

T R A N S C R I P T

LEGISLATIVE COUNCIL LEGAL AND SOCIAL ISSUES COMMITTEE

Inquiry into Anti-LGBTIQA+ Hate Crimes in Victoria

Melbourne – Thursday 25 June 2026

MEMBERS

Joe McCracken – Chair

Michael Galea – Deputy Chair

Ryan Batchelor

Anasina Gray-Barberio

Renee Heath

Ann-Marie Hermans

Rachel Payne

Lee Tarlamis

WITNESSES

Priyanka Purkayastha, Director, Trust and Safety, and

Joe Hack, Head, Global Government Affairs, Grindr.

The CHAIR: Good morning and welcome to the second day of the Legal and Social Issues Committee hearings into anti-LGBTIQA+ hate crimes. I am Joe McCracken, Chair of the inquiry. We will go through and introduce our committee members. I will go to those in the room first and then to those online. I am Joe, the Chair.

Aiv PUGLIELLI: Aiv Puglielli, North-Eastern Metropolitan.

Michael GALEA: Hello. Michael Galea, South-Eastern Metropolitan and Deputy Chair.

Ann-Marie HERMANS: I am Ann-Marie Hermans, Member for the South-Eastern Metropolitan Region.

Ryan BATCHELOR: Ryan Batchelor, Member for the Southern Metropolitan Region.

Anasina GRAY-BARBERIO: Morning. Anasina Gray-Barberio, Northern Metro.

The CHAIR: And we might have one or two joining us throughout, but they will come in as they do.

All evidence taken is protected by parliamentary privilege as provided by the *Constitution Act 1975* and further subject to the provisions of the Legislative Council standing orders. Therefore the information that you provide today during this hearing is protected by law. You are protected for anything you say during the hearings, but if you go elsewhere and repeat the same things, you may not necessarily be protected by that same privilege. Any false evidence or deliberate misleading of the committee can be considered a contempt of Parliament.

All evidence is being recorded. You will both be provided with a proof version of the transcript, but ultimately that will be made public, because it will be put on the committee's website.

Just for the Hansard record, are you both able to say your name, title and organisation? Thank you.

Joe HACK: Sure. Good morning. My name is Joe Hack. I am the Head of Global Government Affairs representing Grindr.

The CHAIR: Thank you.

Priyanka PURKAYASTHA: Good morning. I am Priyanka Purkayastha. I am the Director of Trust and Safety at Grindr.

The CHAIR: Perfect. Thanks very much. I will hand over to you guys now. I will put 5 or 6 minutes on the clock, but if you hear a little beep, do not worry about it; just keep going, okay. It is more for me to manage the time on our end. Thanks very much for coming along and welcome. I will hand it over to you.

Joe HACK: Great. Thank you. Good morning, and thank you, Mr Chairman and members of the committee, for the invitation to join you all today. As I said, my name is Joe Hack. I am the Head of Global Government Affairs for Grindr. And with me today is Priyanka, our Director of trust and safety. We appreciate this opportunity to appear before the committee. I want to say at the outset very clearly that we take what is happening to members of the LGBTIQA+ community, our community, in Victoria and more broadly in Australia with the utmost seriousness and we share your goals to fight the awful crimes that are occurring.

Grindr exists because gay, bisexual, transgender and queer people need a place to find each other safely and on their own terms. At Grindr we have no higher priority than the safety and wellbeing of our users, and we have implemented a range of measures and new tools designed to help protect members of our online community. Like any online platform, there are instances where bad actors attempt to misuse our features, potentially putting users at risk. Grindr is for adults only, and Australian users are required to verify they are over 18 to create and use a Grindr account. We regularly update our features and practices to help reduce the risk of harassment, violence and exploitation. Grindr has invested heavily in safety improvements, and we continue to

refine our systems based on what we learn. We humbly acknowledge our work is never done, and we remain focused on continuous safety, innovation and user education.

Recent anti-LGBTQ attacks, including over the last year, are deeply disturbing to us. Perpetrators using our platform to identify, target and harm the very community we exist to serve represents a direct assault on everything we stand for. We have been actively working with Australian law enforcement, including recent outreach to local departments and detectives investigating these attacks, and we will continue to do so. Determined attackers, however, will always look for ways to misuse online platforms. That is precisely why we do not limit ourselves to reactive cooperation. We are continuously investing in better tools, better detection and deeper community partnerships to better identify and respond to abuse.

We are here today not just to answer your questions but also to listen and to contribute to a stronger collective response, the purpose of this series of hearings you all are holding. Specifically, we would like to highlight a few things that we have already done and are continuing to develop. We have deployed in-app safety pop-up messages in Victoria and the ACT in 2025 in partnership with the local LGBTQIA+ organisations, including Meridian, warning users of violence risks and providing safety guidance. An updated campaign is currently in the app. We have proactively reached out to law enforcement in Australia to better understand the patterns of off-platform harm they are observing so we can improve our own detection capabilities. We cooperate with Australian police investigations through a system called Kodex, our dedicated law enforcement portal. To date we have worked with Australian police to respond to 58 cases in 2025 and 69 cases in 2026. We are also a founding signatory to the Australian Online Dating Code of Conduct. In April 2026 we presented publicly on the topic of anti-LGBTQIA+ hate crimes in Australia during an e-safety industry forum.

