International Enforcement Cooperation Working Group

Report – July 2021

Chair authorities:

- Office of the Privacy Commissioner of Canada
- UK Information Commissioner's Office
- US Federal Trade Commission

Table of Contents

Executive Summary

The International Enforcement Cooperation Working Group (IEWG) is pleased to present this report to the Global Privacy Assembly (GPA) on its activity, progress and successes in 2020-21.

Heading towards the end of its second year in operation as a permanent Working Group of the GPA, the IEWG is co-chaired by the Office of the Privacy Commissioner of Canada, the UK Information Commissioner's Office, and the US Federal Trade Commission. It has increased its membership by over 80% since the virtual GPA in 2020, with a total of 29 members including many from regions not previously represented in the IEWG.

The IEWG's work continues to be integral to the GPA, particularly in advancing its objectives to promote and support enforcement cooperation in Pillar 2 of the Policy Strategy in the GPA's 2019-21 Strategic Plan. To that end, the IEWG co-chairs are pleased to report on an excellent second year in which significant progress has been made to deliver on these objectives and the IEWG's mandate to provide its members with an active forum for practical enforcement cooperation.

This has been achieved through a combination of delivery of tangible products that support cooperation (including the IEWG's safe space framework and the updated Enforcement Cooperation Handbook[1]), and the active participation of its membership in joint compliance activity (such as the establishment and progression of work in sub-groups focusing on video teleconferencing services, credential stuffing, facial recognition technology, and data scraping). In addition, substantive progress has been made in other priority areas of the IEWG's work plan including refreshing the Enforcement Cooperation Repository and engaging with other networks of data protection and privacy enforcement authorities.

Moving forward, and in line with the strategic priorities of the GPA over the next two years, the IEWG will look to maintain the momentum of its work, while also broadening its scope with a particular focus on: capacity building; further increasing the regional and linguistic diversity of the group; and exploring opportunities, with the Digital Citizen and Consumer Working Group, for operationalising cross-regulatory cooperation.

[1] The updated Handbook is to be shared with GPA members in advance of the GPA Conference in Mexico.

Introduction

Background

Building on the work of previous, temporary, enforcement cooperation working groups, the International Enforcement Cooperation Working Group (IEWG) was established as a permanent working group of the Global Privacy Assembly (GPA) following the 41st Conference in Tirana in 2019. The overarching mandate of the IEWG is derived from Pillar 2 of the Policy Strategy in the GPA's 2019-2021 Strategic Plan. This called for the IEWG to refresh its objective as:

> "…an active group considering live issues and concerns related to enforcement, with a focus on sharing experience, tactics and approaches to tackling specific aspects, including common experience in investigating multinational companies."

In its first year of operation as a permanent working group (2019-2020), the IEWG made good progress in working towards delivery of its mandate, as set out in its annual report to the virtual GPA in 2020. Key achievements during this period include the introduction of 'safe space' sessions to support and encourage live enforcement cooperation, and the development of the 'regional champions' model to promote the work of the IEWG and increase the diversity of membership and participation in the group.

Looking ahead to its second year (2020-2021), the IEWG committed to build on these achievements by making substantive progress on other aspects of its work plan, including updating and refreshing practical tools to support enforcement cooperation, and reaching out to other networks of data protection and privacy enforcement authorities.

Membership

Between 2019-2021, the work of the IEWG was led by three co-chair authorities:

- Canada - Office of the Privacy Commissioner of Canada (OPC)
- United Kingdom - Information Commissioner's Office (ICO - also provides IEWG Secretariat)
- United States of America - Federal Trade Commission (FTC)

Working to an engagement plan developed by the OPC, the IEWG co-chairs, Secretariat and regional champions (the OPC, the Turkish Personal Data Protection Authority, and the Privacy Commissioner for Personal Data Hong Kong SAR, China) have worked hard to increase the membership of the group, with a particular focus on enhancing regional and linguistic diversity. The IEWG co-chairs are pleased to report that the group's membership now stands at 29 authorities from six continents; an increase of over 80% since the virtual GPA in 2020. In addition to the co-chairs, the IEWG now comprises the following authorities (new members highlighted in italics):

- *Abu Dhabi - Office of the Data Protection Commissioner, Abu Dhabi Global Market*
- Albania - Information and Data Protection Commissioner
- Argentina - Access to Public Information Agency Argentina
- Australia - Office of the Australian Information Commissioner (OAIC)
- Belgium - Belgian Data Protection Authority
- *Burkina Faso - National Commission for Informatics and Liberties*
- *Canada - Information and Privacy Commissioner of Ontario (IPC)*
- *Côte d'Ivoire - Telecommunications / ICT Regulatory Authority of Côte d'Ivoire*

