International Enforcement Cooperation Working Group

Report – adopted October 2020

Co-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) as an update on progress during its first year of operation. The IEWG is now a permanent Working Group of the GPA. It is co-chaired by the Office of the Privacy Commissioner of Canada, the UK Information Commissioner's Office, and the US Federal Trade Commission, and has a regionally diverse membership of 16 Authorities.

The work of the IEWG is integral to the GPA, supporting its strategic ambitions around leadership, collaboration, and fostering a global regulatory environment of high standards of data protection and privacy. The IEWG also has a key role in helping to advance the Assembly's Strategic Direction and associated GPA Policy Strategy. In particular, it has primary responsibility for leading on delivery of the enforcement cooperation element of the Strategy in Pillar 2 - from which the IEWG derived its mandate to form as a permanent Working Group.

Working from this mandate, in its first year of operation, the co-chairs of the IEWG prioritised activities to rapidly put into action the group's refreshed focus on creating an environment that supports and catalyses proactive, practical enforcement cooperation on current and pressing issues. To this end, in the first half of 2020, the IEWG facilitated two 'safe space' sessions, during which members spoke candidly about their key concerns, policy positions, and regulatory experiences in relation to specific global entities and issues.

These sessions - while valuable in and of themselves in supporting the exchange of knowledge and information on live issues - contributed to the development of two concrete enforcement cooperation initiatives:

- a joint investigation into Clearview AI between the Office of the Australian Information Commissioner and the UK Information Commissioner's Office; and

- an open letter with a joint statement on global privacy expectations of video teleconferencing companies, signed by six member Authorities of the IEWG.

Looking ahead, the IEWG co-chairs are leading a programme of work that will continue to strengthen the group's ability to facilitate live enforcement cooperation, while also: developing and enhancing tools to guide and support organisations in their collaboration initiatives; and exploring ways to better coordinate and leverage activities across the global landscape of Privacy Enforcement Authority (PEA) networks.

Introduction

Background

At the 41st Global Privacy Assembly (GPA) in Tirana in 2019 (then the International Conference of Data Protection and Privacy Commissioners), the GPA adopted its 2019 – 2021 Strategic Plan. Pillar 2 of the Plan's Policy Strategy covers enforcement cooperation. It set out an action to make the (then temporary) International Enforcement Cooperation Working Group (IEWG) a permanent working group of the Assembly. It further mandates the IEWG to refresh its objectives 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."

Establishment and membership

Following the closed session meeting in Tirana in 2019, the UK Information Commissioner's Office formed a Working Group Secretariat function, developing Terms of Reference and a Work Plan, and formally establishing the IEWG as a permanent working group with a diverse regional membership of 16 authorities including three co-chairs:

- Canada - Office of the Privacy Commissioner of Canada (co-chair)
- United Kingdom - Information Commissioner's Office (co-chair)
- United States of America - Federal Trade Commission (co-chair)

- Albania - Information and Data Protection Commissioner
- Argentina - Access to Public Information Agency Argentina
- Australia - Office of the Australian Information Commissioner
- Belgium - Belgian Data Protection Authority
- European Union - European Data Protection Supervisor
- Germany - Federal Commissioner for Data Protection and Freedom of Information
- Gibraltar - Gibraltar Regulatory Authority
- Hong Kong, China - Privacy Commissioner for Personal Data
- Netherlands - Dutch Data Protection Authority
- New Zealand - Office of the Privacy Commissioner
- Philippines - National Privacy Commission
- Switzerland - Swiss Federal Data Protection and Information Commissioner
- Turkey – Turkish Personal Data Protection Authority

Work Plan

The IEWG's Work Plan for 2019-2021 brings together commitments from the previous temporary Working Group's Resolution and Report – presented and adopted at the GPA's Annual Meeting in Tirana in 2019 – and the mandate given to the IEWG in the GPA's Policy Strategy. The Work Plan is divided into three Priorities setting out the broad areas of focus for the IEWG, each encompassing Objectives relevant to that area. The Priorities are summarised below:

- *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.
    - Objective 3 – Further identify legal impediments to enforcement cooperation.
- *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.
    - Objective 3 – Explore need for, and feasibility of, secured online platform.
    - Objective 4 – Explore need for, and development of, authorities database.
    - Objective 5 – Promote and review GCBECA.
- *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.

