Linked by Design: Investigating VPNs Hidden Connectivity

An analysis of Android apps' ecosystems through historical back-end connectivity

Authors:
Thais Lobo, Elisa Oreglia, Ashwin Mathew and Erin Crandell

Date published:
1 September 2026

JANUS

KING'S College LONDON

About the authors:

Thais Lobo is a media researcher combining digital methods, qualitative research, and an investigative perspective shaped by a career in journalism. She holds an MA in Digital Humanities from King's College London.

Myanmar researcher has several years of experience working in the civil society sector in Myanmar and across the wider region. He holds a PhD from King's College London and researches the role of mobile technologies in the everyday lives of ordinary users. For security reasons, the author is credited under a pseudonym.

Elisa Oreglia is a Reader at King's College London, focusing on Chinese technologies in the Global South, approached from a multimethodological research perspective. She holds a PhD from UC Berkeley and brings research experience from IBM Research Labs in Beijing and tech firms in the US.

Ashwin Mathew is a Senior Lecturer at King's College London, with expertise in Internet governance and the social foundations of cybersecurity. He holds a PhD from UC Berkeley, and prior to his academic work spent a decade as a software developer and technical architect in companies including Adobe and Sun Microsystems.

Erin Crandell is a researcher, writer, and digital strategist working at the intersection of human rights and technology. She is currently pursuing a Masters degree from King's College London.

About the research:

This report draws on research conducted as part of DIGISILK: Digital Infrastructures Along the New Silk Road: a mixed-methods exploration of China's digital investments in its borderland regions[1], supported by the European Research Council (ERC) under grant agreement 850891(DIGISILK) and by UK Research and Innovation (UKRI) under the 2025 Proof of Concept Funding Scheme.

[1] https://www.digisilk.eu/

TABLE OF CONTENTS

Key Findings 3

Introduction 4

- What are VPNs 6
- Emerging debates 6
- VPN transparency: From provider to ecosystem 7

Case study I: Unveiling Qihoo 360's interconnected VPN networks 10

Case study II: Adding nuance to investigations of popular VPNs in Myanmar 15

Conclusion 24

Key Findings

As the VPN market becomes more crowded, effective auditing requires incorporating back-end connectivity in three ways: understanding VPNs as ecosystems rather than individual apps; combining multiple sources of evidence; and monitoring how these ecosystems evolve over time to support ongoing digital rights and regulatory work. Using two case studies, this report shows how integrating Janus — our open-source tool for auditing the historical back-end connectivity of Android apps — with existing digital forensic methods attempts to fill this knowledge gap and provides insights often overlooked by front-end observations, snapshots in time, or single-app analysis.

Despite becoming a critical internet infrastructure, VPN services often remain opaque.

Users rely on VPNs to protect privacy and access information in increasingly contested online environments, yet the lack of transparency in the organisations and technical systems makes it difficult to assess who ultimately manages data.

Understanding VPNs reliability requires looking beyond individual providers.

Examining how providers relate to one another and to the wider digital infrastructure can reveal shared ownership, dependencies, and potential risks that may remain invisible when services are assessed in isolation.

Janus reveals connections between seemingly distinct VPNs.

In a cluster of apps linked to Qihoo 360, a cybersecurity company sanctioned over alleged ties to the Chinese military, the VPN family's footprint is embedded in apps' back end, linking to parent companies and permissions beyond core functionality.

In highly surveilled environments like Myanmar, Janus exposes potentially insecure connections.

In popular VPN apps, like Jump Jump's ad-driven back-end versus Outline VPN's minimal external dependencies.

Introduction

Virtual Private Networks (VPN) establish a secure connection between user devices and a remote server, helping protect data as it travels across the internet. They are an increasingly important part of the internet's digital infrastructure as they mediate people's access to online services and information. Widely used across parts of Asia to navigate content restrictions, VPNs are also attracting growing attention in Europe as policymakers consider their potential use in circumventing emerging age-verification requirements. Yet, despite being designed to safeguard privacy and security, the ownership and technical systems behind VPNs remain largely obscured to users.

We use Janus, an open-source tool for auditing the back-end connectivity of mobile applications, to analyse VPNs from a historical and comparative perspective. By looking at an app's back-end connections over time, Janus provides visibility into how VPNs operate and evolve, revealing patterns across individual apps and clusters of connected applications and infrastructures. Seemingly distinct VPN apps may in fact be connected by ownership, or their digital infrastructure may reveal vulnerabilities that have the potential to leak the personal data that VPNs purportedly protect. Taken together, this approach reveals a more complex view of the VPN marketplace that is often overlooked by approaches based solely on front-end observations, snapshots in time, or single-app analysis.

