Observations following the joint statement on global privacy expectations of video teleconferencing companies

What we did

In July 2020, six data protection and privacy authorities from Australia, Canada, Gibraltar, Hong Kong SAR, China, Switzerland and the United Kingdom jointly signed an open letter to video teleconferencing (VTC) companies. The letter highlighted concerns about whether privacy safeguards were keeping pace with the rapid increase in use of VTC services during the global pandemic, and provided VTC companies with some guiding principles to address key privacy risks.

The joint signatories invited five of the biggest VTC companies to reply to the letter. Microsoft, Google, Cisco and Zoom responded, setting out how they take the principles into account in the design and development of their VTC services. Following a review of the responses, the joint signatories further engaged with these companies in a series of video calls, to better understand the steps they take to implement, monitor, and validate the privacy and security measures put in place.

The joint signatories also sent the open letter directly to Houseparty but did not receive a response. In December 2020, the joint signatories encouraged Houseparty to engage with them, including via a press release. To date, the group of joint signatories has not received contact from Houseparty. However, Houseparty has engaged directly with the UK Information Commissioner's Office as part of enquiries separate to those of the joint signatories and provided detailed responses to these enquiries. The UK Information Commissioner's Office recommended certain steps to Houseparty to improve compliance with the GDPR. However, in any event, in September of 2021, Houseparty announced that for business reasons it had already decided that it would cease offering its VTC service.

What we learned

Constructive engagement

This activity is an example of constructive engagement between the privacy regulatory community and the organisations we regulate.

It has allowed the joint signatories to engage, in a coordinated manner and with a uniform voice, with some of the largest and fastest growing technology companies, whose services are used worldwide. It has also given those companies the opportunity to explain their approach to data

protection and privacy through direct and practical interaction with a subset of the global privacy regulatory community representing citizens from jurisdictions across four continents.

The dialogue between VTC companies and data protection authorities has proven effective, efficient and mutually beneficial. Moving forward, the joint signatories highlight this model of engagement as valuable and replicable in circumstances where emerging issues would benefit from open dialogue to help set out regulatory expectations, clarify understanding, identify good practice, and foster public trust in innovative technologies.

Good practice

The joint signatories set out five principles in the open letter to help VTC companies identify and address some of the key privacy risks of their services.

In their responses and subsequent engagement with the joint signatories, Microsoft, Google, Cisco and Zoom highlighted, and in some cases demonstrated, measures, processes and safeguards they implement that take account of the principles and mitigate privacy risks.

The joint signatories recognised several areas of good practice in the approaches explained to our Offices by these companies. Some examples are summarised below under each of the five principles set out in our open letter. We do so to proactively and publicly communicate certain areas of good practice, and to recommend adoption of these measures, and others, across the broader VTC industry.

It is noted that such good practices will only be effective if faithfully implemented and observed. In addition, the areas of good practice set out below relate solely to what was reported to the joint signatories as part of this engagement exercise, noting that the joint signatories did not formally investigate the VTC platforms. They are without prejudice to any enquiries or investigations that each individual joint signatory may have undertaken separate to this joint engagement activity. They also do not reflect the privacy practices of Houseparty who did not take part in the engagement activity with the joint signatories.

Additionally, while Microsoft, Google, Cisco and Zoom described some features relating to the use of their VTC platforms in specific contexts, like for telehealth or distance education purposes, we did not examine nor discuss these aspects in detail. Therefore, our comments and observations relate to general public use of VTC platforms and do not generally address their use for the sharing of sensitive information.

1. **Security**

Testing – Regular testing of security measures is vital to ensure they remain robust against constantly evolving threats. Various approaches to security testing were reported, including: penetration tests; threat modelling; "bug bounty" programs; independent audits; internationally recognised certification; and use of open source code to enable third party scrutiny. The joint signatories recommend VTC companies take a comprehensive approach by overlaying several such measures into an overall and recurrent security testing approach.

Employees and third parties – It is important that employees and third-party sub-processors understand and comply with their obligations around access to, and handling of, personal information. Reported good practice examples of relevant measures included: pre-employment checks; regular employee training on privacy and security; vetting of third parties, including via vendor selection and review committees; regular audits of third parties, including logging sub-processor access to personal information; and a principle of least privilege approach to access controls where employee access is limited to that required for their job functions.

2. **Privacy-by-design and default**

Privacy programs – Data protection and privacy cannot be bolted on as an afterthought; for measures to work in practice they must be embedded. Detailed privacy programs were reported as in place or under development, incorporating various requirements in VTC services from concept to deployment, including: completion of privacy impact assessments for all new VTC features; regular contact between privacy, security and development teams; and adherence to the data minimisation principle. The joint signatories recommend that all VTC companies take a holistic approach to privacy by adopting an overarching privacy program or framework within their organisation.

Default settings – The joint signatories recommend that all VTCs place settings for their service at the most privacy protective by default. We saw examples of this in practice, such as: passwords required by default; virtual waiting rooms by default; privacy protective default settings consistent in browser and app versions of VTC services; and video and microphone off by default.

3. **Know your audience**

Enhanced features – Use of VTC services has sharply increased in contexts where discussions and shared information are particularly sensitive, in education and healthcare for example. VTC companies must ensure robust privacy and security safeguards to adequately protect personal data in these more sensitive environments. While this engagement did not fully explore the use of VTC platforms in such contexts, some good practice examples reported to the joint signatories included: teacher-controlled access to meetings; sole teacher control of screen sharing functions; and secure screen sharing of health documents.