Initial prioritisation

Given the impact of the Covid-19 pandemic on many authorities' capacity and resources, and the primary mandate – from the GPA Policy Strategy – for the IEWG to refresh and review its objectives as an active group, the co-chairs of the new permanent IEWG sought to focus initial work on Priority 1 and, in particular, the rapid establishment of the group as a forum for practical enforcement cooperation on live issues.

As such, for the time up until the end of July 2020, the IEWG prioritised the development of its meetings as a safe space for candid, but confidential, discussion on concerns, experiences and strategies as regards organisations and privacy issues with global reach (see Working Group Activities). This successfully tested the IEWG's ability to fulfil its mandate in moving quickly, proactively, and collaboratively on current issues, and will support the group in maintaining its relevance as an active forum for enforcement cooperation as it builds momentum in progressing Objectives in the Work Plan (see Future looking plan 2020-2021).

Liaison with Strategic Direction Sub-Committee

The IEWG has regularly updated the SDSC on its establishment as a permanent Working Group, and the progression of its work, in written quarterly reports. In addition, the UK co-chair presented at the third meeting of the SDSC in June 2020, highlighting the importance of the IEWG's work in delivering Pillar 2 of the Policy Strategy, and setting out some initial activities and outputs showing good progress. The IEWG received positive feedback from the SDSC chair, recognising the group as an excellent example of the GPA engaging with current and pressing issues, and noting the importance and value of focusing on getting the right structure and frameworks in place to support this.

Working Group Activities

First meeting of the IEWG

The IEWG held its first meeting as a new permanent Working Group of the GPA in April 2020. The meeting was used to formally establish the Working Group, including acceptance of the Terms of Reference, agreement to the Work Plan, confirmation of membership, and appointment of co-chairs.

In addition, the group appointed three member Authorities as 'regional boosters': the Office of the Privacy Commissioner of Canada, the Turkish Personal Data Protection Authority, and the Privacy Commissioner for Personal Data Hong Kong, China. The co-chairs introduced the regional booster role to help increase the diversity of the group's membership. The role of each regional booster is to:

- promote, encourage, and support membership of the IEWG in their geographic region or linguistic networks; and
- amplify the views and contributions of members of their region or linguistic network to the rest of the group.

The IEWG looks forward to reporting back to the GPA in 2021 on the value of this role, and other measures, in bringing new members and perspectives into the enforcement cooperation community.

****Key output – Formal establishment of the IEWG as a permanent Working Group of the GPA****

Safe space session #1

Following the first meeting of the IEWG in April 2020, the group held its first safe space session.

The concept of the safe space is to allow IEWG members to speak candidly about best practices, strategies, and tactics in relation to key issues, themes, and the regulation of multinationals or organisations whose operations have significant global impact on people's data protection and privacy rights.

For the IEWG's first safe space session, members focused, in turn, on two organisations with global service offerings and novel or especially sensitive use of personal data. Members discussed key shared data protection and privacy concerns, respective experiences of engagement with the organisations, and opportunities for any further cooperation outside the session.

Discussion was fruitful and facilitated an excellent exchange of knowledge and information on the organisations and issues at hand. In addition, the session contributed to the development of a concrete cooperation initiative - a joint investigation on Clearview AI between the Office of the Australian Information Commissioner and the UK Information Commissioner's Office. This investigation is now live and focuses on Clearview AI's use of 'scraped' data and biometrics of individuals.

****Key output – Joint investigation into Clearview AI****

Safe space session #2

Acknowledging the work of the GPA Executive Committee in establishing the Assembly as a leading voice on the privacy regulatory community's response to the Covid-19 pandemic, the IEWG co-chairs recognised the importance of their role in considering how to support appropriate practical enforcement cooperation to help address data protection and privacy issues arising as a result of the crisis.

The IEWG co-chairs identified video teleconferencing (VTC) as a potential area of concern to explore, given the sharp uptake in use of VTC services during the pandemic and the new and exacerbated privacy risks this can raise. In May 2020, a sub-group of the IEWG held its second safe space session to discuss these issues and explore possible approaches to help address concerns collaboratively.

The safe space session supported productive discussion on the key issues, and valuable information sharing on research, policy and regulatory work already undertaken by individual GPA members. It led to the agreement of the topic as meriting collaboration between member authorities, and the identification of a coordinated compliance action as an appropriate, effective, and expedient model of enforcement cooperation to help address the issues at hand.