Janus in Action

Developed as part of the DIGISILK project at King's College London, Janus traces how VPNs back-end connectivity evolves over time:



Collects app versions from Androzoo's open archive of Android applications.



Analyses APKs, the installation files needed for an app to run.



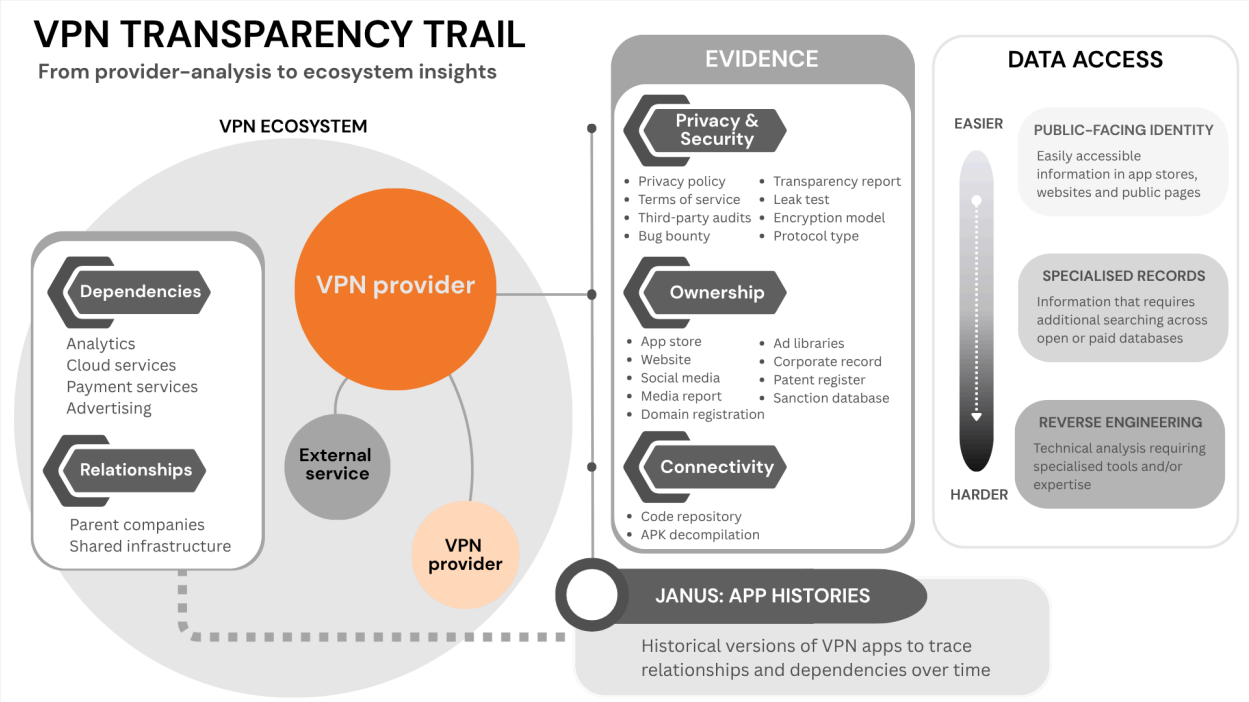
Extracts hard-coded URLs that indicate external data services an app relies on.



Visualises evolving relationships between apps and providers over time.

What are VPNs

VPNs rely on two main security and networking mechanisms: encryption to scramble data, and tunnelling to send it through a protected connection. VPNs may also implement authentication to verify who is connecting to protected networks (such as a corporate network)[2]. When connected to a VPN, the user's web traffic is masked to appear as though it is originating from the IP address of the VPN provider's server rather than from the user's original place of connection. Because of this, VPNs are often known for enabling access to geographically restricted content and reducing the risk of monitoring or interception by third parties.



Emerging debates

VPNs occupy an increasingly prominent position in debates about secure and unrestricted internet access — pitting privacy and data protection against safety and regulatory oversight:

[2] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn

- **Authoritarian Crackdowns:** Countries including Russia[3], China[4], and Myanmar[5] have restricted access to commercial VPNs, leading to their removal from app stores. Instead, users are limited to state-approved VPNs, government-backed platforms, or unverified services downloaded from unofficial sources, which can leave them more vulnerable to monitoring or censorship.

