IAPP Global Legislative Predictions 2017

In anticipation of another big year in privacy, this week's Privacy Tracker legislative roundup consists of contributions from around the globe on expected and potential legislation. With 25 contributions from countries and regions spanning Argentina to Zimbabwe, hopefully we've hit on some important upcoming developments you should have on your radar.

Argentina
Pablo Palazzi, Allende & Brea

The year 2017 predicts an interesting year for data protection in Argentina. The data protection authority, with a new director, has issued several resolutions related to inspections, registration of databases, international transfer agreements and sanctions. In addition the DPA has started an open consultation at the start of 2016 to discuss the possibility of amending the Personal Data Protection Act following the principles of the EU General Data Protection Regulation. The consultation finished and the DPA published on December 19, 2016, a compilation of all the comments to the possibility of amending the law. So we expect 2017 to be a year of debate and activity of the DPA.

Australia
Carolyn Lidgerwood, Rio Tinto Limited

Once again, proposed mandatory data breach reporting legislation is before the Australian Parliament (Privacy Amendment (Notifiable Data Breaches) Bill 2016). It's a fair bet that 2017 will be the year that data breach reporting finally becomes a legal requirement. Many APP entities respect the current Office of the Australian Information Commissioner voluntary reporting scheme, but as the privacy commissioner observed at the 2016 iappANZ summit, many don't. Mandatory reporting raises the stakes. For IAPP members working across jurisdictions, note that the Australian bill has more in common with the pending Canadian data breach reporting scheme (under PIPEDA) than with Articles 33 & 34 of the EU GDPR.

Other things to watch for in 2017: (a) Draft legislation prohibiting conduct relating to "re-identification of de-identified personal information" published or released by (federal) agencies (Privacy Amendment (Re-identification Offence) Bill 2016), which (controversially) includes criminal offences; and (b) the federal government's response to the Productivity Commission's report into "Data Availability and Use." More than a few privacy law issues were raised by the 600+ page draft report; the final report is due before end March. Also keenly awaited is the decision of the full bench of the federal court in the Ben Grubb matter (Privacy Commissioner v. Telstra Corporation Limited), relating to the scope of personal information regulated under the Privacy Act.

Brazil
Renato Leite Monteiro, CIPP/E, Universidade Mackenzie

2016 was a hot year in Brazil for privacy and data protection, and for this year the movements shall not be different. The main focus should go to the bills related to the General Data Protection Law. Two main initiatives are competing towards the finishing line, one in the federal Senate and another in the House of Representatives. Regarding the former, more than ten public hearings will take place at the National Congress to discuss the main points of the Bill of Law 5276/2016, which is very similar to the European General Data Protection Regulation. A final report is expected by the end of the first semester. The Senate bill is already waiting for its final report to be published.

In December, a Presidential Provisional Measure altered the federal law that regulates issues such as credit reports and scoring methods (Federal Law 12414/2011) to make it automatic for personal data to be included on positive credit databases controlled and managed by private data brokers (mandatory opt-in). Citizens now have to opt out from these databases. This measure has already been targeted by critics from the federal Public Prosecutors' Office and consumer groups alleging privacy and data protection rights violations.

On top of all that, Marco Civil da Internet, the law that confers user rights and Internet services obligations, will continue to suffer several amendment attempts, from user consent requirements, net neutrality exceptions to content removal provisions. Courts will also continue to interpret the norm in very different forms, causing legal uncertainty and an unstable commercial and economic Internet environment.

In conclusion, 2017 will probably be a tumultuous and curios year to privacy rights in Brazil.

Canada
Shaun Brown, nNovation

There are a few legislative developments to watch for in 2017. First is the private right of action under Canada's Anti-Spam Legislation, which is to come into effect on July 1. The PRA is a big deal, as it will allow any person affected by an alleged violation of CASL to sue for actual and statutory damages. This opens the door to class-action lawsuits against businesses that violate the law (whether intentionally or by mistake), with no need to prove harm.

CASL is also supposed to be reviewed by Parliament beginning on July 1. It is doubtful that the review will begin then, but it might begin later in 2017.