Guidance – People and businesses are increasingly using VTC services for a wide range of purposes. Tailored privacy and security guidance for specific groups is a good practice to help ensure users are more confident using a VTC service and selecting the settings and features most appropriate for them. The joint signatories saw examples of custom-guidance such as: guidance and documentation for teachers and school administrators; guidance and advice for parents; blogs for users of popular laptop brands; and video tutorials for enterprise clients.

4. Transparency

Layered notices – Keeping people informed about how and why their information is collected and used is a key tenet of data protection and privacy regimes worldwide. Good examples of providing such information to users via a 'layered' approach were reported to the joint signatories, including: detailed privacy notices and dashboards delineating different categories of personal information collected; privacy check-up features; contextual notices in advance of video calls; pop-up written or audible notifications during calls, indicating instances of data collection through recording or transcripts.

Third parties – Increasingly, there is heightened awareness and concern amongst businesses and consumers about how personal information is shared with third parties and for what purposes. Users of VTC services must be clearly informed about who their information will be shared with and why[1]. Reported examples of good practice in this regard included: privacy notices detailing categories of personal information shared, the contractors with whom this is shared, and the reasons for them processing this information; 6-month notification periods prior to use of new third party processors; and publication of

[1] There may be further requirements in contexts, like telehealth or education, which involve the sharing of sensitive information.

transparency reports regarding law enforcement and government requests for access to data.

5. **End-user control**

Meeting controls – It is important that users be given intuitive and clear controls for their interaction with VTC services and that they are alerted to the information about them that is collected. The joint signatories saw some good examples of such controls in practice, including: ability to opt out of attendance or engagement reports; virtual and blurred backgrounds; user consent prior to host unmuting audio or activating video; and the ability to report a user for inappropriate conduct (or ejection by hosts).

Risk management – VTC users may unknowingly put the privacy and security of other meeting participants at risk by making meeting information publicly available, via social media posts for instance. Beyond educational material in guidance products, the joint signatories noted some innovative approaches to mitigating this risk, such as a tool to scan social media and alert meeting hosts of at-risk meetings, encouraging them to secure the meeting or schedule a new one.

Recommendations

As well as areas of good practice, the joint signatories identified opportunities to further enhance or improve some of the measures reported. These are set out below.

As with the areas of good practice set out above, the opportunities highlighted here relate solely to the learnings the joint signatories took from this engagement exercise. They do not reflect, and are without prejudice to, any separate enquiries or investigations that each individual joint signatory may have undertaken, or may undertake in future. They also do not relate to the privacy practices of Houseparty who were not part of the engagement activity with the joint signatories.

1. **Encryption**

The joint signatories acknowledge the reported use by the VTC companies of industry standard encryption as a minimum. They also welcome the development or implementation of end-to-end encryption (where the meeting host creates the key and only they and participants have access to it) in certain circumstances. They recognise certain limitations on functionality that this can pose, such as the inability for users to join by phone and the loss of

transcription, while also recognizing that such limitations may be beneficial in certain circumstances.

To further enhance VTC companies' approach to encryption, the joint signatories recommend the following:

- Making end-to-end encryption available to all users of VTC services whether enterprise, consumer, paid, or free; including via development and implementation of end-to-end encryption as an option in video calls involving multiple participants;

- the provision of clear and easily understandable information to users about the different levels of security and relevant limitations of 'standard' vs. end-to-end encryption;

- more clearly signposted meeting controls and information to allow meeting hosts and / or users to select their desired type of encryption, and so meeting participants can easily see the type of encryption in use in a meeting; and

- the use of end-to-end encryption by default in sensitive one-on-one settings, such as tele-health.

2. Secondary use of data

It is important that VTC services build trust with their users by only using information about them in ways that they would reasonably expect. The joint signatories recognise that many companies will only use personal information to provide the core features required to operate their VTC service, and will not retain it longer than necessary for that purpose.

However, where personal information is used for secondary purposes, VTC companies should explicitly make this clear to users with proactive, upfront, and easily understandable messaging about what information is used and for which purposes.

Where secondary purposes include targeted advertising and/or the use of tracking cookies, it is recommended that VTC companies only do this if users have expressly opted-in to such processing.

3. Data centres

The location where data is held and how it travels across borders and around the world are increasingly important considerations,

particularly for enterprise VTC customers looking to ensure appropriate levels of protection for personal information.

Some positive steps were reported in this regard, and the joint signatories recommend that all VTC companies:

- be fully transparent with users on the locations where data is stored and through which it is routed;
- where possible, give users the choice of which locations and jurisdictions their personal information is routed through and stored; and
- implement measures, contractual or others, to ensure that information is adequately protected when shared with third parties, including in foreign jurisdictions.

What's next

Most people have found VTC services very useful during the current global health crisis. For many, they have been a vital lifeline. Our dependence on, and general use of, VTC services is likely to continue through the pandemic and after we emerge from it.

High standards, robust measures, and best practices for privacy and security in the VTC industry are important for the safe deployment of these services and the ongoing trust of business and personal users.

The joint signatories therefore thank Microsoft, Google, Cisco and Zoom for their engagement and cooperation on this important matter.

The joint signatories will continue to make themselves available to all VTC companies for any further engagement to support the maintenance and development of their services in a privacy protective, safe and trustworthy manner.