- **Age Verification:** In Europe, the United Kingdom, and parts of the United States, the growing adoption of age-verification systems to protect children online has raised concerns that VPNs could become unexpected loopholes that allow users to bypass region-specific age checks. This has fuelled a broader debate: policymakers seek to address potential circumvention and misuse of VPNs[6]; civic-tech organisations are concerned that such measures could weaken privacy and data protection of vulnerable groups; and VPN providers warn against potential limitations that might undermine the functions that their services are intended to provide.[7]

- **Privacy and Data Protection:** In controlled or contested network environments, human rights groups warn that information control tactics endanger the work of activists, journalists, and researchers who rely on VPNs to access data, express opinions, organise events, and advocate for change.[8] These tensions are particularly pronounced in the Asia-Pacific region, where high levels of digital adoption, rapidly evolving state controls, and strong demand for cross-border digital content contribute to some of the highest levels of VPN use globally.[9]

VPN transparency: From provider to ecosystem

Limited transparency in VPN ownership and operation sits uneasily with the trust users are expected to place in these services, as providers ultimately determine how user data, privacy, and network operations are managed. Most often, investigations evaluate VPNs from two complementary perspectives:

---

[3] https://www.surflare.com/blog/russias-vpn-crackdown-whats-really-happening-and-what-you-can-do-about-it

[4] https://www.abc.net.au/news/2026-06-04/as-beijing-cracks-down-on-vpns-internet-users-in-china-adapt/106754254

[5] https://www.rfa.org/english/myanmar/2025/01/02/cybersecurity-law-vpn/

[6] https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782618/EPRS_ATA(2026)782618_EN.pdf

[7] https://www.techradar.com/vpn/vpn-privacy-security/vpn-firms-and-digital-rights-groups-join-forces-to-urge-the-uk-government-to-leave-vpns-alone

[8] https://www.eui.eu/news-hub?id=new-report-encryption-tools-vpns-under-threat-by-governments-globally

[9] https://www.reportsanddata.com/report-detail/virtual-private-network-vpn-market

- **Single-provider assessments** typically focus on the risks and protections associated with an individual service, examining features such as marketing strategies, privacy policies, third-party audits, bug bounty programmes, transparency reports on data requests, encryption models, internet protocols, and leak-test results.[10] VPN ratings and reviews often build on these assessments, but their scoring can be difficult to interpret across different use cases and may reflect commercial interests;
- **Ecosystem-level approaches** look beyond individual features to examine how VPNs relate to one another and to the wider infrastructure on which they depend — revealing broader impacts, dependencies, and potential risks that may remain invisible when services are assessed in isolation. Increasingly relevant to policy-oriented work, Janus makes a distinctive contribution to this emerging line of research by turning back-end connectivity into a source of comparative digital evidence between different apps or across historical app versions.

Ecosystem-level analyses bring together two forms of evidence. The first unveils relationships between VPN providers, where ownership and organisational linkages help identify shared operators, parent companies, or corporate structures. The second indicates dependencies on external services, where back-end connectivity reveals how VPNs rely on cloud platforms, advertising and analytics providers, payment services, and other third-party technologies.

Identifying relationships between service providers

Often, the first step in identifying relationships across services is to look at lists of popular VPNs in regional or global app stores and identify providers or parent companies owning or operating more than one VPN. Multiple VPN brands under the same corporate ownership are not, in themselves, evidence of wrongdoing. For instance, established providers may legitimately operate several services or brands; however, in some cases, relationships between apparently distinct VPNs may reflect efforts to obscure common ownership beyond where an average user would search, such as app stores and provider's websites.

[10] https://www.security.org/vpn/

Red Flags in VPN Ownership

- **White-label VPNs:** Services developed or operated by one company but rebranded and sold under another name[11]
- **VPN clones:** Large numbers of cloned VPN apps produced using similar branding and naming patterns. They rely heavily on advertising and provide limited evidence of privacy safeguards[12]
- **Third-country incorporation:** VPNs based in jurisdictions that can obscure links to their ultimate owners or to countries associated with high-surveillance[13]

Tracing these less-obvious relationships requires a range of sources and methods, including: looking up corporate and patent registration records; identifying professional links between individuals and companies on social media; and drawing publisher information from app stores, specialised websites, and advertisement libraries that may point to domain ownership and common marketing campaign strategies. Additionally, searches of company names in sanctions and regulatory databases can reveal relevant legal or jurisdictional connections.

