Vol. 3, Issue 1 | 2021

NEWSLETTER

GLOBAL PRIVACY ASSEMBLY

GPA
Global Privacy Assembly

Message from the Chair

After a year that brought so much uncertainty, it feels difficult to look ahead to what 2021 will bring with any confidence.

The new year arrives with so many challenges still to resolve, from the impact of COVID-19 itself to the privacy implications of vaccination programmes and immunity passports. But we can have confidence that 2021 will bring the same positive engagement and leadership from our community.

Our COVID-19 Working Group will continue to be active, providing support for Assembly members, and an opportunity to collaborate around the shared challenges we face.

Our other working groups continue to focus on priority issues including facial recognition technology, AI and regulatory cooperation. Central to our work will be the ongoing emphasis on engaging with communities and organisations outside of our membership, and I am pleased that we are already making progress towards launching our GPA Reference Panel. I will be marking Data Protection Day by speaking at an event with the World Bank, and discussing the benefits of international organisations working alongside our network.

And the GPA will continue to modernise. Details are included in this newsletter of our GPA Census, which is a crucial piece of work. We want our community to reflect our members' needs, and so it is important that all members take the time to contribute to the

Census and also fill in the Data Governance in the Public Sector Survey.

At our virtual conference last October, I spoke about 2020 being a Year Zero for data protection and privacy. The accelerated adoption of digital innovation brings an enormous appetite for personal data, amid changing societal views on what data collection and sharing is appropriate. The response of data protection and privacy authorities will make 2021 a pivotal year for our community.

We can be confident the GPA will be there to support members throughout the year, and at our 43rd Annual Conference.

With hopes for a healthy and safe 2021,

Elizabeth Denham CBE
Information Commissioner, UK

Inside this issue:

Horizon scanning

2021 – A Crossroad for Data Protection and Privacy?

Wojciech Wiewiórowski, the European Data Protection Supervisor, writes exclusively for the GPA on the landscape for 2021 and beyond

The outbreak of the COVID-19 pandemic has drastically changed the priorities of various actors around the world, being public or private, including data protection and privacy authorities. In this regard, the health crisis has highlighted and majorly elevated the importance of the digital economy, together with the need to implement effective guarantees with regard to data protection and privacy. Digital devices and communication networks have been increasingly deployed on a large-scale basis as tools to manage the crisis we found ourselves in at the time of the COVID-19 outbreak. Such tools are expected to stay with us longer than we plan them to be, and digitalisation will be at the core of our work in the coming years.

Data protection and privacy will need to be part of the road to recovery

Another consequence of this increased digitalisation, accelerated by the COVID-19 crisis, is the augmentation of the collection of personal data about patients and consumers, but also in the education, employment and social life sectors. The COVID-19 crisis has and will continue to affect individuals, particularly the most vulnerable. The impact of the crisis has turned up the pressure on organisations to increase and maximise their efficiency, while consequently affecting the rights and freedoms of individuals. In this regard, we have seen a sharp rise in the merging and reuse of data from different sources, thus affecting the rights of individuals to make an informed decision to this effect. To this end, when the outburst of the COVID-19 pandemic occurred, data protection and privacy authorities were called to engage and cooperate with each other to reach a fair balance between the need to ensure public health while also protecting the rights to personal data and privacy.

We have realised that processing huge amounts of information in the big data world is not a future challenge for the world of the Internet of Things. It suddenly turned out that we already have to 'digitise' as many of our activities as possible, irrespective of whether we want to do so, or not. We have become more and more dependent on the Internet connection at work, at school and at home.

During the past year, a great number of scientific efforts have been put in place globally against COVID-19 in order to produce research results as fast as possible, revealing how a digital health connection has become even more essential. In this regard, it has become fundamental, more than ever, to improve accessibility, effectiveness and sustainability of the electronic health systems used worldwide, as well as the need for individuals to take informed decisions, while granting the exercise of fundamental rights such as the right to privacy and data protection.

Moreover, artificial intelligence (AI) in the healthcare domain has the potential of offering a number of advantages and can be deployed for a wide range of purposes. One of the most recent innovations in the field is a new diagnosis application (developed by MIT) that is able to detect asymptomatic COVID-19 infections by differentiating cough sounds of healthy and infected people with an accuracy rate of 70%. There is no doubt that we can greatly benefit from AI. However, it is not a silver bullet, and inherent risks need to be considered before its deployment, this being particularly valid when AI is meant to be deployed on a large-scale basis and when being used in the health sector. It is therefore essential to ensure that more transparent solutions are built in order to avoid losing individuals' trust, or abusing it. However, it is also crucial that, prior to any deployment of AI on a large-scale basis, a rigorous and holistic impact assessment takes place.

The year that has just started will not only be a crossroad for

data protection and privacy. We will necessarily need to achieve more than balancing the necessity for public health and the right to data protection and privacy. This year will require the data protection and privacy community to actively contribute to the debate on the use of personal data for the public good, thus requiring rigorous yet creative thinking. This, we believe, will also increase the resilience of our societies in order to already be prepared for forthcoming health crises, including pandemics, by proactively developing solutions rather than having to react to ongoing threats. If well prepared, we will be able to have balanced tools, which will, at the same time, protect and limit the impact on fundamental rights.

This year will require the data protection and privacy community to actively contribute to the debate on the use of personal data for the public good

Improving policy-making decisions will be an essential requirement to take informed decisions while minimising the risks of using crises to advance personal interests. In this context, data will need to aid the public good, in particular with regard to AI and scientific research.

The crisis has also a huge impact on legal and political decisions concerning the application of modern IT and telecommunication solutions by public administrations, both at national and cross-border level. However, the changes observed are not limited to legal questions asked or proposed paths on how to respond to the crisis. They rather scale proposed undertakings and accelerate the speed of transformation. Traditionally, the large-scale information systems sector made public administrations carry out long-term pilot projects and a multi-directional evaluation before each successive expansion, whereas the 2020 pandemic has made governments question whether a huge, interoperable project can be launched within a timeframe of weeks. Public administrations have always been willing to announce the "triumph" of IT projects if at least 10% of citizens have used them once, whereas in the fight against COVID-19, 60% of the population will be using the technical solutions permanently.

Active dialogue with stakeholders, including healthcare professionals, will be necessary. Limiting our involvement as data protection and privacy authorities may be comfortable, yet a shift will also be required to strike the right balance between the response to a crisis and guaranteeing the fundamental rights to data protection and privacy. In this regard, strong oversight and audit capabilities will become even more important, particularly in the context of AI and automated decision-making which affects individuals, including the most vulnerable.

The pandemic has taught us how data protection and privacy can enhance and not be an obstacle to the adoption of specific measures meant to address health crises. In our role as data protection and privacy authorities, 2021 will be a key year, in which we will need to stake our claim as advocates for the rights to data protection and privacy, while also actively focusing on the avoidance of the misuse of personal data and digital technologies. This is particularly important when involving sensitive data such as health data.

The success of any new tool developed to face any upcoming pandemic will need to assure a lawful, responsible and ethical approach, including the respect for fundamental rights. Any tool developed will need to serve as an example of transparency, accountability and balance between the interests of individuals and the interest of society as a whole. We, as data protection and privacy authorities worldwide, will not only need to continuously stand ready to offer practical advice on issues such as technologies that may assist in saving lives, but we will also need to actively engage with competent authorities and, in the case of data processing in the health sector, with public health authorities. We will need to ensure that the 'new normal' does not erode the rights we promote. On the contrary, data protection and privacy will need to be part of the road to recovery.