As a result, six member Authorities of the IEWG jointly drafted and signed an open letter to VTC companies (see Annexe):

- The Office of the Privacy Commissioner of Canada
- The UK Information Commissioner's Office
- The Office of the Australian Information Commissioner
- The Gibraltar Regulatory Authority
- The Privacy Commissioner for Personal Data, Hong Kong, China
- The Federal Data Protection and Information Commissioner of Switzerland

The open letter set out the concerns of the joint signatories, clarifying their expectations and steps that should be taken by VTC companies to mitigate privacy risks and safeguard people's personal information.

In July 2020 the letter was published on the signatory Authorities' websites. The letter was for all VTC companies, but was also sent directly to five VTC companies: Microsoft, Cisco, Zoom, House Party and Google. The companies were invited to respond to demonstrate the steps taken to comply with data protection and privacy requirements. The joint signatories will further engage with the VTC companies as appropriate, on receipt of their responses.

****Key output – open letter with joint statement on privacy expectations of VTC companies****

Forward looking plan 2020-2021

As set out above (see Working Group Activities), to date, the IEWG has made good progress on Priority 1 of its Work Plan (Foundations), in establishing the group's ability – through safe space sessions – to support and catalyse enforcement cooperation between its members.

Moving forward, the IEWG will build on this by substantively progressing other Priorities and Objectives in the Work Plan. The co-chairs remain sensitive to ongoing disruptions caused by the Covid-19 pandemic, and the breadth of the group's Work Plan, and have therefore prioritised the following items for progression between August 2020 and July 2021.

- *Priority 1 – Foundations* (in line with the mandate provided in Pillar 2 of the GPA Policy Strategy to become an active group considering live issues):
    - Objective 1 – Safe space framework

      Based on feedback and experience gained from the IEWG's initial safe space sessions, the group will develop a framework to formalise the approach to, and implementation of, the sessions with a view to more effectively supporting and promoting enforcement cooperation in practice, and capturing, evaluating and feeding back on outcomes achieved outside the sessions.

      Key output for Mexico GPA in 2021 – Completed framework
    - Objective 2 – Framework use and evaluation

      The IEWG will test the framework developed under Objective 1 in at least two safe space sessions, seeking feedback in order to evaluate its effectiveness.

      Key output for Mexico GPA in 2021 – Evaluation report
- *Priority 2 – Tools* (in line with the mandate provided by points 1 and 7 of the previous temporary IEWG's Resolution adopted at the GPA in Tirana in 2019):
    - Objective 1 – Enforcement Cooperation Handbook

      The IEWG will amend, update, and enhance the Enforcement Cooperation Handbook, including working with the Digital Citizen and Consumer Working Group on a new chapter covering cross-regulatory cooperation. Internal and external engagement (with privacy networks e.g. the Global Privacy Enforcement Network and Asia Pacific Privacy Authorities Forum, and other regulatory networks e.g. the International Consumer Protection and Enforcement Network and the International Competition Network) via a survey will elicit feedback on lessons learned, experiences of using the Handbook and other cooperation tools to inform the update.

      Key output for Mexico GPA in 2021 – Updated Enforcement Cooperation Handbook
    - Objective 2 – Enforcement cooperation repository

      The IEWG will continue to promote use of, and additions to, the Enforcement cooperation repository established by the previous temporary Working Group at the GPA in Tirana in 2019.

      Key output for Mexico GPA in 2021 – Update on additions to the repository

- *Priority 3 - Awareness and communication* (in line with the mandate provided in Pillar 2 of the GPA Policy Strategy to refresh the group's aims and objectives):
    - Objective 1 – PEA network analysis

      Through proactive engagement with other global PEA networks, the IEWG will conduct a mapping exercise to better understand each network's respective purpose, objectives, and work plans. The group will make recommendations on how to coordinate and leverage the respective activities of global PEA networks to amplify overall effectiveness, and socialise these with the networks.

      Key output for Mexico GPA in 2021 – Report on recommendations and feedback from networks

    - Objective 2 – Mutual observation agreements

      To support Objective 1, the IEWG will continue existing mutual observation agreements with other networks and setup new agreements as appropriate.