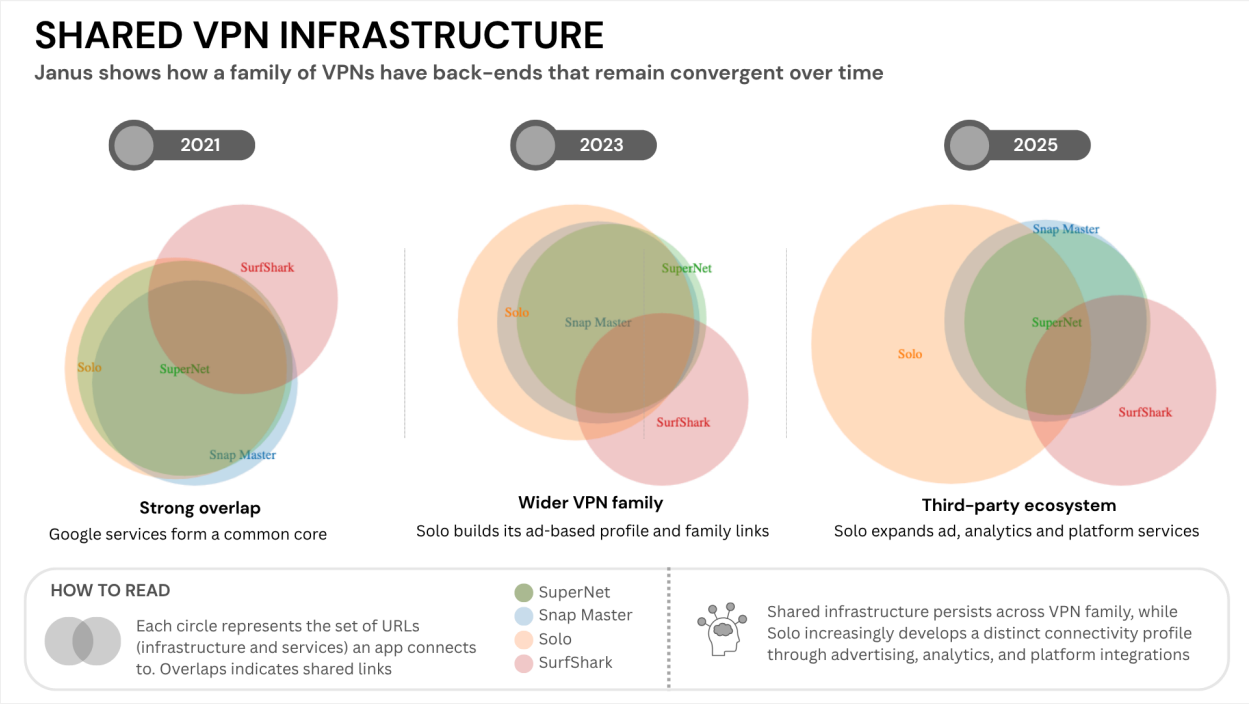
Exploring back-end connectivity

Yet, ownership records do not always show how apparently distinct services are technically connected in practice. Examining back-end connectivity provides an additional way to identify shared infrastructure that may not be visible through corporate records or app-store listings. One emerging method is using Android application packages (APKs) — the app's installation files — to examine underlying code, identify shared vulnerabilities, and compare network fingerprints to understand how apps communicate with external services such as cloud infrastructure, payment systems, social media platforms, and advertising and analytics providers.

Now, with a tool like Janus, we can use those APKs to examine these connections across historical versions of VPN apps and trace how technical relationships and infrastructure dependencies evolve. Janus also standardises back-end connectivity metadata across

[11] https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/
[12] https://www.tomsguide.com/computing/vpns/the-vpn-factory-creating-ad-infested-apps-how-one-developer-launched-39-cloned-vpns-without-a-working-website
[13] https://www.petsymposium.org/foci/2025/foci-2025-0008.pdf

multiple VPN apps — enabling consistent comparisons between providers — while its longitudinal analysis reveals how infrastructure dependencies evolve across historical app versions. Janus complements rather than replaces existing digital forensic methods by providing a capability that existing approaches largely lack, and makes it easier for users, researchers, and technologists to understand and evaluate different VPN apps.