GPA Member Census

Members have until 12 February 2021 to complete the GPA Census

globalprivacyassembly.org/gpacensus

Focus

What next for Convention 108? – A unique forum at global level

Alessandra Pierucci, Chair of the Committee of Convention 108, highlights both the current and future potential of this 40-year-old instrument

28 January 2021, an important anniversary for Convention 108

The Council of Europe, a 70-year-old international human rights organisation based in France, has been, for its 47 member states and other countries across the globe, a precursor and instrumental actor for the promotion and defense of the right to data protection at regional and international levels.

On 28 January 1981, 40 years ago, the Council of Europe opened for signature its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (more commonly known as 'Convention 108'). This Convention remains to date the only legally binding multilateral instrument on the protection of privacy and personal data open to any country in the world.

> **Convention 108+ is the only international instrument with a sound potential to become the global treaty on the protection of privacy and personal data**

Since this landmark date, which is now celebrated globally as Data Protection or Data Privacy Day depending on where you are on the globe, the Convention has influenced various international and national privacy laws. Convention 108 currently includes 55 State Parties and its Committee also welcomes the participation of more than 25 observers, forming a global forum of over 70 countries working together on data protection.

Convention 108 has been modernised in order to adapt this now 40-year old instrument to the new realities of an increasingly connected world, and to strengthen the effective implementation of the Convention. The Protocol amending Convention 108 was opened for signature on 10 October 2018, in Strasbourg and has since been signed and ratified by numerous countries.

Once it enters into force, the amending Protocol will deliver several essential objectives, notably: respecting human dignity and integrity in the digital age, facilitating data flows and strengthening cooperation between supervisory authorities.

Convention 108+ (Convention 108 as amended by the protocol) is seen to become the international standard on privacy and data protection in the digital age and presents numerous advantages for countries ratifying or acceding to it.

Looking ahead: what Convention 108+ will bring us for the next 40 years

The global treaty on data protection

Convention 108+ is the only international instrument with a sound potential to become the global treaty on the protection of privacy and personal data. To date, it is still the only open, legally binding, multilateral international treaty covering those fundamental rights.

Convention 108 already counts amongst its 55 State Parties eight that are not from the European continent.

Recognising its unique potential to become the global instrument on data protection, the United Nations' Special Rapporteur on the right to privacy, Professor Joseph A. Cannataci, has recommended "to all UN Member States to accede to Convention 108+" in two of his reports already: 2018 Annual Report on the Right to Privacy to the Assembly General (Report A/73/45712); and Annual Report of 1 March 2019 to the UN Human Rights Council (Report A/HRC/40/63).

The Convention has always had and will continue to have an influence outside of its State Parties, as many countries can contribute to the normative work and discussions as observers in its Committee.

Convention 108+ is unique: a balanced and protective legally binding instrument available for any country to commit to it (there is no equivalent and no existing alternative); it creates a common, global legal space for privacy and data protection.

An appropriate protection for individuals in the digital age

With its balanced standards, Convention 108+ sets a commonly

agreed level of protection that an individual should be guaranteed in the digital age in order to safeguard her/his dignity and fully enjoy her/his right to informational self-determination.
In recent judicial cases where courts have been invalidating international transfer agreements or mechanisms because of the insufficiency of the protection afforded to individuals, Convention 108+, notably fully consistent with the data protection framework of the EU (General Data Protection Regulation and Law Enforcement Directive) can effectively contribute to the convergence towards a set of high data protection standards globally.

Accession to Convention 108+ implies the recognition of an international best practice and opens opportunities for further, enhanced cooperation, including joint investigations and joint regulatory actions

Considering the global repercussions of the latest decision of the European Court of Justice on international transfers (Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Case C-311/18), the relevance of Convention 108+ can only grow stronger in light of the sound protective international regime that it provides, acting as a 'bridge' between legal regimes and continents, to facilitate data flows to safe destinations.

Convention 108+ represents a viable tool to facilitate international data transfers while guaranteeing an appropriate level of protection for individuals globally.

A booster for international cooperation

States Parties to Convention 108+ commit to mutual co-operation in order to ensure the highest level of data protection as well as compliance with international standards.

Belonging to the 'Convention 108+ club' also means being able to rely on a strong network of peers capable of providing assistance, advice and support. In an era of increasing digitalisation and globally shared challenges, the Convention allows the competent data protection authorities to work hand in hand. Accession to Convention 108+ implies the recognition of an international best practice and opens opportunities for further, enhanced cooperation, including through joint investigations and joint regulatory actions, for which the Convention also provides the legal basis at international level, which is another unique feature of the Convention.

In the 40 years of its existence, Convention 108 has achieved impressive results. As Chair of the Committee of the Convention, I look forward to the realisation of Convention 108+ and witnessing for the 40 years to come the relevance and value of the modernised convention for the benefits of our democratic societies.

The GPA Secretariat — Your central contact point

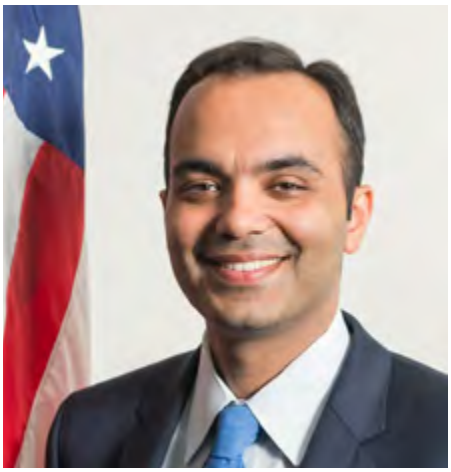
If you are interested in getting more involved in the GPA's work, by joining one of the Working Groups, or volunteering to be a future Assembly host, please get in touch with the Secretariat at secretariat@globalprivacyassembly.org

For more information on the GPA, visit our website at globalprivacyassembly.org

Follow us on Twitter
@PrivacyAssembly

Focus

Data Abuse – Changing Course as an International Community



In an exclusive interview with the GPA, Rohit Chopra, Commissioner at the US Federal Trade Commission (FTC), discusses the responsibility of regulators, and the GPA community, to prevent as well as effectively punish and remedy data abuses

Tell us about the FTC in the US, and its current role in driving forward and protecting 'a vibrant economy', 'vigorous competition' and 'consumer access to accurate information'.

During the dedication of the FTC headquarters in 1937, President Franklin Delano Roosevelt laid out a vision of how the agency should use its authority. In his speech, he said "prevention of unfair business practices is generally better than punishment administered after the fact of infringement costly to the consuming public and to honest competitors."

The FTC was created to make sure that people – and honest businesses – got a fair deal. Our dual charges to look at competition and fair treatment, as well as our special research mission, allow the Agency to look at business practices comprehensively.

In the privacy and data protection community, there is growing scrutiny of the business models of global tech giants. The FTC's mandate requires us to look at how their practices also create risks for consumer protection and competition. Our job is not to simply chase down problematic practices, but to prevent them in the first instance.

What have been some of the most notable challenges for the FTC to date?

Our current biggest challenge is to ensure the effectiveness of remedies for violators when it comes to digital rights. There is a growing global consensus that big fines are not big penalties for the biggest companies in our lives. Forfeitures of ill-gotten gains and redress for victims is critical, but this cannot simply be the cost of doing business. I am concerned that traditional approaches to remedies are not working, so we must change course as an international community.