- *Colombia - Superintendence of Industry and Commerce of Colombia (SIC)*
- *Dubai - Data Protection Commissioner, Dubai International Financial Centre*
- European Union - European Data Protection Supervisor (EDPS)
- Germany - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
- *Georgia - State Inspector's Service*
- Gibraltar - Gibraltar Regulatory Authority (GRA)
- Hong Kong SAR, China – Office of the Privacy Commissioner for Personal Data (PCPD)
- *Iceland - Icelandic Data Protection Authority*
- *Jersey - Jersey Office of the Information Commissioner (JOIC)*
- *Mexico - National Institute for Transparency, Access to Information and Personal Data Protection*
- *Monaco - Commission for the Control of Personal Data*
- Netherlands - Dutch Data Protection Authority
- New Zealand - Office of the Privacy Commissioner
- *Norway – Norwegian Data Protection Authority*
- Philippines - National Privacy Commission (NPC)
- *Senegal – Personal Data Protection Commission*
- Switzerland - Swiss Federal Data Protection and Information Commissioner (FDPIC)
- Turkey – Turkish Personal Data Protection Authority

Work plan

Taking account of the global pandemic, and focusing on the areas of the IEWG's work that would add most value to its members and the wider GPA, the co-chairs prioritised the following items from the IEWG's work plan for progression in 2020-21:

- *Priority 1 – Foundations*: Lay the foundations for the IEWG and GPA to facilitate practical enforcement cooperation, focusing on organisations and issues with significant global impact on people's data protection and privacy rights.
    - Objective 1 - Develop 'safe space' enforcement cooperation framework focused on multinationals.
    - Objective 2 - Use of and evaluation of framework in practice.
- *Priority 2 – Tools*: Build on the work of the previous IEWG to further develop practical tools for enforcement cooperation.
    - Objective 1 – Update Enforcement Cooperation Handbook.
    - Objective 2 – Maintain and promote enforcement cooperation repository.
- *Priority 3 - Awareness and communication*: Ensure the IEWG has a good awareness of the global Privacy Enforcement Authority (PEA) network landscape and maintains or establishes mutual lines of communication and observation to coordinate and leverage activities.
    - Objective 1 – Analyse global PEA networks and make recommendations on coordination.
    - Objective 2 – Develop existing and new mutual observation agreements.

- *Facial Recognition Technology (FRT)*: Work with the Ethics and Data Protection in AI Working Group (AIWG) to deliver the commitments in the Resolution on FRT (adopted at the virtual GPA in 2020) to develop and promote a set of principles for the use of personal data in FRT.
    - Objective 1 – Develop principles, for adoption in a GPA resolution, based on research and stakeholder engagement.
    - Objective 2 – Promote principles and review industry application.
- *Video Teleconferencing (VTC) services*: Progress the VTC joint action by further engaging with VTC companies to clarify and improve privacy practices, and increase public trust in use of VTC services.
    - Objective 1 – Undertake direct engagement with VTC companies on key aspects of their privacy practices.
    - Objective 2 – Issue substantive public statement setting out findings.

In addition, the co-chairs incorporated two further items into the IEWG work plan following safe spaces sessions and interest from members to progress joint activity in these areas:

- *Credential Stuffing*: Establishment of a temporary IEWG sub-group with objectives to explore and consider joint actions to help address and mitigate risks arising from credential stuffing attacks.
- *Data scraping*: Establishment of a temporary IEWG sub-group with objectives to explore and consider joint actions to clarify and set expectations of the privacy regulatory community around companies' obligations to protect against the scraping of publicly accessible personal data.

Liaison with the Strategic Direction Sub-Committee

In 2020-21, the IEWG continued to regularly update the Strategic Direction Sub-Committee (SDSC) on the progress of its work, in written quarterly reports. In May 2021, the IEWG participated in the seventh meeting of the SDSC to provide:

- further detail on activity undertaken to advance the 2019-21 Strategic Plan (including the further development of the safe space sessions, updates to the Enforcement Cooperation Handbook, and engagement with other networks);
- updates on aspects of IEWG work with key links to the broader social, political and economic debate (including work to progress the FRT resolution, and activity on VTCs and credential stuffing); and
- the working group's view on the development of the new 2021-23 GPA Strategic Plan (including highlighting its synergies with the planned future direction of the IEWG, and supporting an approach of 'evolution' rather than 'revolution').

The IEWG co-chairs were pleased to receive positive feedback from members of the SDSC, in particular on the value of participating in safe space sessions to help to inform their considerations and actions on the issues discussed.

Working Group Activities

Safe space framework

In 2019-20, the IEWG took the first steps towards establishing itself as an active forum for enforcement cooperation on live and pressing issues. It did so through the development of safe space sessions. These provided a confidential environment for IEWG members to discuss emerging privacy and enforcement matters of global impact, and explore collaborative opportunities.

Building on the early success of the safe space sessions, the IEWG has dedicated significant effort over the last year in further developing and formalising these sessions through the creation of the Safe Space Framework. The framework (developed by the ICO with support from the GRA and the EDPS) documents what the safe space sessions are and how and why they're run. It puts a structure around the sessions to make them more replicable and accessible for any IEWG member to participate or lead. It does this by:

- establishing three principles that underlie the development of sessions:
    - Global – focusing on issues of global impact,
    - Practical – encouraging consideration of options for cooperation,
    - Inclusive – urging proactive consideration of ways to engage members;
- setting out a flexible timetable for sessions across the year;
- explaining how to prepare to lead a session, including selecting an appropriate topic, setting objectives for the session, carrying out research and preparing background materials;
- describing how to run a session, including the provision of a template slide pack, and recommendations for chairing a discussion; and
- providing a process for following-up a session, including reviewing objectives, circulating a meeting note, and establishing sub-groups where appropriate.