Finally, I would like to highlight that Grindr's commitments in Australia go beyond online safety. Over the past two years Grindr for Equality, our global social impact initiative, has built a deep and active public health presence in Australia by partnering with leading LGBTQIA+ health organisations, including NAPWHA, ACON Health, Thorne Harbour and the national education platform Emen8 to reach users with timely localised health information where it matters most. Through 60-plus in-app campaigns spanning HIV self-testing, STI prevention, PrEP access, mpox response and community safety, Grindr has functioned as a trusted channel between users and the public health system, distributing over 6500 free HIV self-test kits nationwide and responding in real time to emerging health and safety concerns. We look forward to a constructive conversation with the committee today, and we welcome the opportunity to answer your questions.

The CHAIR: Thanks very much. I will go first and then we will go through the committee members, and I will just note Sheena. Welcome to you, too, this morning. Sheena is another committee member. Welcome to you, Sheena.

Sheena WATT: Thank you, Chair.

The CHAIR: I will go first. I will go to you, Joe. You mentioned that you had been working with local authorities here in Victoria. Victoria Police have identified that Grindr is the main app that is used to facilitate these horrible instances that we are hearing about. What work have you done with Victoria Police that has really helped make a positive change in the space that we are talking about?

Joe HACK: I would say that overall we believe our relationship with Victoria Police has been a positive one. I think we have both had to learn how to better enable cooperation. One of the things we encountered initially from some of the inquiries we received was really a lack of detail in connection with either record requests or other inquiries that we were receiving. For example, sometimes we would only receive a display name from the police in regard to a profile, and that can make it difficult to identify the account in question. And so we have shared that with them and have found the police to be collaborative when we have requested additional information to try and locate accounts. We obviously welcome the opportunity to continue working with them as they identify new patterns or emerging risks.

The CHAIR: I noticed as well you said that you have had outreach with other local authorities. What have they entailed?

Joe HACK: We have had both an active and a responsive relationship with law enforcement in Australia. Since 2025 we have received and responded to 126 requests across Australia, 40 of which came from Victoria. In addition to responding to those requests, I think what you are getting at is the proactive outreach. We have

reached out directly to a local department in New South Wales that was investigating app-facilitated attacks on gay and bisexual men to better understand, again, the harm patterns that were occurring off platform, with the goal of refining our own detections. There was also a situation in Sydney that involved a terrorist attack, where we were very actively engaged with law enforcement in real time working to mitigate that situation. I think we have found Australia's law enforcement to be cooperative and to be, I think, fairly straightforward and good working partners for us. But Priyanka, if you have anything to add on that, please feel free.

Priyanka PURKAYASTHA: Thanks, Joe. To add to that, we have been working with ACON, Meridian and Thorne Harbour in understanding what those on-ground trends look like and have used those in framing our reactive messaging and safety messaging, which are more timely, especially if there is a sudden increase in targeted attacks towards the LGBTQIA community. Based on those insights, to your earlier question on how it has improved our process, we have actually also started having more proactive messaging, not just reactive, but we have always-on messages that warn users about in-person safety challenges.

Our help centre resources are also quite extensive – and it comes to meeting tips, a holistic security guide. But we do understand that not everyone is searching for help centre guidance before going on a date, so we try to make it as much in-app messaging as possible, and some of these in-app messages connect to the local resources. As well, sometimes it connects to, say, the Queensland police or New South Wales police if they are working with the police directly, or at other times it connects to documents or resources that ACON or Meridian are sharing.

The CHAIR: Whatever is relevant. Yes. I have only got about a minute left, but on a broader question: what do you see as your obligation to users of your app in order to create a safe experience for them? I guess, firstly, what do you see as your obligations and how do you go about fulfilling them? Does that make sense?

Joe HACK: Yes, sir, it does make sense. I would say that creating a safe environment for members of our community to form connections is of the utmost importance to us. How we fulfil that responsibility, I think, is through a few ways. One is investing heavily in trust and safety, which we do, and working to do more by providing users with tools that they can use, which we are happy to discuss further in additional questions – some of the tools that we do provide our users – to create and ensure safe experiences, but also through education. That comes through some of the messaging that Priyanka mentioned but also through partnerships with local organisations in the community to try and highlight some of the crimes that are occurring and some of the tactics that are occurring and how users can connect in ways that are safe.

The CHAIR: Yes. Thank you for that. My time has expired, and I am going to hand over to Mr Galea.

Michael GALEA: Thank you, Chair. Thank you very much for joining us, Joe and Priyanka. I say as well, it is a credit to you for leaning in and engaging with our inquiry; it is greatly appreciated. I also will note that whilst the media labels for these attacks have been based around your app, it is certainly not the case that it is only through Grindr, and I will just make that note at the head of our conversation. I would like to ask you about the Kodex system, which you said was the way you deal with local law enforcement – and if I am correct, 58 cases in 2025 and 68 this year so far. That is quite a jump on last year, and we are only halfway through the year. Should we read that as an uptick in incidents, or is that more a reflection of local police becoming more and more engaged in the service?