Finally, we should see draft regulations sometime this year from the federal government that are required for the breach notification requirement under the Personal Information Protection and Electronic Documents Act to come into effect.

China
Galaad Delval, CIPP/E, EY Chen & Co. Law Firm

2016 ended up with one of the most important piece of legislation concerning privacy protection and cybersecurity passed by the National People's Congress in the form of the "Cybersecurity Law." This year we should expect supporting guidelines and regulations to interpret and implement the CSL. Among those should be published the final criteria for the examination and definition of the critical information infrastructure (CII) as per the requirement of the CSL along with the relevant guidelines for the security assessment of CII cross-border data transfers. It is to be noted that the national information security standardization technical committee has drafted multiple guidelines such as the "Personal information security specification" and a set of standards covering the "Baseline for Cybersecurity Classified Protection" last year that should go forward toward adoption this year among other standards. Finally, while the draft of the "E-commerce law" was adopted and made public for comments last December, it should be followed this year to see its evolution toward the final version.

EU
Tim Van Canneyt, CIPP/E, Field Fisher Waterhouse

2017 is definitely the year of the GDPR. Not only will organizations need to spend a lot of time assessing and updating their data processing activities, we may also expect additional guidance from the Working Party 29 on some of the more sticky topics of the GDPR. In addition, marketers, telcos and website operators will need to follow up closely on the e-privacy reform. Following the leaked draft end of last year, we may expect a lot of discussions on this topic at the EU level.

France
Myriam Gufflet, CIPM, Promontory Financial Group

A major change introduced by the French Bill for a Digital Republic, adopted in October 2016, and which anticipates the GDPR to some extent, is an increase in the fines that can be imposed by the French supervisory authority, the CNIL. The maximum fine has been raised from EUR 150,000 to EUR 3 million. It can therefore be assumed that organizations will pay even greater attention to the CNIL's 2017 inspection program than in previous years when it is published in the spring. The CNIL can still investigate matters outside of the program such as data breaches. Other changes introduced by the bill are still awaiting further clarification via decrees (e.g., right to a 'digital death'), which are expected to be adopted by March 2017. Last but not least, the bill requires the French government to hand over to the Parliament, by June 30, a report identifying how the French current privacy legislation shall be modified in light of the GDPR.

Germany
Ernst-Oliver Wilhelm, CIPP/E, CIPM, CIPT, GFT Technologies SE

The EU Data Protection Reform Package consisting of the General Data Protection Regulation and the Law Enforcement Data Protection Directive is planned to be implemented in Germany essentially by the so called DSAnpUG-EU law (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU or Data Protection Alignment and Implementation Law EU). However, this law will not only replace the existing national data protection law (Bundesdatenschutzgesetz or Federal Data Protection Law) but will also enhance a series of other laws mainly in area of law enforcement and intelligence services. Furthermore, the DSAnpUG-EU suggests a procedure for national data protection authorities how to challenge adequacy decisions of the EU Commission. The DSAnpUG-EU is planned to enter into effect on May 25, 2018. The first draft of DSAnpUG-EU law was leaked last September and has been harshly criticized. In November 2016, the second draft was officially released to relevant interests groups for feedback. Persisting criticism with regard to provisions of draft law itself as well as with regard to its interfaces with other legislation (compliance with GDPR in particular) are fueling doubts whether the law can pass in the current legislative period (ending in late 2017) or whether the legislative procedure can be executed without comprising the quality and robustness of the law.

Another area of change will be the revision of the ePrivacy Directive. The corresponding proposal of the EU Commission's, leaked in December, now suggests a regulation rather than a directive. Although the corresponding provisions will be directly applicable in all the European Union member states including Germany, there is still a lot of work to be done by the German legislator to ensure alignment with the ePrivacy Regulation, which will affect at least the following existing laws which are considered to contain somehow transpositions of the e-Privacy directive: Telekommunikationsgesetz (Telecommunication law), the Telemediengesetz (Telemedia law) and the Gesetz gegen den unlauteren Wettbewerb (Law against unfair competition). So far only a leaked version of the ePrivacy Regulation is available and neither an official statement nor a draft law for alignment of the above mentioned legislation with the ePrivacy Regulation has been issued (or leaked). However, one might expect that corresponding legislative activities will accelerate soon and unfold along a timeline similar to the one for the implementation of the EU Data Protection Reform package.