Case study I: Unveiling Qihoo 360's interconnected VPN networks

Examining 360 Security Technology through an approach that uses ownership alongside historical back-end connectivity using Janus reveals a network of interconnected VPN providers that would have otherwise been obscured and raises important questions about governance for consumers and regulators. Also known as Qihoo 360, this Beijing-based cybersecurity company was sanctioned by the United States over its alleged ties to the Chinese military and has been linked through previous investigations to a network of app developer firms. Analyses by the Tech Transparency Project[14] and VPN Pro[15] drew on business

[14] https://www.techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military
[15] https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/

filings, app-store information and specialised records, while Citizen Lab[16] research used APK analysis to look into shared servers and hard-coded passwords, revealing connections between Qihoo 360 and Innovative Connecting, Autumn Breeze, Lemon Clove, Free Secure Connected, and Secure Signal — a network operating a total of 16 VPNs across Google and Apple app stores.

What is a VPN family?

A group of VPN providers connected through organisational relationships. Occasionally, these connections are hidden behind different public-facing identities, even though the services are ultimately controlled by the same entity.

How did we find Qihoo 360's VPN families?

[1] Top downloads:

We used Sensor Tower to identify popular VPN apps across Southeast Asian Google Play stores and collected their publisher and app metadata.

[2] Multi-app developer:

We looked for developers publishing multiple VPN apps and cross-checked them against previous open-source investigations

[3] APK availability:

This identified seven developers with two or more VPN apps available for historical analysis. We selected the Autumn Breeze developer for closer investigation.

Building from these prior investigations, we used Janus to analyse historical versions of three VPNs from the Qihoo 360 family — Snap Master, SuperNet and Solo, developed by Autumn Breeze — and compare their back-end connectivity. Surfshark, an established VPN provider, served as an external benchmark for assessing whether similarities reflected common VPN functionalities rather than family-specific connectivity. We discovered:

- **Coordinated back-end evolution:** The three Autumn Breeze apps shared a greater number of back-end connections with one another than with Surfshark. Across the three years analysed, the apps consistently shared a common set of back-end dependencies centred on Google's ecosystem, such as its advertising stack. A notable shift emerged in 2025, when all three VPNs also began connecting to external platforms, including Facebook, YouTube, and the Russian search platform Yandex;

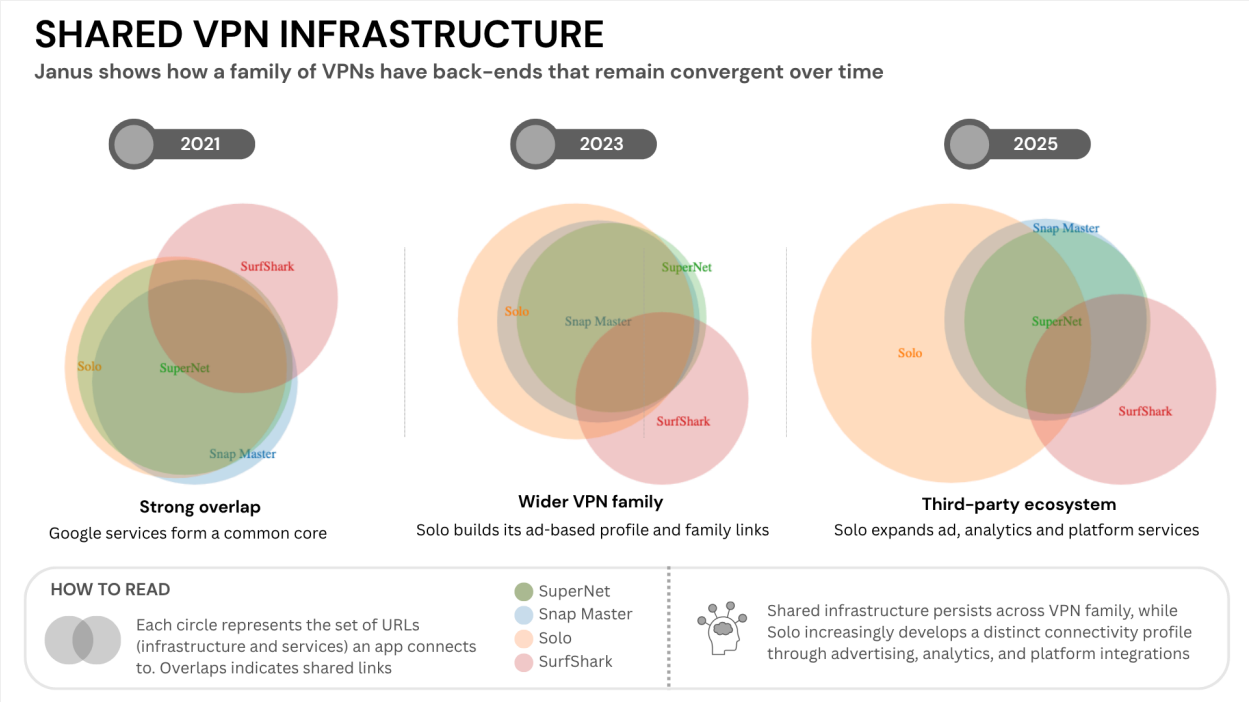
[16] https://www.petsymposium.org/foci/2025/foci-2025-0008.pdf

