

Would background checks make dating apps safer?

Match Group, the largest dating app conglomerate in the US, doesn't perform background checks on any of its apps' free users. A *ProPublica* report today highlights a few incidents in which registered sex offenders went on dates with women who had no idea they were talking to a convicted criminal. These men then raped the women on their dates, leaving the women to report them to the police and to the apps' moderators. These women expected their dating apps to protect them, or at least vet users, only to discover that Match has little to no insight on who's using their apps.

The piece walks through individual attacks and argues that the apps have no real case for not vetting their users. The reporting positions Match as a company interested more in scale than user protection, like many other tech companies. Match told *ProPublica* that it can't perform background checks because the system is not just costly but unreliable. A Match spokesperson told *ProPublica* that the government databases often rely on old photos or lack data on offenders, which doesn't help the company vet users.

But dating apps have a deeper identity problem, and it won't be easy to fix. Even if the databases offer solid information, people might not want to provide their full name on the app because it comes with extra weight that would shift the apps' culture. People might not feel as open to discussing sexual preferences or talking freely. Women might not want their full names on the app out of fear of harassment.

Match says the background check system is unreliable

A dating app that provides full names and detailed information

about users would be a monumental cultural shift for apps like Tinder that are purposely vague. Tinder targets 18- to 25-year-olds who are single and looking to meet new people, mostly without commitment. Adding last names to their profiles makes the app more serious, although the slight trade-off in culture is probably worth it to ensure everyone on the app is who they say they are.

If a background check is too much work, apps could ask users to upload a photo of their ID, like Uber drivers, to verify themselves, and then require that people include their real last name on the app. This way, daters can at least Google their dates and, if they're particularly worried about sex offenders, check public databases. That feels like the simplest solution, although it then requires users' trust in the apps to keep their data safe. It also could leave users vulnerable to stalking if strangers can find everything they want to know about a match.

Overall, verifying identity on dating apps has always been tricky, particularly because of prior stigma surrounding online dating. Every product approaches that problem in a slightly different way. OkCupid, a Match Group property considered an online dating pioneer, allowed users to identify through anonymous usernames up until 2017. When it announced the pivot to real names, OkCupid said it wanted to stay modern. The team said daters should go by who they really are and not be "hidden beneath another layer of mystique." OkCupid crucially doesn't require daters to submit their full names, however, they just have to go by whatever name they prefer when dating.

OkCupid still doesn't require full names

Generally, apps have offloaded the identity problem to Facebook and other social networks. People already share their photos, name, school information, and friends with Facebook, so the app doesn't need to make the case for users to do so again. Most dating apps allow users to sign up through

Facebook, porting their personal details to the app through Facebook's API. They rely on Facebook's identity verification more than their own.

But since the Cambridge Analytica scandal, which resulted in Facebook clamping down on developers' API access, the dating apps started allowing people to create profiles independently from Facebook. They could fill in their own names, often without a last name, and upload their own photos. This, of course, sometimes leads to catfishing, in which people upload fake photos, only to show up on a date looking completely unlike their profile. People can always link their Instagram accounts to their profiles, which provides a layer of authenticity, but still, the actual identity verification part of dating apps barely exists. They mostly rely on social networks' established work in the identity space.

Some apps, like The League, pride themselves on their verification methods. In The League's case, it relies not only on Facebook, but also on LinkedIn. Even with that verification, however, users on the app often aren't given last names, leaving daters to have to ask for someone's name directly or even snoop through mail left on tables to figure it out. The League ultimately knows who its users are on the back end, though, whereas Match Group might not – especially on apps like Tinder and Hinge where most users aren't paying and therefore haven't offered up a credit card.

Daters expect the apps to keep them safe from criminals, which is reasonable, but the industry is broadly unequipped to vet millions of daters. *ProPublica's* story discusses incidents from years ago, when dating apps were used less frequently than they are now. Although dating apps and the industry surrounding them have grown – 15 percent of US adults used them in 2016 – the companies behind the apps haven't made much progress in ensuring people are who they say they are. Now, with more people than ever using apps, Match has to have a legitimate answer for why it can't verify its users. If the

apps keep expanding, users will want to feel safe on them. The question for Tinder – and others – is how.

<https://www.theverge.com/2019/12/2/20991656/match-group-dating-apps-identity-tinder-hinge-background-check>