COVID-19 has shifted more of our interactions through digital channels, amplifying the need for effective regulation and law enforcement in emerging areas, such as video conferencing. The GPA has taken important steps to bring together regulators on these emerging problems. We need a global, all-hands-on-deck approach to tackle these data abuses.

What is a recent achievement of the FTC and any significant lessons that can be shared with the GPA community?

The FTC's enforcement action against Everalbum and Paravision is particularly noteworthy. Everalbum marketed a photo-sharing app called Ever. The companies improperly used individual photos to develop facial recognition technologies. The FTC ordered the companies to delete and destroy not only ill-gotten data, but also any work product made with the data, to include algorithms and models. The deletion of facial recognition algorithms is an important milestone to vindicate data protection rights. This is an important course correction to how we pursue remedies, and I would encourage all regulators to consider all of the ways to ensure that firms in violation of data protection standards forfeit the fruits of their wrongdoing.

Give your views on the important opportunities that lie ahead for the FTC, both in the US with the new administration, and as a key player in the GPA.

In the United States, there is a bipartisan consensus that the largest technology companies have extraordinary power over our lives and our economy. They have developed business models that monetize our personal data in ways that can undermine our privacy, safety, democracy, and national security. The public is demanding action and accountability for these giants, and the FTC and other regulators must clearly demonstrate that no firm, regardless of size or clout, is above the law.

The GPA has provided an important forum for us to tackle these pressing global problems together for the benefit of people around the world.

Case study

C108 – Privacy and Personal Data Protection in Practice

President Awa Ndiaye, Senegal Commission of Personal Data Protection, provides our case study of the ratification and impact of Convention 108, and the updated protocol Convention 108+ both in Senegal and the Africa region

Introduction to the Commission for the Protection of Personal Data (CDP), Senegal

The Commission for the Protection of Personal Data (CDP) is an independent administrative authority, created by the Law 2008-12 of 25 January 2008, dealing with the protection of personal data.

The creation of the CDP is part of a broad movement towards a legal framework for the information society in Senegal. Indeed, in 2008, the State of Senegal adopted specific laws on electronic transactions, cybercrime and the protection of personal data.

The principles of the processing of personal data must be common standards, approved by all countries, only then will international cooperation on data protection and privacy be strengthened in a secure and trustworthy digital world

The CDP comprises a deliberative body, the Plenary Session, composed of 11 Commissioners from the institutions of the Republic, the socio-professional, academic and civil society.

Furthermore, in carrying out the tasks under Article 16 of the aforementioned Law No. 2008-12, the President of the Protection Commission carries out her duties with the assistance of the body's administrative and technical departments.

The CDP monitors the compliance of personal data processing in accordance with the legal and regulatory provisions enacted in Senegal. As such, it authorises the processing of personal data, conducts on-site monitoring or assessment of available evidence, and handles complaints regarding the violation of the rights of individuals concerned. It also provides an awareness and advice service for the public and to all those involved in the processing of personal data.

Faced with the current challenges posed by the rapid evolution of new technologies (biometrics, artificial intelligence, big data), the CDP has initiated a reform of the 2008-12 law, in order to more efficiently address the current problems that challenge regulators responsible for the protection of personal data.

In addition, the CDP is a member of regional and international organisations, such as the Francophone Association of Personal Data Protection Authorities (AFAPDP), the African Network of Personal Data Protection Authorities (RAPDP) and The Council of Europe Convention 108.

The ratification and impact of Convention 108 in both Senegal and the Africa region

As Convention 108 is the only binding international legal instrument for the protection of personal data, its accession and ratification were an imperative for Senegal in order to strengthen its personal data protection system. Indeed, this reinforced the internal mechanisms for the protection of personal information and bound Senegal to international standards.

Senegal joined the Council of Europe Convention 108 on the protection of people in the automated processing of personal data in 2016.

This accession has enabled Senegal to offer sufficient guarantees of data protection to nationals and companies operating in the Member States of the Convention. This trusted digital environment has facilitated the flow and transfer of data conducive to the development of the digital economy.

In addition, in the Office of the Consultative Committee of Convention 108, Senegal holds the second vice-presidency, and represents 'the voice of Africa'. This enables interoperability between the principles of protection of Convention 108, African regional instruments and national legislation, and facilitates

harmonisation.

In terms of cooperation, the Council of Europe's Convention 108 provides a harmonised framework for action between the States Parties. Consequently, it has become common to see bilateral or multilateral initiatives promoting the management and resolution of problem areas common to the data protection and privacy authorities. For African countries, where these authorities are still relatively young, international cooperation represents a great opportunity for progress, and the Council of Europe sessions are a fruitful framework for the exchange of good practices.

To take full advantage of this enriching cooperation, and to align itself with international data protection standards and achieve an adequate level of protection, Senegal is preparing to ratify the Amending Protocol that modernises Convention 108 (Convention 108+).

In this regard, at the national level and under Convention 108+, the 2008-12 law has undergone a thorough review, with the involvement of all stakeholders in the sector, and an updated bill has been submitted to the Government.

Practical advice and lessons learned on the ratification of Convention 108

The ratification of Convention 108 has helped to promote trade and strengthen regulatory mechanisms, including:

- Strengthening the expertise of African data protection authorities (training, seminars, exchange meetings);
- A partnership framework between the Council of Europe and the Network of African Data Protection Authorities;
- A framework for dialogue between the Council of Europe and Data Protection Authorities on current and future issues relating to personal data, including: profiling, facial recognition, data protection in the education system, digital identity, and data protection in the context of political campaigns;
- Bilateral partnership relations between the Institutions, members of the Council of Europe, and those responsible for data protection.

The ratification of Convention 108 has helped to promote trade and strengthen regulatory mechanisms

2021 and the future potential of this legal instrument

For the year 2021, we face significant challenges, relating to the adoption of the new Senegalese law on the protection of personal data, but also to the construction of a robust and modern African environment for the protection of personal data. To this end, the harmonization of African legislation and the support of the African Union (AU) and Smart Africa Alliance initiatives are key for promoting an inclusive economy and building a growth-enhancing African digital society.

In addition, to enable the AU to further promote the protection of personal data on the African continent, the Union Institutions should appoint, like the United Nations (UN), a Special Rapporteur for the protection of personal data and privacy in Africa.

The role of the Special Rapporteur would be to:

- Review data protection and privacy in Africa;
- Examine, on behalf of the AU, the programmes, policies and laws of African countries that concern the field of personal data protection and privacy, and to promote harmonisation;
- Aid Governments to ensure that identification programmes, including biometrics, and mass data collection programmes on the African continent comply with African and international conventions on privacy protection;
- Work closely with the African Network of Personal Data Protection Authorities (RAPDP) to encourage and support states seeking to develop their own privacy legislation.

Furthermore, we believe it is crucial that all African Data Protection Authorities encourage the advocacy of Heads of State and Government, and of African International Organisations, to ensure that the principles of data protection are properly incorporated into the Resolutions taken within the African institutional community.

Moreover, the forthcoming ratification of Convention 108+, by Senegal, and by countries from various geographical regions, remains a high priority, which will ultimately strengthen the fundamental role of bringing national legal frameworks into coherence.

The principles of the processing of personal data must be common standards, approved by all countries. Only then will international cooperation on data protection and privacy be strengthened at the heart of a secure and trustworthy digital world.

Case study

Australia embarks on major review of privacy law

Angelene Falk, Australian Information Commissioner and Privacy Commissioner details the ground-breaking law reform process ongoing in Australia

For data protection authorities, the events that have transformed our world over the past 12 months underscore the fact that new privacy challenges can emerge rapidly, and without forewarning.

