

Collaborating Our Way To Safer Dating February 11, 2020

Presenters

Mark Brooks, Founder of Internet Dating Excellence Association

Geoff Cook, Co-founder and Chief Executive Officer of The Meet Group Companies

Parry Aftab, Cyber Safety Group

Christof Wittig, CEO of Hornet Networks

Jens Kammerer, CEO of Jaumo

Operator

Greetings, and welcome to Collaborating Our Way To Safer Dating webcast. You may submit web questions by using the ask a question box, on the lower left portion of your screen.

I would now like to turn the conference over to your host, Mark Brooks, Founder of Internet Dating Excellence Association. Thank you.

Mark Brooks

Thank you. We're going to paddle (INAUDIBLE). Please, I'd like to introduce you to-- And so, we'll start with a quick overview of each of the panels company's and what makes them quite unique and special. And I'll give you a quick overview of IDEA. IDEA started in 2007, as a community of 700 dating executives and leaders. And IDEA exists to help the dating industry grow and achieve its full potential and promise.

So, I'd like to ask Geoff Cook, first of all, this is the co-founder and Chief Executive Officer of The Meet Group Companies, Unique and Special.

Geoff Cook

Yeah. Hey, Mark. Thanks for having me. So, at The Meet Group, we're working to marry dating with live streaming video across a portfolio of apps, which include MeetMe, Scout, Tagged, La Vue, and Growler. Every day, there's more than four million people logging into our apps, and every month, more than 15 million. As much as a meeting per second is happening across our network.

One of the things we're most excited about, recently, is having built a live streaming dating game called, Next Date. We're working on a number of features as we speak, to engage our users and promote safer dating.

Mark Brooks

Thank you, Geoff. And Parry, could you give your overview on Cyber Safety group, your (INAUDIBLE) and NGO's.

Parry Aftab

Yeah. I'm not in the industry. I'm an internet privacy and security lawyer. And I've advised most of the big players in all of the digital industry, over the years. But most of my time now is dedicated to running the world's first cyber safety organization that's 26 years old. And we do everything from birth to death and do a great deal on cyber dating and digital relationships.

So, I'm the non-commercial internet safety expert in the panel.

Mark Brooks

Great. Thanks, Patty, looking forward to getting your perspective.

Jens Kammerer, you're the founder and CEO of Jaumo, is it Jaumo, or Jaumo?

Jens Kammerer

Yeah. It's Jaumo. Thanks, Mark. Thanks for having me, and thanks for the introduction. So, Jens, CEO and co-founder of Jaumo. I joined the dating industry 20 years ago, something like this.

We're a remote company, based in Germany, and we have several dating apps, including Joyride, and Jaumo. Those are our two flag ship apps. We have 50 million users. Our focus is on casual dating.

So, Joyride is the number one dating app for people that don't look for long-term relationships. So, we have the world's biggest community of real people looking exclusively for a good time.

Mark Brooks

And Christof. Christof, you're the founder and CEO of Hornet Networks. Could you tell us more about your company, what makes it special?

Christof Wittig

Of course. Thanks for having me on the call, Mark. And my name is Christof Wittig. I'm the founder and CEO of Hornet, which is a gay social network with over 25 million diverse users, globally. Our mission is to empower gay men to come out and join in the fun and fabulous, which is the gay community.

So, we are much less of a dating and one-on-one matching, than creating a space or a community, where people can come out and express themselves. And as such, look more like an Instagram or a feed type model, than a more traditional dating model.

Mark Brooks

Alright. Thank you, Christof.

(INAUDIBLE) that you all have in common, is that all of our communities, our key goal is to improve the real world when it comes to safety, and really keep our members safe.

So, I'd like to ask you, what are your companies' approaches to safety, and what do you do to promote safety on each of your apps?

So, Geoff?

Geoff Cook

Sure. So, nothing's more important-- You know, to us than protecting the safety of our members. We have vowed to constantly improve, with best in class safety updates, committed ourselves to high standards, adopted industry leading practices.

The goal of the safety operation, ultimately, is to promote a safe environment so that our users can make meaningful connections. And we approach this, really, in three ways. First, is education, we publicly display our code of conduct and we require agreement to it before every live stream. We provide safety tips to our users, in a form that is easy to understand.