Joe HACK: Priyanka, do you want to answer that one?

Priyanka PURKAYASTHA: Yes, absolutely. I think it is a mix of both. One, there is of course a lot more activity from local police, which is helping get these cases to the surface. But also we are encouraging users to report. A lot of our safety messages are encouraging users to report. We have made our reporting flows also very prominently displayed in every surface of the app, so that it makes it easier for users to highlight that. So even though we understand that under-reporting is a concern, and that will continue to be there, I think – that is a broader conversation beyond app and beyond Grindr specifically about how we can help the LGBTQ community feel safer to come through and complain – we do see that there might be more activity because of some of these proactive measures. It is hard to measure those, obviously, but since we have been doing this since last year, I can imagine that can have some positive impact on people reaching out or feeling comfortable to reach out.

Michael GALEA: Sure. Would you be happy to provide to the committee on notice the stats for the exact number of reports by each Australian jurisdiction over the past two years through this service, just to give us a bit of a broader visual picture?

Priyanka PURKAYASTHA: Yes.

Joe HACK: Yes, we would be happy to check on that and see if we are able to provide that for you.

Michael GALEA: Thank you very much. Given that you are a global app, one of the things that we have heard from stakeholders is that when there are spikes in Victoria or Australia, it is often mirrored with spikes around other jurisdictions around the world as well. Is that something that you see?

Joe HACK: Yes. I am happy to visit with you a little bit about that. Actually, one of the first experiences I had when I took this role was working in partnership in response to an uptick that occurred in Paris. It was anti-LGBTQ-specific violence that was occurring, and so we had outreach from law enforcement. The specific concern related to our previous conversation related to under-reporting, and what happened I thought was quite productive. It started as an informal conversation with industry, community partners and law enforcement that was convened by the French government, and that led to a charter of online safety commitments, which we are a signatory of along with some other peer companies, to encourage individuals to come forward and engage with law enforcement. I suspect many of you are aware of the history of law enforcement and our community and some of the troubles there and the need to establish and foster greater trust. I think that is something that collectively we all need to work towards. But in France, specifically, yes, there was a spike. Similar to what we have seen here, we were able to come together, and we are in the process of working through that charter now.

Michael GALEA: Thank you. And that is a recurring pattern that you still see to this day, is it, that when there is a spike in one part of the world, it does not usually occur in a vacuum?

Joe HACK: In my experience, no. Priyanka, I do not know if you have anything to add on it.

Priyanka PURKAYASTHA: I think the only thing I will add is that it is not like it happens all in the same wave. It often shifts the waves around. Let us say, if Australia is having a flurry of attacks, it does not mean that the UK will also and that when the UK does Australia will too. It kind of shifts around. Grindr is present in 190 countries, and we do see different degrees of targeted abuse and targeted harm for the community in different parts of the world. There is sometimes a seasonal rise, especially with AI use, in certain cases, especially if there are TikTok trends and if there are certain kinds of viral issues that are going through it. But other than that, I would say there is a baseline understanding of this as an issue that affects our community at large across the globe.

Michael GALEA: So you are seeing, if I can just pick on one example there, a direct correlation between a trend on TikTok inciting abuse against the LGBTIQ+ community and attacks facilitated through apps like yours?

Priyanka PURKAYASTHA: Yes. It may not be a severe attack that results in in-person harm all the time, but we see the uptick in, say, reports on harassment, bullying and hate speech and other kinds of attacks, which are not always as severe as offline harm but have online harm as well.

Michael GALEA: That exist in that same ecosystem, yes. Thank you very much.

The CHAIR: Thank you. I will now hand over to Mr Puglielli.

Aiv PUGLIELLI: Thank you, Chair. Good morning. Thank you for joining us for this inquiry process. Some witnesses thus far have suggested things like verifying user identities in the creation of accounts on Grindr. Is this something that Grindr has considered in the past?

Joe HACK: This is a topic we are happy to visit with you. The question of verification is a bit of a complicated one, and we would love to walk you through our thought process on it. First of all, as an 18-plus app, we are in compliance with Australia's age assurance policy, which is of course an initial step of verification when it comes to age which verifies both liveness and the age of the individual. As we move forward, there are other forms of verification that we do deploy within the app, and I will let Priyanka speak to

the specific tools that exist from a product perspective that we leverage but also some tools that we enable users to have at their disposal.

But I do think it is worth taking a moment to talk a little bit about our philosophy here. We want to create a safe space for people to come together online. At the same time we do have a core value as a privacy-forward community where people can come without having to disclose their identity. Grindr is often a place where individuals who are over the age of 18 first come to explore their sexuality. It is also a place where people who are uncomfortable with their sexuality come to make connections and find community who otherwise would have extreme loneliness. We think it is important to ensure that that space continues to exist for people who are not comfortable disclosing who they are. As previously noted, we are in 190 different countries; in 60 of those countries it is illegal to be a homosexual. And for many people Grindr is a lifeline with access to sexual health information and community that would not otherwise exist. That broadly frames how we think about things. Priyanka, I would love for you to share a little bit more in detail about the tools we think about.