While Cervantes wrote that to be forewarned is to be forearmed – and preparation is half the battle – few could have predicted the scale of the COVID-19 pandemic, and the range of privacy issues it has raised.

The response from the global privacy community has been far from quixotic. Instead, data protection and privacy authorities around the world have collaborated and responded with practical strategies to enable the use and protection of personal information as a key tool in the pandemic response.

In Australia, this swift response has been underpinned by our principles-based privacy law. Our regulatory framework is founded on 13 key principles which provide a flexible and technology-neutral approach to protecting personal information. The law applies across every sector of the economy and the national government, with some exceptions for particular acts and practices, national security agencies, and small businesses.

Our Privacy Act was introduced in 1988, and has undergone several significant updates, including the introduction of mandatory data breach reporting in 2018. Privacy law has converged with consumer law in the establishment of our new Consumer Data Right, which is being rolled out across the economy to give consumers greater control over their personal data. We have also established a binding privacy code for Australian Government agencies, with another in the works for online platforms and social media.

While our principles-based framework continues to serve us well, the time has clearly come for our Privacy Act to be updated to ensure it can continue to meet the challenges emerging in the digital age. We also need to reverse declining levels of community trust in how organisations handle personal information.

> **Our ultimate goal is a strong, fair and flexible privacy framework that prevents harm, protects fundamental human rights and builds public trust to support a successful economy**

In 2019, the Office of the Australian Information Commissioner recommended a review of our privacy framework to the ground-breaking Digital Platforms Inquiry, led by Australia's consumer and competition regulator.

The recommendation was accepted by the Australian Government, and it commenced a review late last year to ensure our privacy law is "fit for purpose, can grow trust, empower consumers and support the growing digital economy".

While the pandemic delayed the start of the review, it has also served to reinforce the need for reform.

In the current environment, we are spending even more of our time engaging and sharing information online, as technology, data and security issues continue to evolve rapidly.

Our recent landmark survey of community attitudes to privacy also found that Australians want more done to protect their personal information in light of ongoing and emerging threats.

Our regulatory experience and international engagement points to four key elements needed to support effective privacy regulation over the next decade and achieve our goal of increasing trust and confidence in the handling of personal information:

- Global interoperability – making sure our laws continue to connect around the world, so our data is protected wherever it flows;
- Enabling privacy self-management – so individuals can exercise meaningful choice and control;
- Organisational accountability – ensuring there are sufficient obligations built into the system; and
- A contemporary approach to

regulation – having the right tools to regulate in line with community expectations.

We have proposed a range of changes to the Privacy Act to introduce fairness and reasonableness standards for the collection, use and disclosure of personal information; to place greater emphasis on the protection of individuals, and entities' obligations to ensure business models and practices safeguard privacy; and to both strengthen notice and consent requirements, and address their limitations.

Our recommendations draw from the experience of other jurisdictions, including aspects of the GDPR and recent or proposed reforms in Canada, California, and New Zealand.

Our ultimate goal is a strong, fair and flexible privacy framework that prevents harm, protects fundamental human rights and builds public trust to support a successful economy.

You can read more about Australia's review of its Privacy Act and Commissioner Falk's detailed submission at oaic.gov.au/review-of-the-privacy-act

Report from the UN Special Rapporteur on the Right to Privacy

Professor Joseph A. Cannataci, UNSRP, comments on his forthcoming 2021 report to the UN Human Rights Council

Human rights are of crucial importance in the information society. My forthcoming 2021 report to the UN Human Rights Council addresses the role that human rights, from a privacy perspective, have to play in Artificial Intelligence, and children's autonomy.

Artificial Intelligence

The UN General Assembly and the Human Rights Council have confirmed that the rights people enjoy offline should also be protected online (A/75/62). While easily and well said, achieving this aim is challenging in practice. Technology has advanced so quickly, our practices and regulatory frameworks are still evolving.

While recognising the many economic and social benefits of Artificial Intelligence (AI) solutions, a reference point is needed on how the right to privacy can be protected.

In recognition of this, and in response to the matters raised by CSOs/NGOs, corporations, individuals, and Governments, the Report also provides guiding principles for the use of personal and non-personal information in the context of AI solutions developed as part of applied Information & Communication Technologies.

> **the Report... provides guiding principles for the use of personal and non-personal information in the context of AI solutions developed as part of applied Information & Communication Technologies**

The recommendations emphasise the importance of a legitimate basis for AI data processing by governments and corporations within the overarching framework of the human right to privacy.

The Recommendations are intended to serve as a common international baseline for data protection standards regarding AI solutions, especially those to be implemented at the domestic level. Important components are the inclusion of 'red lines' and the requirement for human rights impact assessments. The position on 'red line' areas is that the use of AI solutions should not be countenanced for final decisions but only as part of decision-support in key areas, for example, judicial or medical decision-making. In a complementary manner, human rights assessments should always be undertaken alongside data protection assessments to establish a holistic understanding

of the framing conditions and potential outcomes.

Implementation requires full collaboration between Governments, civil society, the private sector, the technical and academic communities and regulatory bodies, and needs to be sustained by values of inclusiveness, respect, human-centredness, human rights, international law, transparency and sustainability.

Children's right to privacy

The foundations of future intellectual, emotional and sexual life are developed in childhood and adolescence. The domains instrumental to children's development are usually family life, schools, and social networks.

Article 16 of the Convention on the Rights of the Child (1989) (CRC) addresses children's privacy rights. Their right to privacy enables their access to other rights critical to developing personality and personhood, such as freedom of expression, association, non-discrimination and health. Children's privacy relates to their bodily and mental integrity; decisional autonomy; personal identity; informational privacy; and physical/spatial privacy.

As Tobin has said, children are human *beings* not *becomings*, and are entitled to all the human rights applicable to individuals [Tobin, J. (2015) Understanding Children's Rights: A Vision beyond Vulnerability, Nordic Journal of International Law, 84, pps155-182]. Yet children's enjoyment of human rights is largely determined by adults, particularly those in authority including parents.

A particular feature of childhood and adolescence is the growth of capacity and independence. The CRC (Article 5) requires the child's evolving capacity to be taken into account in decisions concerning children. This poses the question "how do standards reliant upon a child's chronological age recognise 'evolving capacity', particularly when applied to children collectively?".

Essentially, 'age appropriate' standards align poorly with the principle of 'evolving capacity'. The child's readiness for decision-making and self-responsibility is best determined not by chronological age alone but by the context, including the risks and support available; individual experience; the rights affected, and the child's capacity for understanding the implications of his or her actions (or non-actions). Determining when a child is capable, for example, of consenting to the processing of their personal data, must consider their 'actual understanding' of the data processing, their best interests, rights and views. Space does not allow for a greater exploration of these challenges but better and smarter technological design could play a significant and positive role in addressing them.

Lastly, it appears that COVID-19 is going to be present in our lives for much of 2021 and indeed beyond, though hopefully, to a diminishing extent. I wish the GPA and all data protection authorities a safe and productive 2021.

The 2021 report will be available on the SRP webpage in February. Enquiries can be made to Prof. Elizabeth Coombs at **ecoom02@sec.research.um.edu.mt**.

Working Group highlights

International Enforcement Cooperation Working Group

The chairs of the International Enforcement Cooperation Working Group update on progress in fulfilling Pillar 2 of the GPA's Policy Strategy on practical enforcement cooperation, and outline plans for delivery of the Resolution on Facial Recognition Technology, in collaboration with the Ethics and Data Protection in AI Working Group.