For our MeetMe app, for example, we have a three step safety pledge process, which we require all of our users to complete. The user is presented with three screens and they must pledge to each of them. And each, the screens include content like, always meet in public, they must click I pledge, don't share personal info, I pledge, don't send money, I pledge.

You know, the second-- You know, leg of the stool, would be monitoring. We don't wait to be told by our community of content issues. We devote more than half of our workforce to regulating the content of our apps. More than 500 paid moderators, as well as advanced AI and algorithmic processing to police our content.

We also screen all new registrations against RSO, Registered Sex Offender registries in the U.S. While our focus is proactive monitoring, we're also ready to react, when necessary, with highly prominent abuse reporting buttons for the varying types of content we see, from profiles, to photos, to videos.

And then the third leg, we'd say, is enforcement. We generally employ an escalating system of strikes. Although, certain behaviors are one strike and you're out, we generally opt to give you-- There's a couple chances to learn. Typically, when we take action against a particular account, we do give the specific reason, so that users can learn the boundaries.

For example-- You know, users are not permitted to drive, while they live stream. And they may not appear in bathing suits, unless-- You know, for example, they are at the beach. And this type of-- You know, we do believe that at the time of enforcement, is a great time to provide some education. And we see-- You know, the overwhelming majority of users with a single strike, do not repeat the infraction.

And then, in certain cases, of course, we also look to empower our users. We allow our users to block another user. And then we also, within our live streaming function, allow a streamer to appoint what we call bouncers, from among their community, in order to moderate, especially the text comments.

So, that's essentially the essence of our approach.

Mark Brooks

Great. Thank you, Geoff. And Christof, could you describe how your company approaches safety, and what you do to promote safety?

Christof Wittig

I am happy to do that. And many of the things are similar, or the same in fact, as Geoff just pointed out. And I would like to point out a few things that may stand out and go beyond what's of common industry practice.

In version six, last fall, we introduced a Hornet Badge, which is a badge of authenticity, that is prominently displayed throughout the app. That is a badge that people need to earn by, basically, disclosing, or posting, or sharing things about themselves, which then has a certain level of response interaction in the community.

So, we basically encourage people to express themselves and open up. In return, the reaction that they get on that, usually tells us, on our machines, whether that is an authentic profile that gets authentic reactions. Or whether it's a fabricated profile, that often then follows certain patterns that typically, for catfish or spammers. That would be a great way for users to quickly identify those who are way more likely to be authentic and real, versus catfish and spammers, which I think is a huge problem in our industry.

So, that's one very, I think, novel model we introduced. And it's been extremely well received. So, the numbers of spam reports, of catfish reports, for instance, has dropped since, 60%. Simply because it's much more costly and less attractive to go all the way to create these profiles. So, this is how Hornet Badge came out in version six.

Another one that we are doing, is our hacker and anti-bot program. So, these are more technical attacks that happen towards-- You know, the users of the community. And here, we are great fans of the program called Hacker One, which is a (INAUDIBLE) program, where we are constantly, basically, challenging-- You know, hackers to try to break our defenses. And we're paying bounty's, if they do so, so we can remedy it.

So, we, basically, create a platform how black heads can become white heads. And create one of the most defensible, robust tech platform that's out there in the industry, at Hornet.

And last, not least, I just want to, kind of, elaborate that for us, a lot of safety comes from visible behavior through role models. So, we believe this (INAUDIBLE) educational approach, rather than the policing approach when it comes to the behavior of users. And I think we believe most people are not evil. But-- You know, there may be, especially in the context of a gay social network, or something that is more inter personal, they may be triggered by wrong senses. But if you create an inclusive and supportive community, of course, are very strict against the offenders to create a culture of mutual respect and get out all the toxic-ness that is often prevailing today on many of the dating or social network platforms.

Mark Brooks

Thanks, Christof, very fascinating. Jens, what's your approach?