Israel
Dan Or-Hof, CIPP/E, CIPP/US, Or-Hof Tech & IP Law

No doubt that 2017 will be a very interesting year for privacy protection under Israeli law. New privacy-related information security regulations are about to take effect and introduce modern concepts, such as mandatory impact assessments, encryption and breach notification. ILITA, the local regulator, released three new draft guidelines on the right of access, workplace surveillance and direct marketing. The Biometric IDs Act will take effect, after a long struggle over the formation of a national biometric database. The new Credit Data Act creates a reform in personal credit data processing with major privacy implications. The Israeli parliament holds hearings on regulation of unmanned aerial vehicles (UAVs /drones), with specific attention to privacy aspects, and Israeli companies are commencing GDPR readiness assessment programs.

India
Stephen Mathias, Kochhar and Co

Three key developments are likely to see a greater focus on protection of data privacy in India in 2017: (1) The continued rollout of government services using Aadhar — India's biometric based identification system. (2) Demonetization of currency and a focus on replacing cash payments with digital payments such as through use of digital wallets. (3) An increasing awareness of the dangers posed by hacking and other online threats. At the same time, several government proposals are viewed with uneasiness by businesses. These include the proposal that M2M (machine to machine) providers be registered with the government and keep all data within the country; a possible reworking of the draft encryption policy that appeared to lack basic understanding of how encryption works and increasing aggressiveness in pushing businesses to report security breaches and threats to the government agencies. More balanced regulation that achieves the ideals of regulation while addressing industry concerns on over-regulation and lack of competence by government agencies in high technology areas would seem to be the way forward.

Italy
Rocco Panetta, NCTM

As far as Italy and EU is concerned, 2017 will be a crucial year for a number of reasons. First of all, this would be the year in which we understand if the Italian Parliament and government intend to add more rules to the GDPR or not. As known, GDPR grants member states the faculty to add some prescriptions like in the field of criminal sanctions. Italy at the moment has not declared its will in this respect. In addition, we will get clarity on the national implementation of the NIS Directive, the directive ruling the cybersecurity matters. It will also important to see how the Garante intends to treat tons of its resolutions and general guidance issued in the years: Most of them will disappear at the time the GDPR will fully enter into force, unless the DPA will rule differently.

Japan
Satoshi Funayama, CIPP/US, Microsoft Corporation

On Dec. 20, the cabinet set the effective date of the revised Act on the Protection of Personal Information for May 30. People have already assumed it would be sometime in Spring in 2017. Currently the government is in hurry to set the multiple administrative guidelines for the interpretation/implementation of the law.

Already fixed and published guidelines:

- Guidelines regarding the Act on the Protection of Personal Information (general)
- Guidelines regarding the Act on the Protection of Personal Information (transferring PII to the third party overseas)
- Guidelines regarding the Act on the Protection of Personal Information (confirmation and record keeping obligation when transferring PII to the third party)
- Guidelines regarding the Act on the Protection of Personal Information (anonymized information)

Yet to be fixed:

- Guidelines for PII data leak incident response (public comment period by Jan. 6)
- Guidelines for Personal Information Protection in financial sector (public comment period by Jan. 13 with three other financial sector related guidelines)

Mexico
Rosa M. Franco Velazquez, IAPP

It appears that finally, this year, Mexico will have a General Law for the Protection of Personal Data held by Obliged Subjects (in Spanish: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados), a law that, similar to our current Federal Law on the Protection of Personal Data Held by Private Parties, establishes principles, obligations and procedures for the processing of personal data to be respected and followed by any authority, entity, body and agency of the executive, legislative and judicial powers, autonomous entities, political parties, trusts and public funds, of the federation, federal entities and municipalities.