International Enforcement Cooperation Working Group Co-chairs:

Brent R. Homan
Deputy Commissioner
Compliance Sector
Office of the Privacy Commissioner of Canada

James Dipple-Johnstone
Deputy Commissioner
Chief Regulatory Officer
UK Information Commissioner's Office

Rohit Chopra
Commissioner
US Federal Trade Commission

Members are no doubt familiar with the maxim that in today's global digital economy data knows no borders. A cliché perhaps, but true nonetheless. We increasingly see data-driven business models impacting privacy far beyond the jurisdiction where a service is based. To address this effectively, cooperation between privacy enforcement authorities is more important than ever.

The GPA recognised this in its 2019-2021 Strategic Plan, adding enforcement cooperation as the second pillar of its Policy Strategy. This mandated the permanent establishment of the International Enforcement Cooperation Working Group (IEWG) and a refresh of its aims to focus on support of enforcement cooperation in practice.

The permanent IEWG has now been operational for over a year. We therefore wanted to update you on the work that we, and our diverse and engaged membership of over 20 Authorities, are doing this year.

Practical enforcement cooperation

This year, we're carrying out several activities to help fulfil our mandate and support practical enforcement cooperation. Key highlights include:

- Updating the Enforcement Cooperation Handbook – Working with the Digital Citizen and Consumer Working Group, we used a survey to obtain valuable feedback on the handbook. We are now analysing responses and will draft an updated version of the handbook for presentation to the 2021 GPA.
- Managing the Enforcement Cooperation Repository – We are identifying potential for improvements to the repository and ways to better promote engagement with the tool by GPA membership.

Enforcement Cooperation Repository

The **repository** is a great enforcement cooperation tool for dissemination, sharing and access to a variety of resources from members such as policy documents, enforcement decisions, research, guidance and press-releases. Members can access these resources to inform and support their own work. The more up-to-date the repository is, the more useful it can be.

We invite all members to contribute new or recent

resources to the repository. Simply email a link to the resource (with a translated title and short summary in English) to the IEWG Secretariat: **International.Enforcement@ico.org.uk**

- Formalising safe space sessions – The first step we took to establish the IEWG as a forum for practical enforcement cooperation was developing and running 'safe space' sessions to facilitate free and frank discussion on concerns, policy positions and experience of regulating specific global entities and issues. We've seen great value and practical output from this work. A good example is a session that led to a joint letter, issued by six IEWG members, setting industry expectations on appropriate privacy measures for video teleconferencing services during the pandemic. We were also pleased to receive excellent feedback on our open safe space webinar on Facial Recognition Technology (FRT) in the margins of the 2020 GPA. We are building on this by developing a framework to formalise, document and improve the way we run these sessions. We will test the framework and report back to the 2021 GPA.
- Engagement strategy – We developed a strategy to encourage regional, cultural and linguistic diversity in IEWG membership. It also informs our work to ensure: we support cooperation initiatives relevant to members' needs, no matter their size or origin; we find innovative ways of overcoming barriers to members' contribution to the group; and, we reach out and cooperate with other networks.

Facial Recognition Technology (FRT)

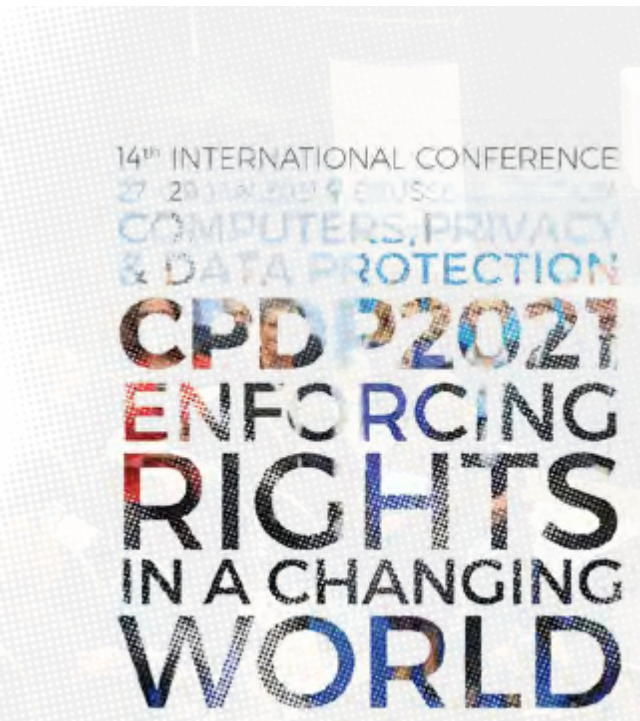
Members will recall that a resolution on FRT was adopted at the 2020 GPA. This tasks the IEWG and the Ethics and Data Protection in AI Working Group (AIWG) to develop a set of principles and expectations for use of personal data in FRT, and to promote the principles to key external stakeholders.

Together with the AIWG we have developed a phased approach to deliver this work. In an initial research phase, we are engaging with GPA members, industry, lawmakers and civil society to review and better understand policy positions, existing principles, and use cases. In a second development phase we will draft and consult on the principles, and develop plans for stakeholder engagement and promotion. And in a final adoption phase, we aim to present the principles to the 2021 GPA, followed by proactive promotion and review of their application by industry in 2021-22.

Join the International Enforcement Cooperation Working Group

Between now and the 2021 GPA we're running two safe space sessions. If you like the sound of them, or any of the work we're doing in the IEWG, we'd strongly welcome your input and participation.

To join, email the IEWG Secretariat on International.Enforcement@ico.org.uk



Brent Homan, Co-chair of the GPA Digital Citizen and Consumer Working Group, will be speaking at **14th International Conference of Computers, Privacy & Data Protection (CPDP)** on 28 January 2021.

The panel **"When Regulatory Worlds Collide – The Intersection of Privacy, Competition and Consumer Protection"** will include Anna Colaps, EDPS (EU); Erika M. Douglas, Temple University (US); Ian Cohen, Lokker (US); Alan Thoma, CT Advogados (BR).

More information at **cpdpconferences.org**

In conversation with...

Chairperson, Ms. Mieko Tanno, Personal Information Protection Commission (PPC), Japan

Ms. Mieko Tanno talks exclusively to the GPA about her role and the data protection priorities of the PPC, Japan, both nationally and on the global arena

As Chairperson at the PPC in Japan, tell us briefly about your background and your views regarding the role of the PPC both nationally and internationally?

I was appointed as the Chairperson of the Personal Information Protection Commission (PPC) Japan in November 2019, after having served as a Commissioner of the PPC Japan since February 2016. Prior to that, I had a career in the field of consumer protection for more than 25 years.

The PPC Japan was established in January 2016, and as a highly independent organisation, it is responsible for the overall administration of personal information protection in Japan. In international settings, as a personal information protection authority, we have promoted international cooperation with other data protection authorities (DPAs) or relevant organisations by, for example, facilitating mutual adequacy recognition on the cross-border transfer of personal data between Japan and the EU, and by participating in international conferences on privacy and data protection, including the GPA.

Our social environment is currently undergoing rapid and major change due to digitalisation and globalisation. The legal purpose of the Act on the Protection of Personal Information (APPI) focuses on both the utility of personal information including the proper and effective application of personal information, and the protection of the rights/interests of individuals.

The PPC Japan, I believe, is required to take action, considering the balance between the protection and use of personal information, and based on that, to respond accordingly to the various changes in scenarios surrounding personal information and personal data.

Please outline the main achievements of the PPC, Japan?