      Key output for Mexico GPA in 2021 – New mutual observation agreements as necessary

Conclusion

The IEWG plays an important role in pushing forward the GPA's agenda, helping to achieve its mission to provide international leadership on data protection and privacy, and support authorities to work together and more effectively perform their mandates. In particular, the IEWG has primary responsibility for advancing Pillar 2 of the GPA Policy Strategy focused on promoting and supporting practical enforcement cooperation.

To this end, the main focus for the co-chairs to date has been in forming the IEWG as a new permanent Working Group of the GPA and undertaking activities to establish the group as a forum within which members can proactively discuss live issues, leading to joint working on matters of mutual concern. The co-chairs are pleased that early efforts of the group in this area have contributed to concrete examples of enforcement cooperation in action. It is acknowledged however that this is only the start, and there is much work to be done to further bolster the group's ability to facilitate cooperation, both between its members and the wider privacy and cross-regulatory communities.

The co-chairs thank all members of the IEWG for their valuable input and contributions in helping to establish the new permanent working group, shape its work, and produce some excellent early practical outcomes. They look forward to continuing to work with members in progressing the group's work over the next year, and reporting back to the GPA Annual Meeting in Mexico in 2021.

Annex

Joint statement on global privacy expectations of Video Teleconferencing companies

Introduction

This is an open letter to companies providing Video Teleconferencing (VTC) services. We write to you as a subset of the global privacy regulatory community, with responsibility for protecting the privacy rights of citizens across the world.

Privacy concerns

Use of VTC to stay connected is not new. But as a result of the Covid-19 pandemic, we have seen a sharp increase in the use of VTC for both social and business purposes, including in the realm of virtual health and education, which can involve the sharing of particularly sensitive information, for particularly vulnerable groups. This increase in use exacerbates existing risks with the handling of personal information by VTC companies, and also creates new ones.

Reports in the media, and directly to us as privacy enforcement authorities, indicate the realisation of these risks in some cases. This has given us cause for concern as to whether the safeguards and measures put in place by VTC companies are keeping pace with the rapidly increasing risk profile of the personal information they process.

This letter

The purpose of this open letter is to set out our concerns, and to clarify our expectations and the steps you should be taking as VTC companies to mitigate the identified risks and ultimately ensure that our citizens' personal information is safeguarded in line with public expectations and protected from any harm.

Note that this is a non-exhaustive list of the data protection and privacy issues associated with VTC. It is intended to remind you of some of the key areas to consider given the increased use of your VTC services.

You should still regularly review your thinking on key privacy questions through privacy impact assessments. Where risks cannot be mitigated, we expect organisations to consult with their privacy regulator(s) to explain the specific risks identified and work through possible solutions on how these might be addressed.

Principles

1. **Security**

With personal information driving our digital economies, cyber-risks and threats to data-security are in a constant state of morphing and evolution. Today's security measures may soon become outdated and compromised by emerging threats. Data-security is a dynamic responsibility and vigilance by organizations is paramount.

During the current pandemic we have observed some worrying reports of security flaws in VTC products purportedly leading to unauthorised access to accounts, shared files, and calls.

In a world of global conversations, with personal information and private communications passing through many countries, we believe VTC providers should have certain security safeguards in place as standard, which would generally include: effective end-to-end encryption for all data communicated, two-factor authentication and strong passwords.

Such security measures should be given extra consideration by organisations who provide VTC services for sectors that routinely process sensitive information, such as hospitals providing remote medical consultations and online therapists, or where the VTC platform allows sharing of files and other media, in addition to the video/audio feed.

Your organisation should remain constantly aware of new security risks and threats to the VTC platform and be agile in your response to them. We would anticipate that you routinely require users of your platform to upgrade the version of the app they have installed, to ensure that they are up-to-date with the latest patches and security upgrades.

Particular attention should also be paid to ensuring that information is adequately protected when processed by third-parties, including in other countries.

2. Privacy-by-design and default

If data protection and privacy are merely afterthoughts in the design and user experience of a VTC platform, it increases the likelihood that you may fall short of the expectations of your users in upholding their rights. For instance, we have seen this manifest itself in well documented accounts of unexpected third-party intrusion to calls.

You should ensure that you take a privacy-by-design approach to your VTC service. This means making data protection and privacy integral to the services you provide to the customer. Always consider, as a starting point, the most sensitive information that could potentially be shared on your platform, and adopt the most privacy-friendly settings as default (similar to the **principle of least privilege** in cyber security). People who use your platform for less sensitive conversations or content sharing can adjust these settings to suit their requirements.