The draft of November 30, 2016, the same which the deputies of the Transparency and Anti-Corruption Commission approved, among other things, intends to guarantee the observance of the general principles for the protection of personal data; guarantee that any person may exercise its rights for the protection of personal data; promote a culture of personal data protection; and establish mechanisms to guarantee compliance with the provisions of the law.

The Netherlands
Lokke Moerel, Morrison Foerster

In the coming year we will probably see the adoption of the Dutch act implementing the GDPR into Dutch national law. The draft bill was published on December 9, 2016, and will be available for public consultation until January 20, 2017 (available here, in Dutch only). The draft bill is one of the first national implementation acts we have seen to date (together with a draft act for Germany) and as such it may set the tone for other national implementation acts to follow. Where German government has opted to implement national deviations where possible, the Dutch draft bill takes a more restrictive approach favoring EU-wide harmonization.

New Zealand
Jacqueline Peace, Air New Zealand

When it comes to Privacy legislation reform in New Zealand, gazing into a crystal ball has become a pastime for privacy professionals. Will there or will there not be an exposure draft of the often talked about but yet to be seen Privacy Law bill? The government advises us that Privacy Law reform continues to be a priority. Frankly, we're all a little skeptical but hopeful for the crystal ball or the government to prove us wrong and to bring our 1993 Privacy Act into this century. As recently as November 2016, in a recent speech to the iappANZ Summit, New Zealand Privacy Commissioner John Edwards reminded us of what we can likely expect when the reform comes — compliance and enforcement notices, increased penalty powers, mandatory breach notification and access determinations. He stated that "because of the delay in our law reform there is a risk that NZ will fall behind in our response to the emerging challenges." With this in mind Edwards is recommending the proposed reform also considers addressing data portability and re-identification. I'm hoping the crystal ball will support our commissioner's predictions. Fingers crossed…

Poland
Dariusz Czuchaj, Dentons Europe

The main challenge facing the Polish government is to align local laws with the GDPR. Wide-scale changes will affect the Polish data protection watchdog, the Office of the Inspector General for Personal Data Protection, which is to be replaced by a new institution. Moreover, many important sector laws need to be amended to work alongside the GDPR, which makes this task a complex one. That said, no immediate results are expected as there is much legislative work to do.

We expect that the government will also need to take another look at the retention of telecommunication data following the ECJ judgment issued in Tele2 Sverige AB (C-203/15) on December 21, 2016. Currently Polish telecommunication law requires telecom operators to keep metadata for 12 months.

Since Parliament passed many regulations in 2016 giving law enforcement authorities almost uncontrolled access to personal data stored by telecom operators, banks and public registries, the perspectives for the year 2017 for the privacy enthusiast look pretty grim.

Russia
Maria Elterman, CIPP/US, Axiom

Russian State Duma (the lower chamber of the Russian Parliament) is going to discuss the adoption of a draft amendment introducing amendments to the Russian Code on Administrative Offenses in the second reading on January 11. The draft amendment would increase the amount of the fines imposed for violating the Russian Data Localization Law and introduce a differentiation of the offenses types. According to the current Law, legal entities that are not complying with the law may be fined up to RUB 10,000 (currently approximately USD 165). The draft amendment explanatory note states the drafters' opinion that the current liability clause does not efficiently protect personal data, and that the increased fine amounts are intended to ensure the protection of data subjects' rights. The proposed version of the draft amendment would increase the amount of fines up to RUB 300,000 (approx. USD 4945) for legal entities.

Singapore
Rizwi Wun, CIPM, RHT Law TaylorWessing

Singapore can look forward to the eagerly anticipated Cyber Security Act in 2017. The Singapore government has already outlined certain provisions that should be anticipated.

- Operators of Critical Information Infrastructure would most likely be regulated;
- CIIOs would most likely be required, amongst other things, to comply with policy and standards and conduct audits and risk assessments; and
- There would also likely be mandatory reporting of cybersecurity Incidents.

One area of interest amongst service providers would be to be to determine who would be deemed as a CIIO under the new law.