The Amended APPI was promulgated on 12th June 2020, in light of increased awareness among individuals regarding their own personal information, balancing protection and the use of personal information while taking technological innovation into account, and the necessity to tackle the emerging risks due to increased cross-border data flows.

> **The 'Data Free Flow with Trust (DFFT)' initiative promotes the free flow of data whilst addressing privacy issues**

Most provisions of the law will come into force, within two years from the date of promulgation.

Broadly speaking, the amendments were made with regard to the following: adding the perspective of individual rights; obligations that business operators should abide by; frameworks to encourage voluntary activities of business operators; policies for data use; penalties; and, extraterritorial application of the APPI and cross-border transfer of data.

At the G20 Osaka Summit in 2019, Japan proposed the 'Data Free Flow with Trust (DFFT)' initiative to promote the free flow of data whilst addressing issues such as privacy. In terms of the proper handling of personal data, the PPC Japan has discussed promoting the DFFT initiative with countries who share the same values of democracy, the rule of law and respect for fundamental human rights, that provide the foundation for trust. This is a key example of our work towards creating an environment in which personal data can be safely and smoothly transferred across borders.

More specifically, the PPC Japan proposed concrete ideas on establishing a framework for free and trusted international flow of personal data and we have been in discussion with the relevant data protection organisations both in the US and EU to achieve this. The PPC Japan has also proposed for discussion the new risks surrounding personal data protection, such as data localisation and unlimited government access, which should be addressed in the review process of the OECD Privacy Guidelines, and I look forward to the PPC Japan continuing to lead the discussion in these areas.

As mentioned earlier, the environment surrounding personal data is in the midst of dramatic

change. Therefore, it is essential to further develop cooperation with DPAs around the world, and I have no doubt that the GPA, which has been leading the global debate on privacy for over 40 years, will be one of the key players in this. The PPC Japan will continue to contribute to the discussions and activities of the GPA through sharing best practices etc.

Please highlight both the current and future challenges facing the PPC, Japan?

COVID-19 has changed our lives drastically, and 2020 turned out to be a challenging year for all DPAs. Striking the right balance between the protection of an individual's rights/interests and the public interest including public health remains an important issue for us to tackle, and we will continue to focus on the protection of personal information and privacy in that regard in 2021.

In addition, emerging technologies, such as Facial Recognition Technologies and AI, are expected to be used more widely in our daily lives and in the fight against COVID-19, and these technologies will contribute to enriching our day-to-day lives. In that respect, it is essential to ensure protection of personal data and privacy as these innovative technologies continue to be applied in society. The PPC Japan is ready to continue to participate in the discussion with DPAs in these areas, engaging with the various international actors including the GPA.

> **It is crucial for us to adapt ourselves to the changing environment around personal data in the digital and global society**

Finally, in your opinion, please describe the important future opportunities for the PPC, Japan, that will have lasting impact, both nationally and globally?

The PPC Japan is still a relatively new organisation in terms of its history, but it plays a vital role in the area of the protection of personal information in Japan. I believe that it is crucial for us to adapt ourselves to the changing environment around personal data in the digital and global society, to listen to the opinions of businesses, individuals, and a wide range of stakeholders, and to carry out agile and effective law enforcement as needed. In the Asia-Pacific region, we aim to continue to strengthen the relationships with DPAs and to cooperate through the regional forums.

In the international community, with its history of more than 40 years since the establishment of the ICDPPC (now GPA), I take the GPA as an important body that provides a foundation for DPAs around the world to exchange experiences and strengthen cooperative relationships. I hope that the PPC Japan continues to engage in the various activities of the GPA and promote international cooperation in the field of personal information protection.

GPA key upcoming dates 2021

- **14 Jan** Launch of Application process for new members and observers opens
  - 18 July 2021: Membership application deadline
  - 22 August 2021: Observers application deadline
- **22 Jan** Application window for GPA Reference Panel Opens
- **28 Jan** GPA Chair Elizabeth Denham speaks on International Data Protection Day, at the World Bank
- **12 Feb** Deadline for completion of the GPA Census and Data Governance in the Public Sector Survey
- **19 Feb** Application window for GPA Reference Panel closes at 12:00 (UK time)
- **17 Mar** GPA Executive Committee Meeting – Workshop on the GPA Strategic Plan 2021-23
- **26 Jul** Deadline for submitting all GPA 2021 draft resolutions and Working Group reports
- **18-22 Oct** 43rd GPA Mexico 2021

Check our website for more information: globalprivacyassembly.org

Get to Know Your ExCo...

President Commissioner, Ms. Blanca Lilia Ibarra Cadena, National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), Mexico

As the newly elected President Commissioner at the INAI, Mexico, outline for us your previous achievements and aspirations for the INAI both in Mexico and in your region?

Since 2018, I have been honoured to be part of the INAI; however, my recent appointment as President of this Institute, in December 2020, represents one of the greatest achievements in my personal career. I strongly believe in strengthening communication bridges with society by guaranteeing the right to personal data protection. I have dedicated more than 30 years of my professional life to the media, holding various management positions in press, radio and television. Also, I served as Commissioner President of the Commission for Access to Public Information and Protection of Personal Data for the State of Puebla, Mexico.

As part of my current role, my objective is for INAI to be a leading national authority for the protection of personal data in the region, guaranteeing and monitoring due compliance with the promotion of the right to the protection of personal data held by both the public and private sectors. In addition, I will collaborate with stakeholders to implement a legal system for data protection that contemplates the highest international standards in this field, by fostering good practices and building trust among citizens.

Simultaneously, one of the Institute's priorities is to continue fostering communication and networking with other personal data protection authorities and international forums. The aim is to build joint debates and solutions to new problems and challenges that may arise, as well as to work on strengthening and enabling cross-border data flows with due protection of the right to privacy.

As the new President Commissioner representing INAI on the GPA Executive Committee and as hosts of the 43rd GPA in 2021, what are the main priorities for the next twelve months for the INAI with regard to its membership of the GPA?

As Mexico will be hosting the 43rd GPA in 2021, one of its priorities is to establish good coordination and communication with the GPA Secretariat and GPA members, so that the Assembly can be held successfully, incorporating the lessons learned from past meetings. Also, INAI intends to actively participate in all GPA working groups, in order to achieve the objectives established in the Strategic Plan 2019-2021, and in the action plans agreed by each working group.

Furthermore, I would like to emphasise that the international activity in the personal data protection field carried out by the Institute is quite significant, since it also participates in several forums and organisations, such as the Asia-Pacific Economic Cooperation (APEC), the Organisation for Economic Co-operation and Development (OECD), the Consultative Committee of Convention 108 of the Council of Europe and the Ibero-American Data Protection Network (RIPD). Thus, the discussions and resolutions carried out in collaboration with the GPA can be shared, disseminated and have a wider scope.

> **INAI is in the process of implementing the APEC Cross-Border Privacy Rules System and is particularly interested in achieving adequacy as a "third country"**

Finally, as a result of the globalisation process – as well as the new social, economic, cultural and political needs to carry out cross-border data flows to facilitate international trade relations – I believe it is essential for countries to work together to design systematic regulations with the highest standards of personal data protection, of international and/or regional application. Moreover, I believe it is fundamental to issue recommendations that offer solutions to the emerging

problems caused by the growing evolution of technology.
To this end, INAI is currently in the process of implementing the Cross-Border Privacy Rules System and is particularly interested in achieving adequacy as a "third country", in accordance with Article 44 of the General Data Protection Regulation (GDPR).