Jens Kammerer

Yes. Thanks for asking. So, similar things here. I mean, dating involves strangers, and with strangers you always have to be careful, no matter if you meet them online via dating apps, social network, or real life, whatever. So, we really want to make sure that only real people use our apps and not fakes, scammers, bots, whatever.

So, we invested a lot in fraud prevention in the last year. So, to detect unwanted users as soon as possible, with a high detection rate. And for example, we scan for the usual activity and if something is not according to the rules, then we, kind of, look closer. We also have moderators to look closer, and our main thing that we introduced a year ago, was a user verification that is fully automated. That means you can upload a selfie via the app, where you may make a certain head gesture and then you shoot a head selfie and our system compares the gesture with the faces of all the photos and everything. And with that check, we check many other things, and that really helps us to improve our system.

So far, 1.6 million users have done that verification very successfully. More than 10,000 users do it every day. And it helps us to, at least a little bit more, to ensure that the user is a real person, of course, all the other things are also in place, like we already heard from the others. And the other thing that I believe is also very important is to perform. The users try to educate them, that they are aware that sharing personal information too early is risky. And all those measures together, I think, helps to improve the safety at Jaumo.

Mark Brooks

Thanks, Jens, much appreciated. Patty, I'd love to get your commentary. What do you think?

Parry Aftab

Well, I've known Geoff for 18 years, maybe, from when he first started my yearbook, perhaps 15 years ago. And so, I saw that he was learning very quickly, because of the expose to all of the crazy things that teens will do. They're very good at breaking the rules. And I find whenever we look to protect adults, if we start with teens, you're more than able. It's like working out with weights that are much harder than you're going to need.

We are putting-- The Cyber Safety Group is a new charity we just created, after having the first internet safety organization that's almost 26 years old. And we are working on standardizing cyber safety, for children, for adults in vulnerable situations and intimate situations, cyber dating, cyber relationships, healthcare, digital hygiene, those who are grappling with how they come out, and different mental health issues and special needs. Those who are often preyed upon more than others, online.

And so, as we do this, I was very interested and happy to hear the different innovative approaches that are being adopted by the three platforms. And so, I welcome learning more about them, and maybe using some of those as a bases to create the standards. I advise the IEEE, the Standards Association, as we're looking to pull these together. And, I think, that his informing users how to be smart about what they're doing, providing a nurturing and supportive community, which is always good. Policing with those who are the outliers here, looking at impersonations, cyber stalking, harassment, to trolling predation. All of the things that, unfortunately, go along with intimate and personal relationships, as people who are lonely. Or who are looking for relationships, and love, and friendship tend to let down their barriers more, because that's the only way you can find that intimacy. And then, in doing so are more vulnerable.

So, I love that they're thinking about it and putting privacy and safety first.

Mark Brooks

Thank, Parry. I mean, really there's a lot of opportunities and standardization, and certainly education. And also, collaborations. Not all safety related issues can be solved in a vacuum and there really are lots of opportunities with the dating industry, to work together. And that's really what IDEA stands for as well, is getting industry together to learn, share, and compare best practices and what's working for them so we can all do better.

So, what other areas of collaboration, that you're either working on or that you would really like to work on, to promote safety? Is there anything you wish existed that didn't, that would really help promote safety? Geoff?

Geoff Cook

Sure. So, we agree that collaboration is critical to safer dating. We actually work actively with partners like NGO's, law enforcement, even competitors in the pursuit of safety. We think safety is not something that's valid to compete over. It's something to ensure the entire industry adopts.

We do collaborate to stay one head of bad actors. An example of this, actually the end of last year, I kind of laid out a vision for what we want to achieve in 2020 on the safety front, including user verification, age estimation, textual analysis, among other things. And in January, just last month, we announced our work with Microsoft, to pioneer Project Artemis, which is an

unprecedented text based anti-grooming solution that detects problematic behavior in real time and allows moderators to quickly remove bad actors. Project Artemis is now freely available to qualified organizations.

Also, at our cost-- You know, we do collaborate with a company, Family Watch Dog, to scrub our registrations and our user base against registered sex offender registries. We also collaborate actively with organizations like the family online safety institute, where we sit on the board, the online dating association, where we sit on the board. Of course, this organization, IDEA, as well as we protect global alliance, among others.