Priyanka PURKAYASTHA: Thanks, Joe. While we are not traditionally looking into that verification for every user, there are many ways we are addressing this problem. We use a mix of technical controls and user-facing signals, as Joe mentioned. One very effective way is using our partners like Twilio for bot prevention, including blocking burner phone fraud and adding device authentication through SMS verification. These happen during the account creation and registration stage, so even before the harm reaches the other users on the app. A similar partner we use called Sift Science helps us distinguish between a bot and human behaviour and also identify known scam and known IP signals that are associated with scam signals or spam signals. These also shift, by the way. It is not a static list. It kind of shifts with the trend and what AI is bringing to the fore. These partners that we have – Twilio and Sift Science – are using world-class technology to stay ahead of that curve and ensure that we are catching some of these harms, even before they are creating accounts.

On the product side, features like ‘Taken on Grindr’, which adds a watermark to photos that are captured within the app, help confirm authenticity and build trust. It is used for users who can show that they are truly who they say they are and can be used during conversations and before meet-ups. On that note, before meet-ups we also encourage users to use video calls before meeting in person. That is something we mention in our safety messages as well as a prompt. At the same time, for LGBTQ+ users privacy and discretion are actually important safety features. Giving our users the agency to control how they show location and if they are comfortable showing their face or not are also ways of protecting them. The challenge for us is designing tools that increase their confidence and reduce misuse, but without forcing users into identity exposure.

Aiv PUGLIELLI: Thank you. I can appreciate what you are saying. I think the difficult thing we are having to navigate is we have platforms where anonymity is a core part of how the space is used, but we are seeing facilitation of attacks on members of the community through that anonymity and through the platforms as they currently exist. Can I ask, and you are welcome to come back to us on notice if this is more useful: what information is currently being kept about users and accounts that are being created?

Joe HACK: Priyanka, would you like to handle that one in terms of the data storage?

Priyanka PURKAYASTHA: Yes. We use automated and human-reviewed safety systems to detect policy-violating behaviour, consistent with applicable law and privacy commitments. Through the time the accounts are active on the app, we get to look at all their actions and all their interactions on the app. When the account is deleted, we keep information in accordance with privacy laws and have that available for law enforcement requests, but we also do give users the option to choose to delete their information completely through that. Overall, the anonymity aspect of it is more for ensuring that users have the comfortable space to show up how they want to show up. But at the end, in our back-end systems, we still have systems and checks in place – the things that I mentioned around, say, Twilio and Sift. They are looking into IPs, phone numbers, emails, the overall action of the account, or the email ID and phone numbers across the internet – using that intelligence to help us inform and keep the platform safe.

Aiv PUGLIELLI: Thank you. Thank you, Chair.

The CHAIR: Thank you. I will now go to our members online. Just so those online know the order, I will go to Ann-Marie first, then Ryan, then Anasina and then Sheena. So Ann-Marie, over to you first.

Ann-Marie HERMANS: Thank you. Thank you so much for coming in to answer these questions for us. As you know, your app – I would not say it is centre stage, but it has certainly been a big part of this inquiry – has been referenced. Either your app or an app like your app has been part of one of the personal testimonies and accounts of a victim that was a victim of violence. So my question is: in that particular incident clearly the users that met with this gentleman were under-age. In one report earlier in the morning it was indicated that there was meant to be a 13-year-old, and another report from the actual person who was the victim said he thought that they were teenagers – maybe around 16. Now, that bothers me, because that means that this app has been used and teenagers are involved in this situation. What are you doing to be able to protect our vulnerable youth from being able to use an app that is available and is set up for adults?

Joe HACK: Thank you for the question. It is a very important topic, and it is one we take very seriously as an 18-plus app. As I said earlier, we are in compliance with the Australia age assurance policy. That requires us to be sure that we are not allowing anyone under-age onto the platform. I am going to let Priyanka walk you through what that compliance looks like so you have a clear understanding of it. But in addition to that gatekeeping function, though it presents challenges to us, one of the benefits of AI from a safety perspective is also the development of tools to detect behaviour, including in patterns of speech or conversation or photo scanning that allows us to detect if someone is under-age, so that we have become much better at being able to do that. In other words –

Ann-Marie HERMANS: I am sorry to interrupt you, because I get a very short time. Based on what you are saying, though, if you detect that, do you go out of your way to detect it? And if you do, what do you do? Because clearly whatever you do has not worked in this instance.

Joe HACK: I am not sure of the timing of the case you are referencing, but I can tell you that we have implemented the age assurance policy – as of I believe December of last year that has been in place – and our auto detection tools have really over the past year or so come into greater usage. Priyanka, I think it would be helpful if maybe you could please describe what the gatekeeping function looks like and then what tools we have now that enable us to detect.

Priyanka PURKAYASTHA: Yes, absolutely.

Ann-Marie HERMANS: And how you use that. Just detecting is one thing, but what do you do with the detection?

Joe HACK: We are happy to respond, yes.