Safe space sessions

The framework was completed in February 2021. Subsequently, IEWG members were invited to use the framework to lead the development and running of safe space sessions. This helped to test the framework in practice. During 2021, four IEWG members led sessions as below:

- *Credential stuffing* – In March 2021, the GRA led a safe space session on the topic of credential stuffing. With objectives to share experiences and consider options for joint working, participants discussed relevant closed enforcement cases, levels of breach reporting and policy and guidance products. Following the session, six IEWG members expressed an interest in joint action on this topic, and the GRA set up a sub-group to progress relevant work. The credential stuffing sub-group has since undertaken research and information gathering across IEWG members and with external stakeholders (including via the GPA's Reference Panel) and is making excellent progress in developing international guidance on credential stuffing for both organisations and the public. This work will continue in 2021-22 as part of the IEWG's forward looking plan.

- *FRT investigative debrief* – In April 2021, the OPC led a safe space session on its recently concluded joint investigation (with Canadian partners) into the FRT image-matching company Clearview AI. In addition to setting out its findings from the joint investigation, the OPC chaired a fruitful discussion where participants moved towards a shared understanding of some of the key privacy principles, issues and concerns in relation to use of FRT. This session helped inform and feed into the work of the IEWG and AIWG in progressing delivery of the GPA's FRT resolution.
- *Global incident* – In May 2021, the PCPD Hong Kong SAR, China led a safe space session regarding a reported incident involving the personal data of individuals across several jurisdictions. Following a presentation on the known background to the incident, participants discussed their respective understanding of the issue and shared information on any steps and/or enquiries being taken domestically to respond and gather further information about the incident. This session was valuable to help participants gain a better understanding of the state of play of the issue, both in terms of a technical understanding of the incident itself, and the positions and action taken or planned by other authorities.
- *Data scraping* – With issue linkages to the 'global incident' session, in June 2021, the OAIC led a safe space session on the topic of data scraping – the practice of extracting data from websites and public facing access points. The session's objectives were to raise awareness of the issue, better understand members' policy and enforcement positions, and gauge appetite for cooperative action. Participants discussed relevant aspects of their domestic laws and closed enforcement cases to help inform how to characterise instances of data scraping, and considered whether joint regulatory intervention of some form would be appropriate. Following the session, several IEWG members indicated appetite to be party to further work to consider and progress joint activity on the topic, and the OAIC are in the process of establishing an IEWG subgroup for that purpose.

Feedback from IEWG members that led these safe space sessions was largely positive, indicating that the framework proved useful in supporting preparation ahead of sessions, through clear guidance, and flexible recommendations and templates. Increasingly positive participation of members in the respective sessions and active discussions were reported, and the framework and sessions were found to be valuable and practical tools to bridge differences in regulatory approach and legal frameworks across jurisdictions. One authority noted the value of the framework and sessions in enabling less well-resourced authorities to leverage the expertise of other authorities and use discussions to inform their own domestic policy and approaches. As regards opportunities for further improvement, it was highlighted that there may be scope to explore how to better support authorities in establishing and progressing joint action that involves use of formal enforcement powers (such as joint investigations), while recognising that this does not diminish the value of other, less formal, forms of cooperation that the framework and sessions currently support.

Enforcement Cooperation Handbook

The GPA's Enforcement Cooperation Handbook was originally created in 2015, and updated in 2016. Based on contributions and experiences of members from across the GPA, it provides guidance and a common foundation for authorities wishing to engage in enforcement cooperation. It sets out: the issues an authority may face in preparing for, and engaging in, enforcement

cooperation; models, approaches, and solutions to address such issues; and how to choose appropriate strategies in different circumstances.

Working with colleagues in the Digital Citizen and Consumer Working Group (DCCWG), the IEWG has this year undertaken several activities to deliver the objective of updating the Handbook to reflect the wealth of experience gained and lessons learned through enforcement cooperation since it was last updated, both between data protection / privacy enforcement authorities and in a cross-regulatory context. This work has been undertaken by the OPC (overall lead), the SIC and the JOIC, with additional support from the ICO.

To better understand how the Handbook has been used by authorities, what works well and what areas of improvement there might be, the OPC developed a survey which was circulated to members of the GPA and several other networks (including the Global Privacy Enforcement Network, the International Consumer Protection and Enforcement Network and the International Competition Network) in late 2020. With an excellent response rate, the SIC and the JOIC were able to analyse and draw out valuable themes from the data to help inform the areas of priority and focus for updating the Handbook. Key findings from this analysis included:

- Most respondents indicated they had the legal and practical ability to cooperate, including in a cross-regulatory context, but there were limited concrete examples provided of cooperation on specific investigations.
- Most respondents also reported that they had not actually used the handbook to support them in cooperation enforcement projects.
- Many respondents were keen for real-world examples of how to apply the theoretical concepts encompassed in the handbook in practice.

Based on these findings, the OPC are now leading the drafting of an updated version of the handbook, with particular consideration given to incorporating case studies and practical tools, such as terms of references, to help give authorities extra confidence in their ability to cooperate with partners across borders and regulatory regimes. To this end, a further targeted engagement exercise is being undertaken to elicit relevant case studies and templates for inclusion in the Handbook. In addition, thought is being given, in parallel with the IEWG's drive to increase the regional and linguistic diversity of the group, as to methods to promote the Handbook and its use in regions that are currently less well-engaged with the IEWG and the practice of enforcement cooperation more generally.

