‘Whisper networks’ don’t work as well online as off − here’s why women are better able to look out for each other in person

Carrie Ann Johnson, Assistant Teaching Professor of Women’s and Gender Studies, Iowa State University

Published: September 30, 2025 8:39am EDT

Would you trust sensitive information from someone you know more than from an anonymous online poster?

kali9/E+ via Getty Images

Whisper networks are informal channels that women use to warn each other about sexual harassment, abuse or assault. The reason they work isn’t because they are secret – they work because they are contextual.

The informal protective communication shared in schools, churches, workplaces and other organizations can be communicated and trusted based on the common language and cultural understanding of those giving and receiving the information.

Since 2017 when the MeToo hashtag went viral, people have been trying to create online whisper networks. Projects like the Shitty Media Men list and the Facebook group Are We Dating the Same Guy are both examples of trying to build a larger warning system. The Tea app sells itself as a digital platform that gives women tools to protect themselves and others when dating men.

However, important components of whisper networks get lost when they are moved to anonymous nationwide warning systems.

I'm an organizational communications and gender scholar. My research focuses on whisper networks and how people use them to keep safe in organizations. When this idea moves to a digital platform, the information may still be useful, but it is harder for participants to gauge how reliable it is.

What makes whisper networks work

Whisper networks form when there is an environment of shared risk. Their purpose is protective. In other words, the people in whisper networks do not share information for punitive reasons, but to protect each other and to make sense of their experiences. There is an unspoken expectation that the receiver of information will also share only with people they trust.

In my study of whisper networks, participants talked about how they could assess the information they receive and give through personal interactions in their offices, congregations, schools and other organizations. They felt like they could measure the trustworthiness of the person sharing information and the trustworthiness of the people with whom they share information.

They also talked about cues, including noticing how the person sharing information treats other people in the office and how they talk about other people when they aren't around. This important component of whisper networks is difficult to translate to an app, even when the app claims to verify people as members.

Women use coded messages and actions in whisper networks to figure out who is safe in any given room, who is in need of whisper network information, and when they decide that whisper network information is worth listening to.

These protective messages tend to be shared either one on one or in small groups. Women know the information is reliable because of how it is shared and who shares it. For example, someone might say, "He is a little creepy toward the undergraduate women." The person receiving the message uses the surrounding context codes to understand the seriousness of the situation.

Another person might say, "He makes people feel special and then uses information to be unprofessional." Instead of a warning about actions, it is a warning about the process the harasser uses and what to watch out for. The person sharing the information wants the person they are protecting to understand the ways this perpetrator tends to move in relation to the people they work with.

None of the language is specific, and it is largely coded so that the listener understands, and the person sharing doesn’t need to worry about the repercussions of sharing it.

Interview participants told me that they usually share information in quiet conversations where they already trust the person they are talking to.

When I asked participants about how they knew they were receiving whisper network information, they talked about how the person would lean in, drop to a different tone or volume, or how the vibe would change. It’s difficult to get any of those clues through an online platform.

The risk of faulty information and misinterpretation goes up when information is shared on anonymous platforms or shared widely. When more specific stories are shared, it’s almost always in a trusted, private setting, not shared widely on an anonymous forum. When protective communication is broad, the network loses the very qualities that made it feel safe in the first place. Few of the nonverbal and social reputation signals exist on an app, and that makes the communication feel less trustworthy.

Anonymous platforms can also create potentially volatile situations. Because people can post anonymously, there is more room for sloppiness, exaggeration and even defamation. These apps build on the myth that there is an individual solution and quick fix for sexual harassment and assault instead of acknowledging the underlying structural and cultural issues.

A different safety concern

Online platforms offer users a limited understanding of how their data is used and stored, so the user’s safety takes second place to the platform owners’ and investors’ financial incentives. These apps have largely been created by people who carry less risk and who are concerned with monetization, even if they also care about safety. The risks disproportionately affect those whose safety is already at risk.

In addition to the issues of effectiveness and trust is the question of safety. The Tea app has been in the news because of two separate data breaches, including over 70,00 images that were leaked to online message boards. Data included government-issued IDs, personal information and private messages. A separate breach exposed direct messages on the app.

So while it’s conceivable that some online lists could be created for specific communities that share a common culture and language, no matter how good the intent is, it is unlikely that the creators of apps and websites are at the same risk of exposure as the people who use them. In addition, apps built for specific communities or communication styles would probably be significantly less profitable than those that are promoted nationally or worldwide and so are less likely to be built or sustained.

All of this isn’t to say that apps aren’t useful and necessary. But based on my research, I don’t believe they provide the same safety and protection as in-person, organizational whisper networks.

Carrie Ann Johnson does not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.