Priyanka PURKAYASTHA: Thank you, Ann-Marie. To share more context on that, I am not sure of the exact incident date, but if it was before December 2025 it is possible that it was not part of our age assurance checks then. The age assurance check significantly has ensured that the number of under-age reports we see on the platforms have reduced. We have seen that happen, so it is working. Like any other system, it is not perfect. There are I am sure ways kids are finding to evade systems as well, and that is when it comes to other systems that we have. We use FaceTec as the facial age estimation during the check, but if there is by chance somebody who can evade the system and can be on the app and is under-age, we have proactive detection tools which, if they are detecting any under-age activity, ban the account but also ban the device, which ensures that the user cannot create any new account from that device. In the case of under-age users especially, we look further into any connected device. In that same device, if there are any connected profiles, we look into those devices as well for any under-age activity. So we go through layers of investigation when it comes to under-age activity, and the device ban as a tool has been very effective in preventing recidivism, as we call it, which is repeat offenders, ensuring that the same user just cannot create another account and come back immediately. So that is one of the helpful tools. Another aspect I will call out is the AI part that Joe mentioned. We are constantly –

Ann-Marie HERMANS: Sorry, can I –

The CHAIR: Ann-Marie, your time is up, but I will just let you finish this part, okay?

Ann-Marie HERMANS: Just because it actually froze. Did it freeze up on your end at all? No. You all heard everything that was said.

The CHAIR: No. We all heard everything, yes.

Ann-Marie HERMANS: Okay. I missed out on some of the answers to that, that is all. I would not mind, if it is possible, to be sent something in writing, if you do not mind, on what you are doing to protect young people and how you go about it. Once you find that this is an under-age person, what do you do, and how many cases, at least in Victoria, have you already uncovered, and what have you done about it? If that is possible, just because it froze and I could not hear your responses. I am so sorry.

Priyanka PURKAYASTHA: I am so sorry about that. Go ahead, Joe.

Joe HACK: I was just going to say we would be happy to provide for you in writing just an explanation of what our tools are, what our policies are, how they work and, as you mentioned, if there have been any recent cases in Victoria.

Ann-Marie HERMANS: And what you have done about it. Thank you.

The CHAIR: That is great. Thank you very much. Mr Batchelor, over to you.

Ryan BATCHELOR: Thanks very much, Chair. Joe, Priyanka, I really appreciate you taking the time. This is a complex technical side of these issues that we have got to get our heads around. I just want to spend a bit of time better understanding how your back end on the app deals with problematic accounts. You mentioned earlier you have got systems in place to try and detect bots and spam accounts and remove them from the platform. From the evidence that we have had so far it appears to us that the issues are not by bots or spam accounts but malicious actors undertaking impersonation – [Zoom dropout]

The CHAIR: I think Ryan might have frozen. We might come back to Ryan when those technical issues are sorted. Anasina, I might throw to you, if that is okay, and then when Ryan comes back in I might put him next on the list. Apologies about that, but we will hand over to you, Anasina.

Anasina GRAY-BARBERIO: No worries. Thank you so much for your presentation and your testimony this morning. We really appreciate it. This is our second day of the inquiry. Yesterday we heard from a lot of witnesses who have called for a digital duty of care for platforms. Is this something that Grindr would support, these types of policies being made mandatory rather than just voluntary?

Joe HACK: My understanding as far as a digital duty of care goes is that it is about ensuring that platforms take measures and implement tools to keep their users safe. We believe that through our trust and safety initiative that Priyanka helps lead we have implemented a number of tools to do so. As for a broader policy, I think it is just important to think through how it applies differently to different types of platforms, different types of apps and different types of websites that have different types of communities. As we shared earlier, we sit in an interesting space in the community we represent and in the online space we try and foster, and we agree that greater safety is always the goal. We are happy to work constructively with policymakers and regulators as they think through this. I know that there is a lot of activity in this space right now, and I think we would welcome the chance to weigh in on any rules to ensure that they are consistent, they are predictable and they are workable for companies like us. Because we have such a well-known brand I think a lot of people think we are a massive company. We are not Meta. We are not Google. In terms of sorting through how you implement things like this, I would just think a nuanced approach is often the right way.

Anasina GRAY-BARBERIO: Thank you. The example I want to use is Equality Australia, who came before us yesterday and were calling for the ability to develop binding or authoritative practice guidelines particularly tailored to relevant settings in relation to social media platforms complying with and clarifying the duty that is required in practice. Is this something that Grindr supports?

Joe HACK: I would need to learn more before I could comment on that. I am sorry, I am just not terribly familiar with that particular position.

Anasina GRAY-BARBERIO: No worries. Is that something you could take on notice after you have had time to explore that?

Joe HACK: Yes, we would be happy to look at it. I do not know if any members of your team would be able to share more information about that with us. We would be happy to review it.

Anasina GRAY-BARBERIO: Thank you. I will move on. You have spoken in your presentation about app features like watermarking of photos to show that they were taken in-app. Would you be prepared to make features like that mandatory to form part of the platform's model?

Joe HACK: I think a big way we approach things, as Priyanka articulated earlier, is giving users the opportunity to exercise control and determine the types of connections and relationships that they are interested in exploring. I do not know that we would support making it mandatory. I think we want users to be able to determine what they are comfortable using and doing so.

Anasina GRAY-BARBERIO: Thank you. Priyanka, you spoke about AI before. What implications has AI had on the use of your platform, in your understanding and awareness?