The IEWG and DCCWG aim to finalise their update to the Handbook and share it with all GPA members ahead of the Mexico GPA in October 2021.

Enforcement Cooperation Repository

In 2019, the then temporary IEWG established the Enforcement Cooperation Repository. The repository is a digital library on the GPA website that centralises links to publicly available and non-confidential resources of value to the global community of data protection and privacy enforcement authorities. Amongst other things, the repository links to guidelines, regulatory opinions, investigation reports, enforcement notices, annual reports, Memoranda of Understanding; press releases and joint statements.

To remain useful, it is vital that the repository remains up to date, is actively managed and, where necessary, improved. To this end, the IEWG carried out two key activities in 2020-21. These pieces

of work, summarised below, were led by the Turkish Personal Data Protection Authority, with support from the OPC and the ICO:

- *Repository refresh* – Most content in the repository was added at the time of its creation in 2019. To ensure these resources remain valid, and to refresh and add new resources, the IEWG used several communications channels. In August 2020, the IEWG reached out to all GPA members via the GPA Secretariat to promote the repository and seek further resources for inclusion. In January 2021, the IEWG contributed a Working Group update to the GPA's Newsletter, and used the opportunity to invite members to contribute new or recent resources to the repository. And in May 2021, the IEWG sent targeted emails to around 40 authorities and networks with the dual purpose of eliciting further valuable resources for the repository, and fixing broken links. These efforts proved successful, with the provision of over 70 new resources, from 14 authorities and networks, for inclusion in the repository. The IEWG Secretariat is now working on a bulk upload of these resources to the repository.
- *Repository Road Map* – As regards ongoing maintenance, the IEWG developed a 'Road Map' for the repository (see Annexe). This is a short document that sets a governance structure and scope for iterative improvements over the short and longer-term. Key proposals include:
    - the establishment of a voluntary Steering Committee of three IEWG members with responsibility for maintaining and updating the repository at regular intervals;
    - short-term enhancements including more intuitive naming of the different parts of the repository, and improved formatting and filter options; and
    - longer-term enhancements including improved search and tagging functionality, and automatic notifications of new resources.

  The IEWG plan to begin implementation of the proposals in the Road Map following the Mexico GPA in 2021.

Network engagement

Awareness of, and communication with, other networks of data protection and privacy enforcement authorities is vital to ensure IEWG activity can feed into, and be informed by relevant works across several other groups. The IEWG made substantive progress in this regard in 2021, led by the ICO with support from the BfDI, the FDPIC, the NPC and the OPC. In February 2021, the IEWG reached out to 17 global, regional and linguistic networks to set out the IEWG's network engagement activity and gather up-to-date information from the networks as regards their respective overarching purposes; current objective and areas of focus; and activities of relevance to enforcement and cooperation.

The IEWG received an excellent response to its outreach, with all 17 networks engaging positively and providing valuable detail on their activities and forward looking objectives. The responses were analysed and summarised in infographic form as a 'landscape snapshot'. While the primary purpose of the snapshot was to inform the next stage of the IEWG's network engagement activity, it is also a valuable resource for the broader GPA membership as a centralised summary of the work and focus of the majority of the world's data protection and privacy enforcement authority networks. As such, the infographic is available to all members in the Enforcement Cooperation Repository.

Working from the landscape snapshot, the IEWG developed a more detailed set of recommendations for areas of work and ambition across the IEWG and other networks that could benefit from coordination and / or leveraging of activity to the mutual benefit of two or more networks. Proposals include the development of permanent communication channels between and across the IEWG and networks; joint capacity building activities; and back-to-back events.

Following consultation with IEWG members and discussion amongst the authorities leading on and contributing to this activity, the IEWG is now in the process of drafting an engagement plan to implement the proposals, with short-term goals to establish systematic cooperation links between the IEWG and other networks, and medium to longer-term goals to develop those links into tangible opportunities for coordination and joint activity. The engagement plan will be finalised ahead of the Mexico GPA in 2021 and will form part of the IEWG's work plan for 2021-23.

VTC sub-group

In 2020, the IEWG established a sub-group to explore possible collaborative actions to help address concerns around the increased privacy risks from the sudden growth in use of VTC services during the global pandemic. This led to six IEWG members (the OPC, the ICO, the OAIC, the GRA, the FDPIC and the PCPD Hong Kong SAR, China) jointly signing an open letter. The letter set out the concerns of the joint signatories and provided VTC companies with guiding principles to address key privacy risks. Some of the biggest VTC companies were invited to respond to the letter to set out how they take the principles into account.

Following replies from Microsoft, Google, Cisco and Zoom, the joint signatories each issued a press release in December 2020 as an interim update and to briefly set out next steps. The VTC sub-group collaboratively analysed the responses and identified areas of interest for follow-up with the VTC companies, including their approaches to end-to-end encryption, privacy-by-design and default, processing of personal data by third-parties, and end-user control.