To conclude, please identify in your view the prerequisites for the GPA to remain relevant and effective in the data protection and privacy arena.

In the context of the current international health crisis, there is a strong need to make use of new technologies that have been helping us to simplify many daily activities.

> **Recommendations and best practices should be designed to develop national strategies on cybersecurity, in which data protection awareness is a priority**

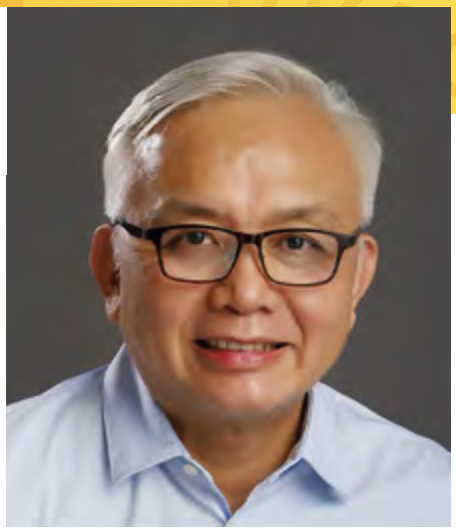
Nevertheless, it is important to ensure that there is no harm to individuals' privacy while using these new technologies. Therefore, international debates should promote privacy by design and by default, as well as impact assessments, as fundamental elements to guarantee the protection of personal data.
Also, recommendations and best practices should be designed to develop national strategies on cybersecurity, in which data protection awareness is a priority.

Finally, we must work towards the construction of new models that overcome the conflict of different fundamental rights and promote their proper application, so that we do not prioritise one over another.

Observer on the Road

Update from the GPA observer at the International Organization for Standardization (ISO)

Raymund E. Liboro, Privacy Commissioner at the National Privacy Commission (NPC), Philippines, reports as the GPA representative at the ISO



Active involvement in the ISO standard development process

Strengthening relationships with other international bodies and networks advancing data protection and privacy issues is a key priority of the Global Privacy Assembly (GPA), (formerly the International Conference of Data Protection and Privacy Commissioners or ICDPPC) as part of its 2019-2021 Strategic Plan.
In fact, a Resolution on Development of International Standards was issued during the 29th ICDPPC in Montreal, Canada in 2007. Even as early as then, the Conference called on its members to consider potential mechanisms for effecting liaison with the ISO on behalf of the Conference, and to become more actively involved in the ISO standards development process via their respective national standards development organisations.

Aligned with the GPA's current strategy, the NPC has been making a significant contribution to the development of global standards for data privacy and protection since 2017. The NPC is actively involved as both the Philippine representative and GPA Observer to the Sub-committee 27 of the ISO's International Electrotechnical Commission's Joint Technical Committee 1 or the ISO/IEC JTC 1/SC 27.

Specifically, the NPC is part of Working Group (WG) 5 of the SC 27. It contributed extensively to the development and maintenance of data protection standards and guidelines addressing security aspects of identity management, biometrics, and privacy.

The NPC is one of the few nascent data protection authorities actively participating as members of the ISO/IEC JTC 1/SC 27 & WG 5.

It is worth noting that the NPC contributed to the data-sharing agreement content of various ISO issuances, namely on security techniques and privacy information management guidelines. This ably positioned the NPC to weigh in on the discussions and adoption of standards that

have strategic importance to the future of global privacy.

As early as 2007... the Conference called on its members to consider potential mechanisms for effecting liaison with the International Organization for Standardization (ISO)... via national standards development organisations

The NPC has taken on notable roles and responsibilities, such as: being a member of the advisory group on strategy; liaison representative to the GPA; and co-editor for issuances on organisational privacy risk management, consent record information structure, entity authentication assurance framework, digital authentication: risks and mitigations.

Additionally, it has also provided valuable inputs on the ISO Working Draft to implement privacy by design for consumer goods and services.

NPC's role in the development of national and international standards

In the ASEAN region, the NPC is a privacy and data protection trailblazer in terms of incorporating ISO/IEC JTC 1/SC 27 & WG 5 standards throughout the promotion and institutionalisation of best data privacy and protection practices in the region.

Within its jurisdiction, the NPC has expanded its influence by becoming a vital cog in the formulation of ICT standards and compliance monitoring.

The Commission is currently a member of the Department of Trade and Industry's Bureau of Philippine Standards Technical Committee on Information Technology and its sub-committee on information security, cybersecurity, and privacy protection. These respectively serve as counterpart groups of JTC 1 and SC 27 in the country as they review and adopt specific international standards as Philippine National Standards (PNS).

The NPC employs an effective strategy to ensure the country's compliance with international standards for data protection by adopting standards published by the ISO/IEC. These include standards for privacy technologies, identity management, and information security which are generally accepted international principles and standards for data protection.

Reviewing and adopting the guidelines, requirements, and specifications set by ISO/IEC are crucial for the NPC. These standards promote organisational accountability and encourage public and private organisations to implement data protection guidelines that conform to the country's Data Privacy Act and other global regulations.

To date, the NPC has been using PNS as references in creating guidelines and policies issued to stakeholders and industry sectors for privacy risk management and implementation of data protection controls and procedures.

The Commission is also incorporating relevant privacy management standards from the European Union's General Data Protection Regulation and the UK's Information Commissioner's Office (ICO), both global benchmarks for the robust protection of data privacy rights.

Secretariat note for GPA Members: The GPA Secretariat, in coordination with the NPC has recently distributed more information by email to GPA members about how you can obtain more information about the activities at ISO, and potentially get involved in future work.

Contact **secretariat@globalprivacyassembly.org** for more information.

Have you thought about contributing to the GPA Newsletter?

We are now planning editorial for the May edition of the Newsletter, please contact the GPA Secretariat if you would like to contribute, and for more information on any of the issues highlighted, contact secretariat@globalprivacyassembly.org.

Report on the 54th Asia Pacific Privacy Authorities (APPA) Forum by the Office of the Victorian Information Commissioner (OVIC), Australia

Hosted by the Office of the Victorian Information Commissioner (OVIC), Australia, the 54th meeting of the Asia Pacific Privacy Authorities (APPA) took place from 8-10th December 2020. Due to the COVID-19 pandemic, the forum was held virtually. It was well attended by all 19 member authorities and 8 observers.

The agenda over the three days covered a range of items including updates from the APPA Working Groups, sharing of jurisdiction reports, and discussions on topical privacy issues currently faced by many authorities.

Privacy implications of COVID-19 pandemic

One of the key topics discussed throughout the forum was the privacy challenges associated with the COVID-19 pandemic. Governments globally have had to implement extraordinary measures to manage the spread of the virus. Some of these measures, like contact tracing, involve the collection and use of personal information and it was encouraging to hear members confirm that they were consulted by their respective governments at different stages of the development of these measures. Members agreed that while public health measures enforced in response to the virus were crucial, it was also necessary to ensure that they did not unreasonably infringe upon individuals' information privacy rights.

The COVID-19 pandemic caused a significant shift to remote working and learning, and an increased reliance on digital tools. Members presented on the privacy and cybersecurity challenges that emerged during the pandemic. Of interest was the discussion on digital learning tools and children's privacy. Members recognised that without adequate education and guidance on the risks of online learning, children are susceptible to digital harms. These discussions highlighted the need for members to work with schools and government to ensure digital tools adequately protect children's privacy.

Facial Recognition and Artificial Intelligence

Members presented on the increasing use of facial recognition technology and artificial intelligence in their respective jurisdictions, and shared case studies that highlighted the importance of ensuring that fundamental rights to privacy are protected.