Priyanka PURKAYASTHA: The big one, I would say, is the proliferation of harm, because AI has now led to making things happen in seconds that can scale faster. For example, one account can run a script that sends harassing messages to many people in their entire inbox at the same time. And there are these novel technology use cases that we are seeing, or even, say, the NCI – non-consensual intimate – images, the use of AI in doctoring images. It is interesting, because sometimes it is also done with consent; people can use filters and can edit photos, so where do you draw the line between impersonation and inauthentic use of AI versus regular, authentic use of AI? These are the kinds of challenges that we are seeing on our platform right now with AI.

Anasina GRAY-BARBERIO: Thank you. Now, you –

The CHAIR: Sorry, Anasina. That is time, I am afraid. So sorry.

Anasina GRAY-BARBERIO: Okay. Thank you both. No worries. Thanks, Chair.

The CHAIR: I will now go back to Mr Batchelor. I believe Ryan is back online. Over to you, Ryan. I will give you your full 5 minutes again, so go for it.

Ryan BATCHELOR: Thank you. Where I was getting to was you have got some mechanisms to detect bots and spam accounts. These are not bots and spam accounts; they look like they are malicious actors who are doing impersonation, using whatever mechanisms to lure people in. Do you have a reporting mechanism within the app for users to report suspicious behaviour? How does that work? And do you have a reporting mechanism in the app for users to report instances where they have been the subject of an assault or similar harm? And then what do you do with that information?

Joe HACK: Yes, we have a pretty sophisticated reporting system. Priyanka, if you could describe it, that would be wonderful.

Priyanka PURKAYASTHA: Yes. We use structured reporting flows with drop-downs to help route and prioritise reports. A user can select different types of issues, and according to the type they are selecting it gets routed to priority queues. So, for example, 'underage' is one of the topmost priority queues, and that will always be looked at first. Similarly, we have a separate, specific channel dedicated to serious in-person incidents. If you select the option of 'serious in-person incident' through the drop-down form, a reporting flow, it will take you to a form that then brings the case to one of our most trained and most capable escalation specialists, who can handle it with immediate attention and can reach out to law enforcement or reach out to our internal teams when needed to fix anything. That process is something that I would say is how we are handling both the aspect of reporting suspicious behaviour angles at scale but also trying to create space for people reporting in-person, immediate harm. The in-person reporting channel bypasses the automation and any kind of regular moderation queues and directly jumps into sophisticated escalation handling, whereas there are suspicious behaviours that might come in with less evidence and others might be more prioritised for the queue and automation process.

I do want to call out that we do see malicious users misusing the reporting flow, and that is something we are thinking of how to deal with. For example, they go ahead and flag good users. Malicious users keep falsely flagging good users, because it inundates our systems and it is easier for them to get that one bad account through. We do see interesting tactics like that by malicious actors as well that we are dealing with.

Ryan BATCHELOR: Do you have any relationships with law enforcement, either in Victoria or around the world, to receive reports from them about instances that you can provide access to your back end to try and track down alleged perpetrators? You mentioned earlier there is sort of IP checking and you can try and find devices that are repeatedly creating multiple accounts to shut them down for the future. Describe to me how the company handles those circumstances.

Priyanka PURKAYASTHA: Yes, we do. The law enforcement process is called Kodex, and through Kodex, once we get a request from law enforcement through that Kodex process, we initiate a deeper investigation with that and share as much information as we can to support that investigation. In some exceptional circumstances, we have even gone further. In one instance involving a terrorist threat in Sydney, Grindr joined live calls with law enforcement to respond to questions in real time and assist in the case resolution. This kind of direct, immediate engagement reflects that we are ready to be supportive and be there as a strong partner. In some cases we have also reached out directly to local departments, like in New South Wales, investigating some app-facilitated attacks on gay and bisexual men, and we reached out to better understand the off-platform harm patterns they are observing in New South Wales and how we can improve our internal detections based on those insights.

Ryan BATCHELOR: Are your detection systems internally learning and adapting from the changed patterns of behaviour?

Priyanka PURKAYASTHA: Yes, absolutely. It is an ongoing, constant update. For example, for underage users or any kind of malicious users, they are constantly updating their playbook, which we also have to do. I used to refer to saying that this game used to be a whack-a-mole game, and now it has become chess. So we all are playing chess with a lot more sophisticated, malicious actors.

Ryan BATCHELOR: Are there any regulatory issues that you encounter that make it difficult for you to undertake that sort of work? Are there things that you would like to be able to do to improve your own internal systems and processes and quality assurance that you feel you cannot do because there are regulatory barriers, or is it more user interface and technology-based sorts of limitations on what you are able to do?

Joe HACK: I think in my view – go ahead, Priyanka.

Priyanka PURKAYASTHA: I was referring to more privacy laws and following through those across, rather than regulation around. It does not only happen to be safety regulations but more broadly thinking of online platform regulations across the globe, because we are, as Joe mentioned, a small company supporting a really global app. So we do try to have that global approach as well. There are those limitations there, but they are not something that I would say is severely blocking us from keeping the platform safe. Go ahead, Joe.