In April and May 2021 the VTC sub-group engaged directly with Microsoft, Google, Cisco and Zoom in a series of video calls, each chaired by a different member of the sub-group. The calls allowed these VTC companies to elaborate on the steps they take to implement, monitor and validate the privacy and security measures they put in place, and in some cases show how such measures work in practice.

Following this engagement, the sub-group assessed the further information provided, and developed a concluding substantive public statement on the joint activity. Each member of the sub-group plans to publish the statement in a press release shortly after submission of this report in August. The statement highlights areas of good practice reported to the joint signatories (including security testing, implementation of privacy programs, and provision of meeting controls), and identifies some opportunities for further enhancement or improvement (in the areas of encryption, secondary use of data, and location of data).

Reflecting on this joint activity, the IEWG co-chairs consider that the coordinated work of the sub-group has proven effective and proportionate in helping to improve privacy practices across the VTC industry, representing an efficient option on the collaborative enforcement response continuum. They highlight this model of engagement as valuable and replicable in other circumstances where emerging issues would benefit from open and constructive dialogue to set out regulatory expectations, provide opportunities for demonstration of compliance, and ultimately foster public trust in innovative technologies.

IEWG-AIWG FRT sub-group

Background

The virtual GPA in 2020 adopted a resolution that tasked the IEWG and AIWG with developing a set of principles and expectations for the use of personal data in FRT. With coordination from the IEWG Secretariat, an IEWG-AIWG FRT sub-group was established in late 2020 to progress work mandated by the resolution. The sub-group comprises the EDPS, the FDPIC, the ICO, the IPC, the Japan Personal Information Protection Commission, the OAIC, and the OPC.

Project plan

In January 2021, the sub-group developed and agreed on a project plan for delivery of the resolution. The plan sets out three deliverables:

1. A concise and meaningful set of principles that are designed with a focus on usability and application in practice.
2. Plans for promoting the principles via stakeholder engagement and evaluation of industry application of principles.
3. Reflective report on stakeholder engagement and industry application of principles.

The plan also sets out a phased and collaborative approach for delivery of the deliverables:

- a *research phase* to gather relevant material from GPA members and external stakeholders;
- a *development phase* to analyse the information gathered, and draft and consult on the principles; and
- an *adoption phase* to present the principles for adoption by the GPA, and promote and review their application in practice by industry.

State of play

The sub-group is currently making good progress in undertaking the research phase. In February and March 2021, subgroup members each carried out desk-based research to create an initial pool of relevant material reflecting policy and enforcement activity on FRT by the members themselves, as well as court judgements, reports and articles from other bodies that have helped inform that activity.

In April 2021, the subgroup developed a survey to elicit feedback from GPA members on their views and experience of FRT. The survey sought specific input from members on any policy and guidance products they had developed on FRT, any enforcement actions taken, and any stakeholders engaged as part of that work. It also asked members to set out, with brief explanation, their views on the riskiest purposes for deploying FRT, the most significant data protection and privacy risks associated with those purposes, and any real world examples of use cases they were aware of in their jurisdiction.

There was an excellent response rate to this survey, with over 35 replies from a geographically diverse mix of authorities, providing valuable information on their activities and perspectives on use of FRT around the world. It is clear there is significant and important work across the GPA

membership on FRT, and the sub-group take this opportunity to spotlight some key policy and enforcement updates from that work here.

Key updates

Australia – Office of the Australian Information Commissioner (OAIC) and Office of the Victorian Information Commissioner (OVIC)

The OAIC's regulatory role includes handling complaints, conducting investigations, monitoring, advice and providing guidance on proposed uses of biometric information under Australia's Privacy Act. The OAIC has conducted assessments of the handling of personal biometric information collected through and used in facial recognition technology.[2]

Australia's proposed Identity-matching Services (IMS) Bill 2019 contains provisions which will permit the use of FRT for several national security and law enforcement purposes. This draft legislation has been reviewed by the Parliamentary Joint Committee on Intelligence and Security (Parliamentary Committee)[3] but has not yet passed into law.

The OAIC made a submission to the Parliamentary Committee on the IMS Bill which suggested that the Bill required further consideration to better ensure that any adverse effects of the proposed enactment on the privacy of individuals are minimised.

As well as producing general guidance on biometrics and privacy for the public sector in Victoria (which highlights some key privacy challenges including issues around covert data collection and validity of consent) the OVIC has made a number of submissions specific to the IMS Bill, including a public submission to the relevant Parliamentary Committee. The submission highlights OVIC's concerns with the bill, including: a lack of enforceable governance for use of FRT; the potential for scope creep; inadequate reporting / oversight.

Belgium – Supervisory Body for Police Information (COC)

In Belgium, the Federal Police at Brussels Airport (Zavaentem) carried out a test using FRT. As part of the test, LFR was deployed on four cameras to match individuals walking through the airport against a wanted list. The COC, which has the role of Data Protection Authority for law enforcement processing of personal data, carried out an investigation into the test and issued a report to summarise its findings and the action taken. The COC found that although the test was partially discontinued due to high margins of error, the LFR system actually remained active in part. Based on an analysis of the test against the legal framework, the COC also found that there

[2] See for example https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-the-oaics-assessment-of-department-of-immigration-and-border-protections-handling-of-personal-information-using-smartgate-systems/ and https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-the-oaics-assessment-of-ibms-handling-of-personal-information-using-smartgate-systems/.

