

Think your VPN keeps you safe? Think again

ASU doctoral student shows how privacy apps can become surveillance tools

By Kelly deVos, ASU News
October 23, 2025

More than 700 million people around the world trust virtual private network, or VPN, apps to keep their data safe.

Travelers use them on public Wi-Fi, people living under restrictive governments use them to reach blocked websites and many users rely on them to hide browsing habits from their internet service providers.

The promise is simple: A VPN creates a private tunnel between your device and the wider web. But new research led by Arizona State University student Benjamin Mixon-Baca shows that for many popular free VPNs, that tunnel may be riddled with cracks.

Mixon-Baca, a computer science doctoral student in the [School of Computing and Augmented Intelligence](#), part of the [Ira A. Fulton Schools of Engineering](#) at ASU, helped uncover “secret families” of mobile VPN apps that appear distinct in app stores but share infrastructure, code and sometimes the same hard-coded encryption keys.

His paper, “Hidden Links: Analyzing Secret Families of VPN Apps,” coauthored with [Jedidiah Crandall](#), a Fulton Schools associate professor of computer science and engineering, along with Jeffrey Knockel of [Citizen Lab](#), shows how those hidden ties translate into serious security failures that put everyday users at risk.

“VPNs aren’t a magic bullet for security,” Mixon-Baca says. “In a lot of ways, they can make you less secure.”

Why people turn to VPNs and why that trust matters

VPN adoption has surged for many reasons. People use VPNs to unlock streaming libraries while traveling, to avoid intrusive censorship or to protect themselves when connecting to a coffee shop’s Wi-Fi.

For journalists, activists or anyone else who is worried about privacy, a reputable VPN is a practical tool. But the very power of a VPN — funneling all of a device’s traffic through a remote server — also makes it an unprecedented point of control and surveillance if misused.

Mixon-Baca's team combined forensic reverse engineering of Android app packages with painstaking business record sleuthing to map which VPN brands were really operated by the same entities. That work revealed three major "families" of providers responsible for hundreds of millions of Google Play installs. In the online store, these apps look unrelated but in practice behave like branches of the same company.

"The investigative work, the process of linking different providers together, was the most difficult," Mixon-Baca says. "You're tracing shell companies and legal records across jurisdictions, which isn't my home turf like reverse engineering is."

Surveillance capitalism under the hood

Beyond ownership obfuscation, Mixon-Baca's group documented behaviors that reveal a commercial motive: the collection and monetization of user data. Many of the apps contact third-party analytics platforms, including Google Analytics, the Huawei Analytics Kit and Yandex Metrika to harvest information useful for targeted advertising.

That's surveillance capitalism in action. Data about your location, the websites you visit or device behavior is packaged and monetized by ad networks and data brokers.

Some of the most alarming technical findings were equally blunt. Several apps contained hard-coded Shadowsocks passwords embedded in their application packages. Because those secrets are identical across multiple apps, anyone who extracts the password can decrypt user traffic. Mixon-Baca also found weak or outdated encryption choices and design quirks that enabled attackers to infer or tamper with VPN connections.

"These apps were reaching out to a third party to infer where you were," Mixon-Baca says. "The user would have no idea."

Plain stakes, clear advice

What does this mean for someone on hotel Wi-Fi, a student on campus or an ordinary person streaming at home? If your VPN is insecure, an eavesdropper could read your unprotected traffic; your location could be quietly tracked; and the privacy you thought you had obtained could be far worse than using no VPN at all.

Practical takeaways

Mixon-Baca offers a number of practical takeaways for users:

Be skeptical of free VPNs. If you're not paying, your data could be the product.

Scale makes the problem urgent. The paper's findings affect VPN providers whose apps have been installed hundreds of millions of times.

The issue is both technical and ethical. Users can't make sensible choices when ownership and behavior are concealed. But app stores are strained; they can't manually vet every VPN developer, every line of code or every back-end relationship on a global scale.

ASU's team is trying to change that by moving beyond exposure of the problem to a solution.

They're developing the Common Transparency Scoring System, which can provide a score to rate VPNs on ownership disclosure and technical practices so users and platforms can see a clear signal before hitting "install."

Mixon-Baca presented this work at DEF CON 33 in August and has already seen news coverage and industry conversations follow. For the School of Computing and Augmented Intelligence, the research highlights the kind of high-impact, public-facing cybersecurity scholarship produced by its doctoral students.

"Ben's work demonstrates ASU's commitment to assuming fundamental responsibility for the economic, social, cultural and overall health of the communities it serves," Crandall says. "Ben used the skills he developed in our doctoral program to uncover a serious threat to VPNs."

"There's a real need for transparency," Mixon-Baca says. "If providers are hiding who they are or reusing the same keys across different apps, that's a red flag users deserve to know about."

This story originally appeared on [ASU News](#).

Prefer audited or open-source VPNs from providers with clear, verifiable ownership.

Avoid protocols not designed for confidentiality. Mixon-Baca specifically warns against using Shadowsocks for privacy. Look for modern options such as WireGuard, IPsec or a well-configured OpenVPN.

Remember: A VPN helps in specific scenarios, but it is not an invisibility cloak.

Main image



Benjamin Mixon-Baca, a computer science doctoral student and cybersecurity researcher in the School of Computing and Augmented Intelligence, part of the Ira A. Fulton Schools of Engineering at Arizona State University, presented research at the DEF CON 33 convention in August, discussing how he helped map hidden ties between some of the world's most-downloaded virtual private network applications. Photo illustration by Erika Gronek/ASU