We are also beginning to see a shift in outlook, from the inevitability of suffering a cyber attack, to a focus on managing the aftermath and liability consequences of a cyber attack. We also foresee that remedial solutions, such as cybersecurity insurance, would possibly play a bigger part.

The benefit from all of this increased awareness is that organizations can look forward to more focus, attention and resources committed by the authorities to combat this threat, more opportunities for training and education, a professional body of technicians, and greater coordination and cooperation amongst nations.

South Africa
Russell Nel, CIPP/US, CIPT, Privacyconsulting

With the Information Regulator appointed as of December 1, 2016, South Africa can finally expect some traction in the area of privacy in 2017. However, an exact compliance date has not yet been set.

Advocate Pansy Tlakula, who chairs the body, will have her work cut out for her in setting up the regulator's office – defining necessary processes and artifacts. Alliances with existing regulators will probably be formed to assist with implementation and enforcement.

For the Protection of Personal Information Act (POPI) to become effective, the regulator will also need to publish regulations in order to provide more guidance on certain parts of this law.

If after all that they have some spare time, they may review some of the industry codes of conduct which will be put forth by various industry bodies – almost certainly starting with the financial services sector and direct marketing.

For organizations that haven't yet started on their privacy journey, there is a strong likelihood that the regulator will govern by exception, with a focus on those bodies responsible for data breaches or reportable privacy incidents.

Turkey
Begüm Yavuzdoğan Okumuş, Gün + Partners

On October 20, 2016, the Ministry of Health published the "Regulation on the Processing of Personal Health Data and Maintenance of Privacy." The regulation introduced detailed provisions regarding the processing and transfer of personal health data, particularly in relation to the format of consent and the requirement for anonymization before transfer. While the regulation primarily contains measures that must be taken by health care service providers and other associated persons, there has been uncertainty regarding the scope of application of the regulation.

The current wording of the provision detailing the scope of application is phrased in a way that includes all data subjects whose health data is processed and any data controller that may be processing personal health data pursuant to a legislative requirement. Further it creates ambiguities with regard to transfer of health data abroad.

The impact of the regulation once again shows the necessity for the establishment of the Turkish Data Protection Authority, which was supposed to be formed by October 7, 2016. As the DPA has not yet been formed, there is a lack of both ancillary regulations and a body that can be petition for guidance regarding data protection issues. We expect that these ambiguities will be clarified in 2017 with more guidance on application of the Turkish Data Protection Law as well as the regulation.

UK
John Bowman, CIPP/E, Promontory

Brexit will continue to dominate the headlines in the UK throughout 2017 with negotiations to exit the EU expected to commence in April. The government has announced that the GDPR will become directly applicable in UK law on 25 May 2018 and plans to consult stakeholders on key GDPR measures where national flexibility can be applied. The government has also made clear its intention to preserve the free flow of data with the EU post-Brexit. How the government plans to achieve its objectives remains to be seen, but secondary legislation may be the preferred vehicle for national flexibility while the issue of adequacy could form part of the Brexit negotiations. Questions remain ahead of Brexit though. Will UK-based organizations need to designate a new main establishment in the EU for the one-stop shop? Will the new Investigatory Powers Act present an obstacle to achieving adequacy post-Brexit? Many stakeholders will be hoping for some clarity on these points and more during 2017.

US
Jared Bomberg, Hogan Lovells

In the United States, privacy legislation in 2017 will again touch on a variety of policy issues. At the federal level, we should expect to see a renewed push for updates to the Electronic Communications Privacy Act, which would require a higher bar for the government to obtain emails that are more than 180 days old. ECPA reform nearly became law last year, as it passed the House unanimously but failed to make it through the Senate. The Congress also will take up data breach notification legislation to create a unifying framework for notifications to consumers in the wake of a data breach. The states, too, will work on data breach notification laws, with some states potentially following California's lead to require reporting when certain encryption keys are stolen. Other matters at the federal and state level include student data privacy, drones, and other technology specific legislation such as connected cars and rules related to internet service providers.