[3] Please see the Parliamentary Committee's report of October 2019 at: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024343/toc_pdf/AdvisoryreportontheIdentity-matchingServicesBill2019andtheAustralianPassportsAmendment(Identity-matchingServices)Bill2019.pdf;fileType=application%2Fpdf.

was insufficient clarity on the appropriate legal basis for the test, and documents such as risk assessments had not been completed. The COC therefore issued a corrective order to suspend the LFR test project.

Canada – Information and Privacy Commissioners

Data Protection Authorities in Canada have long given detailed thought to the theoretical implications and real-world impact of deployment of FRT, issuing guidance and carrying out investigations that date back to the beginning of the century. Recently, in addition to a joint investigation into Clearview AI (Federal, British Columbia, Alberta and Quebec privacy authorities), a Special Report was tabled in Parliament regarding the outcome of the OPC investigation into the federal police service's use of FRT, as well as the commencement of public consultations on guidance for police force use of FRT. Further, the Atlantic Information and Privacy Commissioners of Canada joined together to issue a statement on the implications of FRT. In particular, the joint statement highlights the authorities' concerns with the accuracy of FRT systems, the potential for scope creep, and the proportionality of using FRT when less privacy invasive measures may be available.

European Union - European Data Protection Supervisor (EDPS)

In 2020 and 2021, the European Commission took significant steps in progressing plans to establish a legal framework for AI in the EU. The proposals, set out in a White Paper in 2020 and as a draft Act in 2021, include risk-based provisions that limit the use of AI for automated recognition of human features in publicly accessible spaces (such as LFR). The EDPS published an Opinion on the White Paper in 2020, and a Joint Opinion with the European Data Protection Board on the Act in 2021. Both Opinions are based on a comprehensive assessment of the objectives and approach of the proposals, and expert analysis of the potential implications. In its Opinions, the EDPS notes the extremely high risks posed by remote biometric identification of individuals in publicly accessible spaces and, as a starting point, calls for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context.

Japan – Personal Information Protection Commission (PPC)

The Ministry of Land, Infrastructure, Transport and Tourism (MLIT) of Japan launched a "FAST TRAVEL" initiative to address increased demand for air travel and shortage of human resources. As part of this initiative, airport companies in the Tokyo metropolitan area are introducing 'One ID', an optional service that streamlines boarding procedures using FRT. A study group was set up to examine the handling of personal data in the One ID service, including a call for public opinion and the development of guidelines for its use by airport companies. The PPC participated in the

study group as an observer and provided advice on privacy protection. This led to the publication of a Guidebook in 2020 which, amongst other things, highlighted that: the use of personal data should be limited solely to boarding procedure purposes; personal data should be deleted within 24 hours; and passengers should consent to the One ID service based on an easy-to-understand explanation of the service and how their personal data is used.

Philippines – National Privacy Commission (NPC)

In addition to publication of an Advisory Opinion on the use of FRT for ID systems (which set out the need for a valid lawful basis for processing personal data and transparency obligations to ensure individuals are aware of its use and how to exercise their rights), the NPC has also taken enforcement action against an organisation's deployment of FRT in one of their products. Grab Philippines is an app that provides several services including food delivery and ride hailing. In 2020, the NPC assessed, amongst other things, a pilot run by Grab using FRT for 'passenger selfie verification' as part of its ride hailing service. The NPC found that Grab did not sufficiently identify and assess the risks to the rights and freedoms of data subjects, and failed to identify an appropriate lawful basis or justify its proportionality. As such, the NPC issued a cease and desist order.

United Kingdom - Information Commissioner's Office (ICO)

Following investigations into trials of live facial recognition technology (LFR) by police forces in the UK, the ICO issued its first formal regulatory Opinion on the deployment of LFR by law enforcement in public places. In the Opinion, the ICO clarifies its position on the application of data protection law, including that use of LFR for law enforcement purposes constitutes sensitive processing; data protection impact assessments must be implemented; and those deploying LFR must meet the high bar of strict necessity. Building on this, the ICO issued a further Opinion on the use of LFR in public places by private companies and public organisations. Rooted in law, and informed in part by several ICO investigations into use or planned use of LFR, the Opinion sets out the ICO's expectations for assessing the crucial concepts of fairness, necessity and proportionality, and clarifies that organisations must also demonstrate high standards of governance and accountability, as well as being transparent with individuals about how their data will be used if they decide to go ahead with an LFR deployment.

United State of America – Federal Trade Commission (FTC)

In 2012, recognising the increasing use of FRT by organisations across the US, the FTC issued best practice guidance for use of FRT, highlighting amongst other things the need to ensure consumers are aware of the deployment of FRT, and for consumers to have a choice not to have their biometric data collected and used for FRT. Subsequently, in 2021, the FTC took enforcement action against Everalbum in the form of a proposed settlement for alleged issues in relation to its

use of FRT in its Ever app – offering cloud based photo storage. According to the complaint, many consumers were not informed about Ever's default use of FRT to automatically tag photos, they did not have an option to disable this, Everalbum did not inform consumers that it also used their photos to help train its FRT tool in the first place, and in addition, it retained images indefinitely even after account deletions. The FTC's proposed order requires Everalbum, amongst other things, to delete the FRT models and algorithms it developed, and to obtain users' express consent before using or developing FRT using their personal data.

