Legislative / Regulatory Report Q3 FY18

This report is a limited list of some recent legislative and regulatory initiatives around the world that relate to privacy/data protection and cybersecurity issues and that could impact ICANN's mission, operations or issues within ICANN's remit. It's becoming increasingly important that we, as both an org and a community, pay closer attention to potential legislative efforts so that we are prepared for any impacts.

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 Numerique: Digital economy law
The Code du Numerique 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 is currently (January 2018) moving into its implementation phase.

South Africa
The Protection of Personal information (POPI) Act
POPI introduces an overarching regulatory framework for the processing of personal information. The Act was signed into law on 19 November 2013. POPI intends to promote the protection of personal information processes by public and private entities. POPI also provides for the establishment of an information Regulator. The Protection of Personal Information Act 4 of 2013 ("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. Expectations are that the President will proclaim the rest of the provisions of POPI into effect once the Information Regulator has been established but the Information Regulator has not been appointed yet. 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 information and protection of information.

Qatar
Law No.13 of 2016 Concerning Personal Data Protection (DPL)
In Nov 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 to comply.

Turkey
Data Protection Law (DPL)
Similar in content to the GDPR the Turkish law was enacted in April 2016. Regulatory implementation began in 2017 and Turkey has set May 2018 as the deadline for compliance with the law. The Turkish Data Protection Law 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 boarder transfers of data.

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 legislation will need the validation of the Prime Minister's cabinet of ministers and then go to both houses of parliament for ratification. While no deadline has been given for the process, it will likely take most of 2018 to conclude. White paper: http://bit.ly/2n22joJ

China
Cybersecurity Law Implementation

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

1. 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.
2. The National Information Security Standardization Technical Committee released a second draft of Guidelines for Transborder 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.

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 will come into force on 25 May 2018.
ePrivacy 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: 1. Proposal provides updated privacy rules in the light of the revision of the GDPR & tries to ensure consistency between both instruments. 2. It extends scope to cover Over-The-Top (OTT) media services and protects the confidentiality of the device. 3. Proposal sets Do Not Track (DNT) as an option in browser settings; websites may still obtain the consent of the user at website level 4. Achieving 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

Regulation on a framework for the free flow of non-personal data in the European Union
Policy objective - using a regulation to restrict 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

LATIN AMERICA - CARIBBEAN

Brazil
Three law projects about data protection currently in different houses (PL 5276/2016; PLS330/2013 and PL4060/2012)
The objective is to have new legislation addressing personal data (equivalent to GDPR). It is expected that the three proposals will be combined in a single piece of legislation. In 2017 there were 11 public hearings and 1 international seminar on the legislation. In 2018, it is expected that the data legislation will be advanced.

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

ASIA PACIFIC

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.

1. Registration data must be stored within China;
2. Combined with Cyberspace Administration of China's (CAC) Measures for the Security Assessment of Transborder 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.
3. 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.

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 under negotiation by the co-legislators (European Parliament and Council). Text of the proposal: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0225(COD)&l=en
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 and is being transposed to each member state. Implementation might be as early as June 2018. The aims of the directive: 1. Improving cyber security capabilities at the national level. 2. Increasing cooperation on cyber security among EU member states. 3. Introducing security measures and incident reporting obligations for operators of essential services (OESs) in critical national infrastructure (CNI) and digital service providers (DSPs). 4. 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.

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=FR
e-Evidence
The e-Evidence proposal was published on 17 April 2018. It includes the electronic evidence Regulation which aims at facilitating securing and gathering of electronic evidence in the framework of criminal proceedings stored or held by service providers in another jurisdiction, by introducing European Production and Preservation Orders. 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. Press release and the proposed legislation are at: http://europa.eu/rapid/press-release_IP-18-3343_en.htm Electronic evidence regulation Legal representatives directive