There was reflection on the adequacy of remedies available to individuals when facial recognition technologies are used in harmful or unlawful ways. This prompted members to consider the value of understanding the incentives that drive businesses to engage in unlawful practices as a way of determining how to discourage such practices.

It was clear from discussions that the use of facial recognition technologies and artificial intelligence will only become more relevant in the years to come.

Privacy law reform and the future of privacy frameworks

Members provided updates on legislative developments and regulatory changes in their respective jurisdictions, and the issues that those changes are seeking to address. These included how contemporary privacy issues such as transborder flows of personal information, consent, the definition of personal information, mandatory data breach reporting schemes, and the regulation of children's privacy might impact the future of privacy frameworks. The objectives of these reforms - or proposed reforms - include ensuring privacy laws are fit for purpose in the digital era, strengthening protections for personal information and more closely aligning privacy laws with international jurisdictions such as the European Union's General Data Protection Regulation.

There were engaging presentations on different cultural attitudes towards privacy. These discussions highlighted that privacy law, which is predominantly focused on individual privacy rights, may not accurately reflect the values and norms of groups of people whose cultural background places stronger emphasis on the collective rather than just the individual. Notably, some members are working with such groups on solutions to this issue.

OVIC would like to thank all attendees who contributed their ideas and shared their experiences during the forum, and the APPA Secretariat for their assistance in organising the meeting. It was an honour for OVIC to host the 54th forum.

The 54th APPA forum communique is available online at appaforum.org.

The 55th APPA forum will be hosted by the Personal Information Protection Commission, the Republic of Korea in June 2021.

Meet our Member

Nelson Remolina Angarita, Deputy Superintendent for the Protection of Personal Data, Superintendence of Industry and Commerce, Republic of Colombia

The Challenge of the 21st Century

The Superintendence of Industry and Commerce (SIC), established in 1959, acts as the Data Protection Authority of Colombia and guarantees that public and private entities comply with both the principles and rights in the treatment of personal data.

As a constitutional right, data protection should not be regarded as a conflict of interest but as a right that benefits all – citizens, companies and public authorities. Regulation is thematically and technologically neutral because it applies to the processing of data through any technology, present or future, and to any related activity (artificial intelligence, etc.). Contemporary society demands that this is initiated from the beginning of any project involving the processing of personal data. The law should be implemented, taking into consideration privacy, ethics, safety and accountability, both by design and by default.

The adequate processing of personal data is the right of the 21st century for citizens, but, at the same time, the effective protection of such a right is the main challenge of this century. As of January 2021, more than 4.788 billion people have access to the Internet, which is equivalent to 63% of the world's population. How do we effectively protect – not merely formally – the rights of these cyber-citizens from the processing of their personal data by any person, company or government anywhere in the world?

What happens on the Internet affects billions of people of different nationalities. It is an issue that potentially involves all of us. Therefore, it is crucial that data protection authorities work permanently as a team, and not in an isolated or sporadic manner. Take, for example, the following scenario: a security breach that happens anywhere in the world can affect billions of people in all countries. For this reason, all – not just one or a few – data protection and privacy authorities must initiate an investigation ex officio against the data controller responsible to demand greater security measures.

> It is urgent – to redesign the rules that regulate the international collection of personal data

The Internet cannot become a scenario where anarchy and impunity reign. It is possible that a company domiciled in a nation without data protection laws or a data protection/privacy authority, has information regarding billions of people worldwide. That company may claim it can use information for any purpose, without respect for individual rights, because, according to the company, it is domiciled in a country without data laws and, therefore, can act with impunity, given there is no regulation on that subject. Can this type of scenario be avoided? How can we guarantee that the information of any cyber citizen is collected and processed lawfully?

The Internet changed the world, but the world has not changed appropriately for the Internet. Throughout history in this field, until the twenty-first century, we have had regulations based on a territorial location. Although our planet has always been geographically divided, it is undeniable that it is now technologically merged, and that the phenomenon of cyberspace is becoming increasingly noticeable. If we continue to do more of the same, we will not be successful in protecting the rights of data subjects in the cyberspace. The socio-technological reality of the 21st century requires adopting different measures and reinforcing existing ones.

It is urgent – to redesign the rules that regulate the international collection of personal data

Indeed, strict measures have been implemented for several decades concerning the export of data from one country to another (international transfers of personal data). But little to nothing has been done to address the phenomenon of the international collection of personal data. In this regard, data leaves a country because someone from another country collects it through web pages, apps, digital social networks, and, in general,

using technological innovation/ tools. Faced with this, there is no control, and personal data can be transferred to anywhere in the world. The SIC as Data Protection Authority, has understood the need to address this situation and has taken several actions against businesses who misuse the duty of personal data protection in international collection.

For a long time, we have focused on international data transfers to protect the rights of data subjects whose information is sent from one country to another. But we have not paid attention to another phenomenon through which more data is moved from one country to another: the international collection of personal data.

Your GPA News Highlights

For each edition of the GPA Newsletter, this section features your GPA News Highlights

Happy New Year and welcome to our January 2021 edition of the GPA Newsletter. As the world continues to grapple with the COVID-19 pandemic, the GPA community comes together to share and disseminate knowledge amongst members and in support of this, the GPA Secretariat has outlined initiatives below for your information, requiring your valuable contribution.

The GPA Census and the Data Governance in the Public Sector Survey

The Global Privacy Assembly Census and the Data Governance in the Public Sector Survey will provide a vital insight into the way members and the data protection landscape are changing. Your contribution is important, identifying important patterns and trends, and analysis will form key work items for our working groups.

The **GPA Census** is designed to give a detailed 'snapshot' of privacy and data protection authorities' activities across the globe, as well as contributing to the aims of the Resolution on developing new metrics of data protection regulation.

The Data Governance in the Public Sector Survey is running in conjunction with the Census. This survey is run by the GPA's **Strategic Direction Sub-committee** to inform future work in the GPA on public sector data processing issues. Both the Census and the Survey are open from **1 December 2020 to 12 February 2021 for GPA Members only**.

GPA members will have already received the links to these surveys. Please contact the Secretariat if you have any queries: secretariat@globalprivacyassembly.org.

The GPA Reference Panel – Application process now open

At the GPA 2020 Closed Session, members agreed to relaunch the application process for the GPA Reference Panel in 2021. The GPA Reference Panel will be a contact group involving a variety of external stakeholders to provide expert knowledge and practical expertise on data protection and privacy related issues and developments in information technology.

We, therefore, invite applications from relevant external stakeholders, including civil society organisations, academic institutions, think tanks, non-privacy supervisory authorities, representatives of public authorities, such as law enforcement authorities, and representatives of the private sector with an interest in the vision/mission of the GPA.

The application window is **22 January 2021 until 12:00 noon GMT, 19 February 2021**. The call will run for 4 weeks; all relevant information is on the GPA website.

Accreditation 2021 – Now Open

The Global Privacy Assembly's (GPA) application process for new members and observers is now **open** for the 2021 cycle.

Since its foundation in 1979, the GPA has been continually growing and now includes more than 130 authorities from across the globe. The GPA now welcomes new applications from authorities who wish to become members and from public entities or international organisations that wish to participate in the GPA as observers.

- Applications for membership will remain open until **end of day, Sunday, 18 July 2021**
- Applications for those public entities or international organisations who wish to join as GPA observers will remain open until **end of day, Sunday, 22 August 2021**

All information including application forms can be found on the GPA website.