US — California
Hank Dempsey, Assembly Privacy and Consumer Protection Committee

For California, key themes in privacy this year will be resistance to federal information sharing, scrutiny of law enforcement technology and cybersecurity. Expect opposition to the new administration to take up a lot of oxygen, so watch for legislation that restricts information sharing by state agencies and local law enforcement with the feds to foil immigration enforcement and the building of discriminatory registries. This resistance may also spill over to greater scrutiny of new law enforcement surveillance technologies, like automated license plate readers, facial recognition and social media monitoring software. Finally, cybersecurity is becoming an important legislative area related to privacy, in part because of high-profile email hacks. Look for efforts to harden the cyber posture of public agencies, discussions over the security of Internet of Things devices, attempts to deal with ransomware, and perhaps even a renewed focus on workforce and economic development for the state's cybersecurity industry.

US — Human Resources
Philip Gordon, Littler Mendelson

Laws restricting employers' ability to ask about, and to use, applicants' and employees' criminal history will continue to be enacted in 2017. In the past five years, more than 25 U.S. jurisdictions, including states (e.g., Illinois, Massachusetts, and New Jersey), counties (e.g., Montgomery County and Prince George's County (Maryland)), and cities (e.g., Baltimore, New York, Philadelphia, San Francisco, and Seattle) have enacted such "ban-the-box" laws. Most recently, Los Angeles enacted a ban-the-box law that goes into effect in January 2017. With pre-employment screening being a critical component of any insider threat reduction program, these laws pose significant challenges for organizations. The laws not only delay the point in time when an employer can inquire about criminal history, but also bar employers from considering certain categories of criminal history and require an individualized assessment of the criminal history before it can be used to justify an adverse employment action.

US — Federal Communications Commission
Yaron Dori, Covington & Burling LLP

In the U.S., expect the Federal Communications Commission to revisit the privacy regulations it imposed on broadband providers in November 2016. Those regulations were promulgated in the wake of the FCC's "Open Internet" ruling, which reclassified broadband providers as "telecommunications carriers" in order to subject them to Net Neutrality obligations, such as prohibitions against "fast lanes" for favored internet content. When this happened, broadband providers no longer were subject to the jurisdiction of the Federal Trade Commission (because the FTC Act excludes common carriers from the FTC's jurisdiction), so the FCC felt the need to step in and impose its own privacy regulations on them. The FCC could scale back these regulations, eliminate them entirely, or potentially take some other approach that draws an appropriate balance between the needs of broadband providers and consumers.

US — Health Care
Kirk Nahra, CIPP/US, Wiley Rein

For better or worse, the only meaningful health care legislation we are likely to see in 2017 (at least the first half) will relate to the repeal and replacement of Obamacare. That package (still being developed) will occupy virtually all of the healthcare thinking for the near future. There's no indication at this point that privacy will be a relevant component of that legislation in any direction. The 21st Century Cures package had a few privacy provisions for the healthcare industry, so that seems to have taken care of the only "pending" issues on the Hill in this area. The biggest "need" at this point is legislation to deal with the growth in "non-HIPAA health data" (think wearables and mobile apps) but there's even less chance of this legislation under this Congress and the new administration.

Zimbabwe
Kuda Hove, Center of Technology Law and Development

In his speech on October 6, 2016, to mark the opening of the fourth session of the eighth Parliament of Zimbabwe, President Robert Mugabe expressed his hope that the current session of Parliament will debate the Data Protection Bill, the Electronic Transactions and Electronic Commerce Bill, as well as the Computer Crime and Cyber Security Bill.

The three bills currently exist as ministerial drafts that indicate how government proposes to regulate among other things, data protection, electronic commerce, and computer crime and cyber security. These bills have been in development since 2013, and 2017 might be the year the respective bills are finalized and debated.

These bills will have an impact on privacy in Zimbabwe. The current draft Computer Crime and Cyber Security Bill has been criticized for giving unchecked surveillance powers to government agencies, for example, by permitting government agencies to remotely install keystroke logging software on individuals' computers. The draft Data Protection Bill on the other hand has been criticized for not adequately complying with regional and international data protection principles.