data is subject to law enforcement request (content of electronic communications and cloud stored documents, as well as non-content data relating to electronic communication such as transmission records and user-account information.) The CLOUD Act asserts that US data and communication companies must, when requested by US law enforcement warrant, provide stored data for U.S. citizens on any server the companies own and operate. It also provides mechanisms for the companies or the courts to reject or challenge these requests/warrants on the basis that the request violates the privacy rights applicable within the foreign country in which the data is stored. The CLOUD Act also provides for foreign law enforcement agencies expedited alternative to mutual legal assistance treaties (MLATs) through "executive agreements"; the Executive Branch is given the ability to enter into bi-lateral agreements with foreign countries.

Previously to this change, foreign law enforcement agencies were generally directed to submit a request for mutual legal assistance to the US Department of Justice, which then made the data request to the US provider so that the requests were under the law enforcement exemption in the SCA. The CLOUD Act permits foreign law enforcement agencies from countries with an Executive Agreement with the US Government to make requests directly to the US service providers as long as the data request: identifies a specific person, account, address, or personal device; is limited in time and scope; is for the purpose of obtaining information related to a serious crime, including terrorism; is supported by articulatable and credible facts; and remains subject to review by a court. A provider may still move to modify or quash a data request if it reasonably believes the customer or subscriber is not a US person and does not reside in the US, and that the disclosure would create a material risk the provider would violate the laws of the foreign government.
No changes since the last report.

Cybersecurity

AFRICA

African Union
The Africa Union Convention on Cybersecurity and Personal Data
The Africa Union Convention on Cybersecurity and Personal Data was proposed in 2014; it is yet to be ratified by the required minimum of 15 members states. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
No changes since the last report.

ASIA PACIFIC

Australia
Assistance and Access Bill (Anti-Encryption Bill)
The legislation has passed the Australian House of Representatives but is yet to become law. Once confirmed, this legislation will require technical companies to assist law enforcement to bypass encryption in private messaging apps, as long as the backdoors do not constitute a systemic weakness in the service's security.

China
Cybersecurity Law
The Cybersecurity Law states the requirements for the collection, use and protection of personal information, presents a definition of network operators and security requirements, and places greater demands on the protection of "critical information infrastructure." It requires that personal information/important data collected or generated in China to be stored domestically, and if data is transferred abroad it needs to go through a security assessment. It is worth noting that the law is general; enforcement of the law will depend on the publication of the relevant measures and guidelines. Registration data must be stored within China. Combined with Cyberspace Administration of China's (CAC) Measures for the Security Assessment of Trans border Transfer of Personal Information and Important Data, companies must undergo governmental assessment if they transfer more than 1000 GB data or data on more than 500,000 people from China to abroad. Otherwise, self-assessment will be conducted. The Law was passed in November 2016 and came into effect on 1 June 2017. See Privacy and Data Protection section above for companion legislation
No changes since the last report.

EUROPE

European Union
EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)
Main elements of the proposal: Voluntary European Cybersecurity certification framework to enable creation of individual EU certification schemes for ICT products and services. The proposed legislation is still under negotiation by the co-legislators (European Parliament and Council). Some issues still under discussion include, identifying who has the initiative to start work on certificates, and whether some sectors should be legally obligated to certify products Text of the proposal: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0225(COD)&l=en The proposed regulation is still under negotiation.

EU Directive on Security of Network and Information Systems (NIS)
Part of the EU cybersecurity strategy led by 3 EU Commission Directorate-Generals (CONNECT, JUST and HOME - and European External Action Service (EEAS)). First published in July 2016, the directive has been adopted at the level of the EU Council and the Parliament. The deadline for national transposition by the EU member states was 9 May 2018. The aims of the directive: • Improving cyber security capabilities at the national level. • Increasing cooperation on cyber security among EU member states. • Introducing security measures and incident reporting obligations for Operators of Essential Services (OESs) in Critical National Infrastructure (CNI) and Digital Service Providers (DSPs). Member States are responsible for determining which entities meet the criteria of the definition of OESs, including whether IXPs, DNS Service Providers; TLD name registries are OESs. The list of identified operators should be reviewed regularly by Member States and updated when necessary. NIS covers 'operators of essential services'; but the process of determining which services are treated as 'operators of essential services' is still underway. Therefore, the legislation is still pending implementation until the categorization of services are completed. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=FR
E-evidence
The Commission proposed and published on 17 April 2018 new rules in the form of an Electronic Evidence Regulation and a Directive. By introducing the regulation proposal on European Production and Preservation Orders for electronic evidence in criminal matters, it aims to improve the facilitation, securing, and gathering of electronic evidence stored, or held by service providers in another jurisdiction. The Regulation is complemented by a Directive laying down rules on the legal representation in the Union of certain service providers for the purposes of gathering evidence in the framework of criminal proceedings. Providers of Internet infrastructure such as IP address and domain name registries, domain name registrars and associated privacy and proxy services are within the scope of the proposed legislation. The proposed regulation is still under negotiation. Proposed regulation: https://ec.europa.eu/info/files/proposal-regulation-cross-border-access-e-evidence_en Directive: https://ec.europa.eu/info/files/proposal-regulation-cross-border-access-e-evidence_en

Russia
Sovereign RuNet legislation
Proposed legislation was submitted to the State Duma (Russian Parliament) at the end of 2018 to create autonomy for the operation of RuNet. The proposal is meant to ensure continued operation of the Russian segment of the Internet in the case of disconnection from foreign servers. The proposed legislation would create the mechanism for setting up rules for traffic routing which would create “an infrastructure that allows to ensure the operability of Russian Internet resources in case of impossibility of connecting Russian telecom operators to overseas root servers of the Internet.” All network operators would be required to install “technical means” allowing the determination of the source and direction of all traffic and thus to ensure network operators abide by the routing rules (or amendments to them) as prescribed by the regulator (RosComNadzor) to counter threats when required. In cases of threats to the integrity, stability and security of the functioning of the Internet in the country, the service will exercise centralized network management in a manner determined by the government. Additionally, there has to be equipment installed to allow filtering online resources with content prohibited in Russia. This system of organizing the exchange of traffic on the Russian territory must pass only through identified IXPs and according to certain rules to be specified. The legislation requires IXP owners notify RosComNadzor of their activities, ASs and routes used and the usage of software and hardware in compliance with the regulator’s requirements. It is also proposed to create a national system for obtaining information on domain names and network addresses, a certain registry that will duplicate the list of domain names and autonomous system numbers delegated to Russian users. http://asozd2c.duma.gov.ru http://asozd2c.duma.gov.ru/addwork/scans.nsf/ID/E794ACF3791E3C7B43258363004AC230/$FILE/608767-7_14122018_0138233894-1.pdf?OpenElement
Draft law to be discussed in the Douma in early 2019

MIDDLE EAST

Egypt
Cybercrime Cybersecurity Law
The cybercrime law includes 45 articles that cover blocking websites, protection of privacy, e-crimes, the creation of fake accounts and the protection of personal data. Signed by the President in August 2018 the legislation is pending implementation as Executive statutes are required. It is expected that the Executive Statues should be issued in early 2019. Full text of the law: http://www.laweg.net/Default.aspx?action=ViewActivePages&ItemID=112278&Type=6