Simple measures to achieve this include:

- creating privacy conscious default settings that are prominent and easy to use, including implementing strong access controls as default, clearly announcing new callers, and setting their video / audio feeds as mute on entry;
- implementing features that allow business users to comply with their own privacy obligations, including features that enable them to seek other users' consent; and
- minimising personal information or data captured, used and disclosed by your product to only that necessary to provide the service.

VTC providers should also undertake a privacy impact assessment to identify the impact of their personal information handling practices on the privacy of individuals, and implement strategies to manage, minimise or eliminate, these risks.

3. Know your audience

During the Covid-19 pandemic, we have seen many examples of VTC platforms being deployed in contexts for which they were not originally designed. This can create new risks that you may not have anticipated prior to the current crisis.

Therefore, make sure that you review and determine the new and different environments and users of your VTC platform as a result of the pandemic. This is particularly important when it comes to children, vulnerable groups, and contexts where discussions on calls are likely to be especially sensitive (in education and healthcare for example), or when operating in jurisdictions where human rights and civil liberty issues might create additional risk to individuals engaging with the platform.

Consider what the data protection and privacy and requirements are for all contexts in which your platform is now in use, and implement appropriate measures and safeguards accordingly.

4. Transparency and fairness

As a result of several high-profile privacy breaches over recent years, there is heightened community awareness and expectations regarding how organisations handle personal information and use data in today's global digital economy. This is no different when it comes to VTC platforms. Failing to tell people how you use their information, and not considering whether what you are doing is expected and fair, may lead to a violation of the law and of the trust of your users.

You should be up-front about what information you collect, how you use it, who you share it with (including processors in other countries), and why – even if you do not consider the collection, use or sharing of that information to be particularly significant yourself, it is still important that its use is honestly communicated to the customer at all times. This is particularly the case when what you do with people's information is unlikely to be expected because it would not be seen as a core purpose of the VTC service. This information should be provided pro-actively, be easily accessible and not simply buried in a privacy policy. Where user consent regarding the handling of personal information is required, you should ensure that such consent is specific and informed.

Consider how any changes you make to future versions of the platform will affect all of the above. Assess their impact and consider whether it is important to make users aware of these changes. This will allow them to make informed decisions about how they use your platform moving forward.

5. End-user control

End-users may often have little choice about the use of a VTC service if a particular platform has been purchased, or is being exclusively utilised, in a given work-place, school or other setting. Some of the more novel features of VTC platforms may raise the risk of covert or unexpected monitoring.

While the companies and institutions using your VTC platform have their own data protection, privacy, and broader legal and ethical considerations in making decisions about the use of monitoring features, you should take your own steps to ensure that end-users of your service are empowered by having appropriate information and control.

For instance, if you offer a VTC platform that allows the host to collect location data, track the engagement or attention of participants, or record or create transcripts of calls, you should ensure that the use of these features is clearly indicated to those on the call when they are activated (through icons and pop-ups, for example). Where possible, you should also include a mechanism for end-users to choose not to share that information, for example via opt-out, noting that opt-in mechanisms might be more appropriate in certain instances.

Summary

We recognise that VTC companies offer a valuable service allowing us all to stay connected regardless of where we are in the world; something that is especially important in the midst of the current Covid-19 pandemic. But ease of staying in touch must not come at the expense of people's data protection and privacy rights.

The principles in this open letter set out some of the key areas to focus on to ensure that your VTC offering is not only compliant with data protection and privacy law around the world, but also helps build the trust and confidence of your userbase.

We welcome responses to this open letter from VTC companies, by 30 September 2020, to demonstrate how they are taking these principles into account in the design and delivery of their services. Responses will be shared amongst the joint signatories to this letter.

Elizabeth Hampton
Deputy Commissioner
Office of the Australian Information Commissioner
AUSTRALIA

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

Paul Canessa
Information Commissioner
Gibraltar Regulatory Authority
GIBRALTAR

Stephen Kai-yi Wong
Privacy Commissioner for Personal Data
HONG KONG, CHINA

Adrian Lobsiger
Federal Data Protection and Information Commissioner
SWITZERLAND

James Dipple-Johnstone
Deputy Commissioner
Regulatory Supervision
Information Commissioner's Office
UNITED KINGDOM