In progress

The sub-group is currently concluding its plans for the final element of the research phase - engaging with external stakeholders. Relevant questions are finalised for organisations and industry bodies that develop and offer FRT services; organisations that use and deploy FRT products; lawmakers and regulators that set and enforce relevant regulatory frameworks; and civil society and research bodies that advocate or provide independent advice on development and use of FRT. The stakeholder list is being finalised, with the aim of ensuring a broad collection of experiences, views and opinions on FRT from organisations and bodies the world over. The sub-group expects to reach out to stakeholders in the weeks following submission of this report at the end of July 2021.

Next steps

In July 2021, the sub-group set out plans to commence the development phase of the project, beginning with analysis of the materials collated during the research phase. Sub-group members will work collaboratively to extract key themes, commonalities and areas of contrast, with an initial focus during August and September 2021 on documentation obtained from the desk-based research and survey of GPA membership, followed by analysis of responses from external stakeholders in September and October 2021.

Following the GPA in Mexico, the sub-group will work together on an initial draft of the principles by early 2022, using this analysis as an evidence base. The sub-group will undertake stakeholder consultation on the draft principles and iteratively work towards a final draft by mid-2022 for submission to the GPA Closed Session as a resolution for adoption. In parallel, the sub-group will draft engagement plans for promotion of the principles and review of their application by industry for implementation post-adoption.

Forward looking plan 2021-2022

Looking ahead, the IEWG co-chairs are pleased that enforcement and regulatory cooperation are likely to remain priorities in the GPA's refreshed Strategic Plan for 2021-23. The IEWG is committed to continue to deliver on these areas and is developing a programme of work with the aim of maintaining the momentum built up over the last two years, and further strengthening and expanding the scope of the group's activity.

In particular, the IEWG will continue to progress and / or enhance several areas of activity from its previous work plan. These include:

- *Safe space sessions / closed enforcement sessions* – Continuing to promote and use the framework for IEWG members to lead and follow-up on safe space sessions examining a variety of emerging digital risks, including an increased focus on developing and running sessions for capacity building. With a view to better reflecting the content and purpose of safe space sessions, from October 2021 the IEWG will refer to them as 'closed enforcement sessions'. The framework will be updated to reflect this change in terminology.
- *Enforcement Cooperation Handbook* – Following publication of the updated Handbook prior to the Mexico GPA this year, the IEWG will incorporate promotion and guidance on the use of the Handbook as part of its capacity building and network engagement activity, with a particular focus on regions with less experience in practical enforcement cooperation. It will also encourage the posting, by GPA members, of further enforcement cooperation case summaries to the Enforcement Cooperation Repository as a complement to the handbook.
- *Enforcement Cooperation Repository* – Implementing the repository Road Map by establishing a Steering Committee to regularly refresh resources and make iterative improvements to functionality.
- *Network engagement* – Beginning implementation of the engagement plan, including identifying IEWG leads for other networks, establishing systematic communications channels, and identifying initial opportunities for tangible joint activity, such as workshops or back-to-back events.
- *FRT sub-group* – Prioritising and progressing the FRT principles development and consultation stages of the FRT project plan with a view to adoption of the principles at the 2022 GPA.
- *Credential stuffing sub-group* – Following the completion of research and based on consultation with external expert stakeholders, the sub-group will finalise and publish guidance notes for organisations and the public on mitigating risks around credential stuffing.
- *Data scraping sub*-group – Progressing development on the IEWG's consideration of data scraping and identifying and delivering on an appropriate collaborative approach to provide clarity and positive impact on this global issue.

In addition, the IEWG aims to broaden the focus and impact of its activity by:

- *Diversity* - Further growing and servicing the regional and linguistic diversity of both its members and their active participation in the various work streams of the group.
- *Cross-regulatory cooperation* – Developing closer links with the Digital Citizen and Consumer Working Group to explore opportunities for practical cooperation across regulatory regimes and networks on real-world cases and issues.

Conclusion

In 2020-21, the work of the IEWG has continued to be central to the ambitions of the wider GPA as regards the promotion of regulatory and enforcement cooperation amongst its members and beyond. In particular, the IEWG has taken great strides in advancing Pillar 2 of the Policy Strategy in the 2019-21 GPA Strategic Plan by successfully delivering on its mandate to refresh and establish the group as an active forum supporting practical enforcement cooperation.

The IEWG co-chairs are pleased that, thanks to the considerable efforts of IEWG members, the last year has seen the delivery of some key outputs for the GPA (such as the safe space framework and the updated Enforcement Cooperation Handbook), and many tangible examples of collaboration (including joint working on the issues of credential stuffing and data scraping). In particular, the IEWG co-chairs draw attention to the success of the VTC sub-group in leveraging collaborative engagement between the privacy regulatory community and global technology companies to improve privacy practices in the VTC industry in a proportionate and effective manner.

But the IEWG co-chairs recognise that there is more to do. Regulatory and enforcement cooperation only continue to grow in importance as emerging technologies, data-intensive business models and cyber threats increase digital risks on a global scale. As such, the IEWG must maintain its momentum, and broaden and strengthen its activities to keep pace and provide the GPA community with the right platform and tools to address these increased risks collaboratively.