Joe HACK: I was just going to say I think one of our greatest threats, as Priyanka articulated, was just malicious actors leveraging AI and their ability to sort of scale attacks, whether those attacks are through spam or other things that sort of disrupt the community and the ecosystem. It is not just creating a messy user experience. What happens then is it really creates an uptick in reporting that then has to be sorted through and processed. So it creates resource challenges that we have had to overcome to really stay on top of things. The scale at which threats and problems are rising is quite significant, and I think it is something to be taken into account as you are contemplating this. Frankly, I would commend the committee on the holistic view I think you are taking on the problem. Obviously, platforms like ours are abused in ways that are unfortunate, but as we know, there are a lot of different aspects of the problem, whether they are societal or regulatory or other factors that need to be considered. I think the way this inquiry has been conducted has been very holistic.

Ryan BATCHELOR: That is all from me, Chair. Thanks.

The CHAIR: Thank you. I will just double-check to see if Sheena is online, but I think she might have dropped off. We have got a few more minutes left, so I might ask some of the people in the room. I know there are some extra questions, so I might go to Mr Galea first, and then I will go to Mr Puglielli for some additional questions, and then we will wrap up.

Michael GALEA: Thank you. Chair. If I can just ask a bit of a nuts and bolts question, if I was a user of the app and I have experienced one of these assaults, having met up with someone, how do I specifically – aside from, as we have obviously talked about, the holistic approach going through law enforcement here – if I was

to make a report through the app, how would I do that? What sorts of supports could I expect to receive? If the users deleted their profile, is there any way I can report it? What would the steps be, and what would someone who is in that situation expect to be able to receive in terms of support from Grindr?

Joe HACK: Priyanka, do you want to walk through that process?

Priyanka PURKAYASTHA: Yes, please. So for starters you can reach out to us through the app but also through a contact form that is available on the help centre. A Google search will show up our help centre contact form, which also has different reasons one can select. And again, there is an option of selecting 'I'm at risk of an in-person safety incident', which will then again bring it to the priority queue.

Within the app, generally a lot of apps we see have reporting flows more hidden in settings or in one particular corner of the app, but for us it is present in literally every surface of the Grindr app, whether that is on the grid or it is your DMs, albums or profiles. Right now every single platform has an easy option to do it through. We ensure that reporting flow is not the only action we are giving users. We also have an option to block or hide, and that is a helpful option as well.

To your specific question on when a user is deleting information, we have usually found if they have any screenshots saved of their conversations, or anything that can help us identify those accounts and the perpetrators, that will be very helpful. I mentioned earlier that we do not have deleted information for an indefinite amount of time, but within the first seven to I think 28 days, if I am not mistaken, we will be able to find details, especially when it comes to serious law enforcement issues. We can go ahead and put in that search with our security team and look into the deeper databases to find that information even if the account is deleted.

Michael GALEA: Thank you. And if the attacker has deleted the app and you have not taken screenshots, for example, would the data that you keep be able to work it out from – for example, if I was to make a report, would you be able to see from all the accounts I have interacted with which ones have been deleted, and would you then be able to use that channel to identify the user, even if they have deleted it and there are no records that the user has on their device?

Priyanka PURKAYASTHA: Yes, we would be, in our internal back-end systems, able to see the conversations they have had. It is to be taken with a little bit of a pinch of salt, though, because oftentimes these are not sure-shot easy answers to get through because we are relying on a cloud database. So there are sometimes missing gaps in information, but especially if we are aware as soon as possible, then we can act quickly.

Michael GALEA: Would you generally advise users in these situations to make reports through both, in our case, Victoria Police and through Grindr directly, or is there a pathway that you would particularly seek to recommend?

Priyanka PURKAYASTHA: A pathway through law enforcement is better when it comes to looking for this deleted information or information that more pertains to the other user, because we do not share that information, for privacy reasons, with anyone else. So that is where law enforcement approaches are good, but to inform Grindr about any incident that has happened either path works. In-app reporting – these channels are also prioritised and we look at them with priority.

Michael GALEA: Those protocols, the Kodex protocols, will work easier through law enforcement, which obviously makes sense from a privacy perspective. Thank you.

The CHAIR: Thank you. Mr Puglielli, over to you.

Aiv PUGLIELLI: Thank you, Chair. Just to pick up some points that were raised earlier in the session. Obviously you are not Meta and you are not Google. You are a very large company, though, with market capitalisation of, I understand, US\$2.34 billion. You have to understand that as a committee I think our core focus needs to be on prioritising safety over any particular platform's business model. I am just noting, while we of course appreciate you appearing before us today, Grindr has not provided a written submission to the inquiry as yet. Can I ask, given that: are you able to come back to us? You know, you have noted that you are updating your systems over time based on what you learn. Can you come back to us with an exhaustive list of

what updates you have undertaken since the more recent publicly reported attacks in Victoria have occurred, say, over the last three years?

Joe HACK: Yes, we would be happy to provide the committee with a written outline of what our safety practices and protocols are, as well as the tools that are available to users.

Aiv PUGLIELLI: Thank you. Just to pick up some of our earlier exchanges before, do features of the app change in different countries around the world?

Joe HACK: No, they do not.

Aiv PUGLIELLI: Is it possible for that to be the case? Is it feasible for there to be features implemented that are specific, for example, to the Australian context?