And then, I think-- You know, as far as the second part of your question. You know, what other things could be out there. You know, I would love to see a conversation started around collaborating across the industry to determine-- You know, the feasibility of keeping bad actors of one dating app, off of other dating apps. And working with industry players on enhancing device blocking capability in particular.

While we all have ways of keep unwanted devices from accessing our services, I'm sure, we need more fool proof ways of doing so. And serious conversation around black lists and data sharing. And-- You know, I think we recognize that in any event-- You know, to achieve our vision of meeting the universal need for human connection, it will be critical to elaborate on safe practices, moderation, and education. I think there's always something we can learn, and forms like this are a good opportunity for that.

Mark Brooks

Wonderful. Thank you, Geoff. Christof, how would you like to see the industry work and collaborate more together?

Christof Wittig

Yeah. I would like to (--CROSSTALK--). Yes. So, I'd like to welcome, of course, any of these corporations, with Geoff, that Geoff mentioned. I wanted to point out, maybe, a slightly different angle that applies to a gay social network. There's 72 countries worldwide, which still criminalize LGBT.

So, at some stage, or some frontier, we are not able to rely on, for instance, people sharing their real name or ID, because that could be used by governments, for instance, to entrap these people and potentially-- You know, to harm, all the way to, potentially, injury, or death. As it happens in some countries across the world. So, we need to find ways, how technology creates-- You know, authenticity, or confirms that people are real, or somewhat existing actors, without incriminating them or potentially entrapping them, in some form or the other for being, for instance, gay.

One of the initiatives who are working on here, and that is, maybe far out, but in the long run, I believe that is one of the ways technology can solve a big problem, is the LGBT token, block

chain based. Both identification and transaction system, which creates a record of one's spending and earning with that token. And if you think about it, in real world-- You know, often even ID isn't accepted as an identification. You were actually asked to produce utility bill. And that's the equivalent on a block chain, you can actually show your history of, for instance, transactions, and that makes you a more real actor, without having to give up your pseudonymity, i.e., the person who you actually are. So, you can't feel entrapped unless you enclose your identity at your leisure.

So, block chain can play a big role when we're working on the LGBT token, and that is something that may stimulate for the discussions and corporation also among different parts of the industry.

Mark Brooks

Absolutely. Christof, thank you so much. Jens, what are you working on? What areas of collaboration are you working on that promotes safety?

Jens Kammerer

Yeah. Nice ideas, regarding the block chain, Christof. Thanks. I fully agree with what Geoff said, it's not something to compete on, or is something-- Yeah. It's something we have to work together, as the whole industry. And I mean, it's not just the dating industry, I mean, it can be the whole social networks, all the social apps or services. We can share more learnings and improvements, for example, because we should make it really hard for the bad people to be successful.

And it's not just by the right technical measures, but also the way we educate the users at the same time. From the technical side, it could be, of course, by sharing more data, black list patterns, or whatever we see on our day to day business. And from education, it's the same thing. There are, like, some industry standards. I really like the idea of the Internet Dating Excellence Association, and all of the social safety batch. I think great first steps here, to bring everyone closer together and have some, yeah, industry standpoints for social safety. I really like the idea and the initiative. Thanks, Mark.

Mark Brooks

My pleasure. Thank you, Jens. And Parry, you have the benefit of great perspective. What would you like to see happen, in terms of collaboration across the dating industry?

Parry Aftab

Well, I think that we need to start looking at black lists. And that, of course, includes policies and appeals. And you can look to the casino, gambling industry that has been very good. Even though they're competitive, for the high rollers, they're very good at sharing information about card counters, and those who are engaged in fraud and technology to unfairly win. And looking to what they've done is very helpful.

I'm looking to what we're doing with children. So, we are engaged in block chain, and authentication that then turns into block chain, on identifying children without identifying who they are, just what they are. Yoti's been doing some very interesting work on authentication and not storing the data afterwards. And the cyber safety group is charity. We function in 76 countries around the world, with separate charities in certain other countries. And we're, at the base of it, we're a large U.S. charity where we're all unpaid volunteers. But with 16,000 of us, there's a great deal that can be done.