The IEWG co-chairs are confident the group is well prepared to meet these challenges through progression and enhancement of ongoing activity, and the addition of new work streams to expand the group's focus and leverage a greater range of skills, views and contributions to its work. The IEWG co-chairs thank all members of the group for their commitment and invaluable contributions over the last year.

Looking ahead to the next two years, the OPC plans to remain in place as co-chair, with the ICO and FTC stepping down in October 2021. The ICO and FTC plan to remain active members of the IEWG and look forward to handing over to a refreshed line-up of co-chairs that will ably steer the group through the next two years. In particular, the ICO and FTC place on record their gratitude to the OPC for remaining in position and providing the continuity of leadership and expertise vital to the continuing success of the group.

Annexe

International Enforcement Cooperation Working Group

Enforcement Cooperation Repository

-Road Map-

Content

Reason and Background

With the global development of digital tools and communication technologies, the issue of personal data privacy becomes more complex. To address this, cooperation amongst Data Protection and Privacy Enforcement Authorities is increasingly important. Supporting and informing each other's regulatory activity by proactively sharing key resources is vital part of cooperation. To facilitate this, in 2019 the GPA created a digital library on its website, named the Enforcement Cooperation Repository (the repository).

Purpose

The repository aims to centralize and make available online non-confidential resources that may be useful to Data Protection Authorities and other stakeholders in the realm of privacy and personal data protection.

Objective

The objective of this document is to identify how the current version of the repository can be improved and how to foster its use to the benefit of GPA members and external stakeholders.

Scope

Suggested improvements take into consideration the short-term challenges of applying any substantial changes to the website due to technical, capacity and resource limitations. However, the 'Next version' section below explores potential enhancements should such limitations be overcome in the future.

Suggested improvements cover the following areas : 1- Content; 2- Structure and format 3- Promotion 4- Update and maintenance 5- Governance 6- Next Version

Content

Links to DPA's non-confidential resources that may benefit other GPA members and external stakeholders, including but not limited to:

- Guidelines
- Opinions
- Reports of investigations
- Researches
- Public strategies, policies and procedures
- Decisions of Courts & DPAs

- Legislation and Regulation
- Newsletters, Articles
- Bulletins
- Memorandum of Understandings
- Social Media Posts such as video streams of Conferences, Panels, and Meetings
- Real-Life Case Scenarios
- Resolutions
- Joint Letters
- Statements

Structure and format

It is useful to rename the subgroups according to criteria such as networks, national or sub national authorities. They are renamed as;
1) Network Documents and 2) Authority Documents
In order to normalize the content of the repository which will use of the following structure (to be fine-tuned) to describe the resources.

Title	Type	Summary	Country	Year	Author		

Content should be uploaded in the original language with a brief summary or/ and title in English **and if possible** are also translated into French and/or Spanish by the Steering Committee.

The repository is currently split into two parts:

- Enforcement Cooperation Resources (resources from networks)
- Document Library (resources from authorities).

It is also recommended to develop a practical strategy on how to make the content more accessible to GPA members whose main language is not English.

Promotion

In order to encourage the use of the repository, it is suggested to :

- Prepare, publish on the GPA's website and circulate a tutorial on the repository that summarizes its content and explains how to locate specific resources despite the limited search feature.
- Send periodically (eg. twice times a year) the list of new uploaded resources with a notification e-mail by the Secretariat.
- Ask periodically (eg. twice a year) GPA members what resources may be useful for them and prioritize search for content accordingly.

Update and maintenance

Content should be updated and maintained. That is to include additional resources periodically and also to remove any that are outdated. To this end, the Steering Committee can rely on a network of contact points within GPA members. For this purpose, each GPA member will designate a specific contact point for the Repository.

With a mechanism operated by the IEWG Secretariat and supervised by the Steering Committee, GPA members will regularly receive notifications and the members will be asked to check whether the existing contents are up-to-date and share new contents -if available- with the Secretariat.

Explore the possibility of an open source automated tool that identifies and highlights broken links.

Governance

Some of the foregoing actions require a periodic follow-up. Therefore, it is useful to set up a steering committee that will ensure that the repository is maintained properly and regularly. The first Steering Committee (SC) will be established following the Mexico GPA. SC will mainly oversee the Repository activities at international level. The SC will also, with the IEWG Secretariat, manage the network of point of contacts among DPAs that volunteer to contribute to the repository. The SC and the IEWG Secretariat should meet as appropriate to coordinate their work.

The SC will be led by three DPAs, while other member DPAs and networks will contribute to the work on a voluntary basis. Each year at the plenary meeting of GPA, three DPAs are invited to volunteer for the SC membership candidacy.

The SC and the Secretariat will examine the opportunity and the conditions that should govern any addition to the repository of other publically available resources issued by external stakeholders.

Next version

Once possible to include substantial technical amendments to the GPA's website, it is recommended to consider the following :

1- Advanced search feature to find resources of interest. This will rely on metadata to describe each content
2- Audience Measurement (website activities could be tracked through cookies for measurement and analysis)
3- Notification Mechanism
4- Other features that may be useful to collaborative work.

Annex (templates)

- Letters prepared by Turkey