Joe HACK: I think it would depend on –

Aiv PUGLIELLI: I highlight it because earlier, when we were talking about things like identity verification, the instance was referred to of countries around the world where being homosexual, for example, is illegal. In the Australian context, it is not. So would it be feasible for an Australian-specific measure to be implemented that allows the information that needs to be kept to be kept?

Joe HACK: It would certainly be something we could explore, but I would say that I think one of the concerns as well is creating a system where users who are not comfortable disclosing who they are somehow get put in a separate caste within the community that they do not necessarily want to be in. In other words it could signal something about a user that is disparaging but not true. I think that is just something to think through. I will say this is a topic that we have thought through a bit, and it is something that we are sensitive to based on feedback we have received from the community, that there is a sensitivity around this in terms of creating different – I do not want to say ‘castes’, but I cannot quite think of a better word. I would also just add that some of the other companies in this space that have implemented verified profiles still have problems and issues with off-platform violence. So it is not a panacea here that is going to really I think, unfortunately, be a cure-all.

Aiv PUGLIELLI: Do you accept that it would hurt your business model for this change to be implemented?

Joe HACK: I do not know that it would.

Aiv PUGLIELLI: Based on the feedback you have received, you do not think it would?

Joe HACK: What I am sharing is that what we have heard from users is that there is a concern in terms of signalling that if they are not verified, because they are not comfortable disclosing who they are, it would somehow signal that they are perhaps a bad actor when they are not. That is something that we take into consideration in trying to foster and encourage a community where people can comfortably find connections and explore on their own terms who they are.

Aiv PUGLIELLI: Thank you. Thank you, Chair.

The CHAIR: Thank you. I will finish off with just a couple of final questions.

Ann-Marie HERMANS: Joe, I have had my hand up for a little while. Sorry, you might not have been able to see it.

The CHAIR: Sorry, no, I did not see that. I will finish off mine if that is all right, Ann-Marie, and we will see if we have –

Ann-Marie HERMANS: Okay. Because I just want to build on something Aiv asked, but that is fine.

The CHAIR: No worries. As an inquiry, our job is to make recommendations to the government. In this sort of difficult environment where there are a lot of factors that lead to these situations, what things do you think government could do better to ensure users are ultimately safe?

Joe HACK: I think a few things. I think some of the learnings we have had have come through experiences in other countries, one of which we described in France earlier. But I do think a key is really, first of all, education, ensuring that people are aware that these crimes are happening and what sorts of tools there are and measures they can take to protect themselves. That education responsibility also falls on us. One of the things that we have learned is that just simply having these tools exist is not enough; we need to remind users regularly that they exist. So we are looking at ways that we can increase the frequency of not just our safety messaging when there are problems but also messaging around the tools that are available for people to take measures to keep themselves safe.

I also discussed earlier ways to increase trust between our community and law enforcement. I think that is important. I think taking localised approaches to these issues as well: our community is small but mighty, and we are a community really that has over time benefited from mutual care. I think that sort of responsibility within the community is a strength but also something that we can leverage through community partnerships to try and do more and increase resilience. It is collective work that needs to be done, which again I think is why the approach the committee has taken is a great one. It does remind me a lot of the work we have done in France. We stand ready to work with you all as a partner in this.

The CHAIR: Thank you. I will go to Ann-Marie for a quick 30 seconds. We have run out of time, I am afraid.

Ann-Marie HERMANS: Thank you, Joe and Priyanka. I hope I said your name right, sorry. I just want to go back to this same incident where we had the under-age – we have got a youth crime issue. How much of it is actual youth? How much of it is actually people enticing youth to do crime? It is a bit difficult to determine. I just wondered, in terms of your data and the under-age usage, what percentage you would say from our state or from our nation appear to be under-age young people that are trying to access and pose as people who are perhaps older – or maybe they are not trying to pose but they are under-age. In terms of the data that you are receiving, of those, what percentage are people wanting to commit acts of criminal intent and violence against the LGBTIQ community?

Joe HACK: Priyanka, do you want to take that one?

Priyanka PURKAYASTHA: Yes. Firstly on numbers, we will have to come back to you on the exact numbers and percentage of what this breakdown looks like. But based on what I have already observed in our earlier numbers check, we are seeing a significant drop in under-age user activity on the platform since the introduction of the age assurance solutions in December. But obviously there will still be folks who are finding ways to evade it.

Ann-Marie HERMANS: What is a drop? What are we looking at? What percentage?

The CHAIR: Hold on, Ann-Marie, the time is up, so we will just have to finish on this, sorry.

Priyanka PURKAYASTHA: I will follow up with more details on what exactly that drop looks like and what that number is. But one last point I will call out from before is the device ban point. A very important action we take on under-age accounts is banning that device so that they cannot create any new accounts from the same device. That has been a very helpful tool for us to avoid recidivism or repeat offenders coming from the same account.

The CHAIR: If you are happy to send through some additional information on that point, that would really be much appreciated as well. Thank you.

That brings our session to an end. I just want to thank you both for your time today. As I said, you will be provided with a proof version of the transcript to have a look over and review. But from us, thanks very much for your time. We really do appreciate you taking the time out of your day – or night, as it might be – to appear.

Witnesses withdrew.