From looking to see what other adjacent industries are doing, and adopting that, is crucial. And I think as we start looking at awareness-- I've been in this field so long; I'll be retiring once I can find somebody else to do this for free. You need to look out to your user base. So, The Meet has a lot of video and influencers who are doing remarkable entertaining things. You have different people with the other apps that have talent. Reach out to them on challenges, give them some parameters on safety and ask them to create awareness models, things that they can share that can get out there, that's less like mom telling you what to do and policing, and more, how can we create the kind of world we want to populate. And doing it in your own way.

So, everyone will have a slightly different flavor because of what it is you try to conceptualize, and you try to encourage within your communities and using them to do some of this work, so that they truly do adopt this. But we're going to be helping. We're going to have seals, and audits, and rankings of those. If they artier to the seals, I'm excited about the opportunity and introduction to IDEA. I think there's a lot that we can do, and you can do, and across industry on standards. I think that there's so much that can be done that work for the industry, and work for safety at the same time.

Mark Brooks

That's fascinating. Absolutely fascinating. Thank you so much, Parry. And very inspiring, actually. There are other industries that are going through similar problems that we really need to look to and be inspired from.

So, the next question I'd like to ask the panel is what's the most interesting thing that you're working on right now, to promote safety, on your apps, in 2020 and beyond? Geoff?

Geoff Cook

Sure. So-- You know, we're always working on a number of different projects. You know, I think one, that's certainly top of mind today, we announced in a blog post, that we're working on exploring a technology called Face Tech, to make progress toward some of the goals I mentioned around authenticity, age estimation, device blocking. Essentially, leveraging through the face verification.

We expect to launch a verified badge across, at least a couple of the apps, by year end 2020. Verification would eventually encompass different attributes, like proving you're a human and not a bot. This is called a liveness check. We'll also be exploring the possibility of showing the

confidence level, giving user looks like their profile photo, potentially making catfishing a thing of the past. And, I think, far exceeding some human solutions to that same problem. While also exploring advanced age estimation algorithms that the 3D face map verification technology provides.

What's more, they want to identify a bad actor using this technology. We can ensure the same person cannot verify another profile across any of our portfolio, of our apps. And so, we have a team right now that's been working for a couple months on this and will be planning to beta launch this in March or April, on our MeetMe app, in our first use case. so, that's what I'd say I'm most excited about right now.

Mark Brooks

Fascinating. Okay. Christof, what would you say is the most interesting thing you're working on, right now for safety in 2020 and beyond?

Christof Wittig

For sure it's the Hornet badge, and further tweaking the algorithm behind it to, again-- You know, foster the idea of an authentic user. And that, is a user that's complying with the cultures, and the norm, and the tone, that we try to promote on the network.

I do believe that there is a problem with networks that are too large. So, one size fits all. That basically creates way too much and anonymity and-- You know, too much stranger-ness, if you will, to (INAUDIBLE). But, I think, we want, probably, to look at-- You know, a village doesn't need that much of a police, because there's less strangers. Because you know each other and you usually are aligned around the certain, normal, culture. And there's simply less crime in a village, than there is in the city, and there is in the internet at large.

So, I think, creating safer virtual spaces creates a culture, but the community becomes, sort of, the self-regulating ultimate, sort of, force to bring out the best in people and effectively bring those few bad apples that are out there, out of the system very fast.

So, for me, it's about creating smaller, vertical social networks, which more are keen to try it. And I give one example, very often is Strava, which is a social network of athletes. I've never, ever seen a catfish or a toxic post on Strava, because it's an inclusive and supportive community of athletes. And there's simply no culture of being abusive, toxic, or trying to extort people. Maybe that exists at the margin, but it's way, way less viable than what you would see, for instance, on the one size fits all social networks today.

Mark Brooks

Great point. Great point. Jens, what's one thing that you're working on right now?

Jens Kammerer

There're basically two things that we're working on right now. So, firstly, we keep optimizing our system with the goal to have a full automation for the whole moderation and fraud detection process. So, we're almost there. A couple of months ago, we still had quite a few moderators that are prominently 24/7, dealing with many manual checks. And it was, like, (INAUDIBLE) and we really tried to reduce this, and we reached much higher automation.

And we're very good in detecting bots and profiles that were automatically generated, but we still want to improve in the detection of real person, low frequency spammers that are not as obvious as bots, for example. So, they try to fly under the radar, by being quite passive, only sending a few messages. So, it's a bit harder to catch those kind of fraudsters and we're working on that, that we will improve here too.

And secondly, we want to bring more information about safety, directly to our apps and not just our website. We have it on our website, typical dating safety tips. We think it's better to show those tips directly in the apps where the users are, at the moment they really need the information.

For example, if they share or exchange their mobile phone number in chat, or schedule a date, something like this that we (INAUDIBLE) user know that they should be careful doing this, that they shouldn't share personal information too early, for example. And in the long run, it would be ideal if the anti-fraud system better understands the context of the communications of the chats that are going on, so that we can distinguish between a normal and healthy conversation. And one that could lead to fraud or unsafe behavior.

And, of course, for this, there is a lot more to develop and a lot more machine learning has to be involved, because this, of course, has to be done, fully automated and respecting the privacy.

Mark Brooks

I see. Thank you, Jens. And Parry, I should ask you, what is taking your focus for 2020, for your group? What are you promoting for good solutions for safety?

Parry Aftab

Well, having been in this field 25, almost 26 years, and safety, and digital privacy, and security, we're seeing a lot more emphasis on the human side. Vince Cerf, the man who is credited with helping invent the internet, created the People's Centered Internet Group, that a lot of us were brought in on to look at the digital risk management people. And trying to come up with a human centric design.

Now, all of these three, are dealing with that and they're looking at it. My advice is, A, the world is now re-thinking safety, security, privacy. At the very high level government, at the United Nations level, at the Standards Associations level, a lot of people are tired of the abuse that they've been seeing recently. And in fact, I was just invited by our attorney general, in the

United States, down to a small meeting that's going to be at (INAUDIBLE) headquarters near the end of the month where we are looking at reconsidering a law called, Section 230, of the Communications Decency Act. Which gives all of the providers immunity for what it is that the users do on their system. It was designed just for defamation, but it's been expanded by the court, far beyond that.

And now, politically, for the very first time, you're seeing a willingness to cut back on these areas of immunity. And I was called in by the judiciary committee, to senate, to discuss with them, ways of using standards that have been approved and kicked by the cyber safety groups, the digital best practice risk management groups, law enforcement, etcetera. And using those as a basis for some companies being able to keep this exemption and immunity, as long as they adhere to these.

So, I think the days of the wild west are finally over, as a lot of people who've realize that the Facebook's of the world have gone too far. And I was one of five members of their safety advisory board for many years, until I learned what they were doing. And I can guarantee you that we will not be working with them going forward. And some of them are bad actors and you know they are. And others are just negligent, or too many people are designing cool technologies without thinking about the impact.

But it's time. The world's health organization is looking at this now. Law enforcement are looking at it more deeply. When you see some of the things, like, Artemis, that The Meet's working on, you recognize that the people who are adults looking for relationships, often have children. And when they post pictures and talk about their children, their children may be the targets of someone who's coming in to pretend their interested in the parent but are really trying to get there on the children.

So, a lot of people think of protecting their direct users without recognizing there's a responsibility to all of the adjacent users as well. And you can do that. It's good for business. You want to be on the front stage of the New York Times for the right reasons, not the wrong reason. And in the end, your insurance cost will come down.

Mark Brooks

Great, Parry. Thank you so much. And I think that brings us to a very nice point to close out the panel and see if there's any questions from the community that are listening in. I certainly appreciate all of your answers and there's an absolutely smorgasbord of wisdom for the industry and our listeners to listen to again, and really get their heads around the initiative the dating industry are leaning in on to improve safety.

So, let's see if there's any questions from the community. I think we're good for now. So, I think that brings us to our close. Thank you so much for your time. (CROSSTALK)

Geoff Cook

Aright. Thank you, Mark.

Christof Wittig

Thank you very much.

Parry Aftab

Thank you.

Operator

Thank you. this concludes today's webcast.