- **VPN-family footprint:** Across all three years analysed, the apps retained common infrastructure associated with All Connected, another app developer company in the Qihoo 360 VPN family. In 2021 and 2023, Solo VPN back-end presented links to VPN Proxy Master, including its privacy policy, Instagram page, and terms of service, suggesting branding connections between both services. The relationship also points to changes in publisher attribution over time: VPN Proxy Master was initially developed by All Connected, later attributed to Lemon Clove, and subsequently to Secureguard Group, a developer not mapped in previous investigations of the family. Secureguard currently appears as the publisher of Snap Master VPN, while Google Play archived page lists Lemon Clove as its previous publisher, suggesting that the same apps have been attributed to different entities over time;

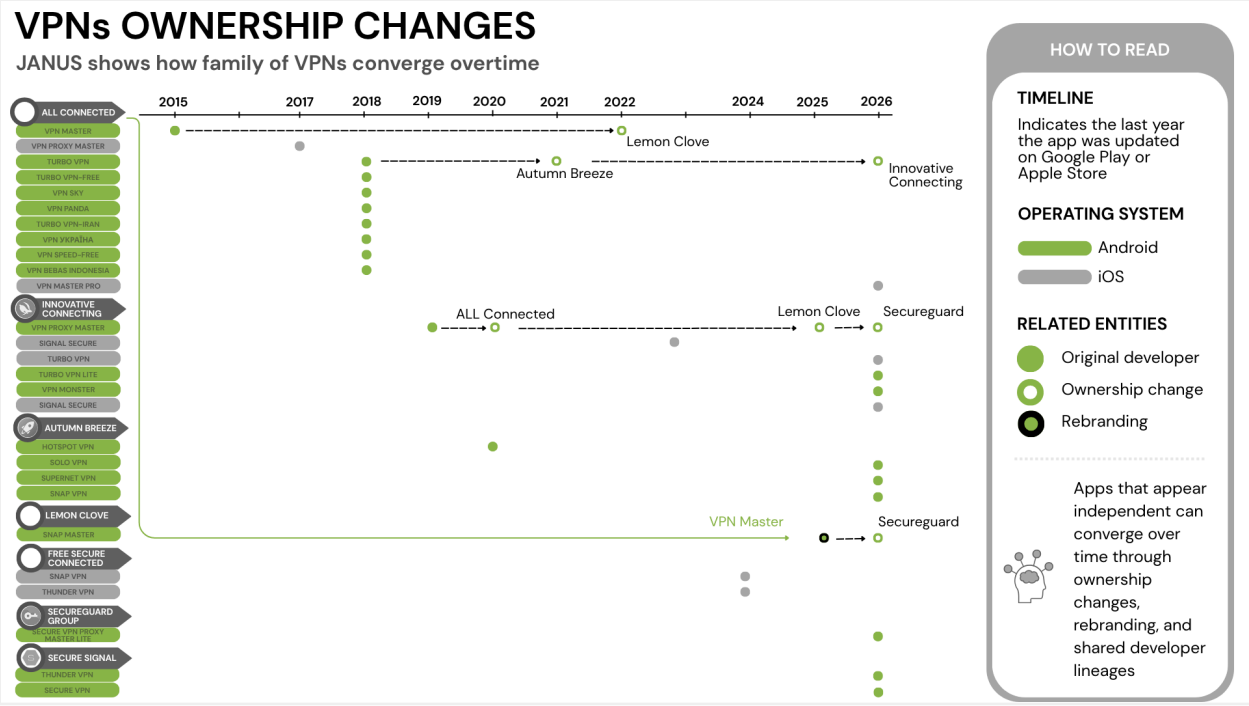
- **Dynamic relationships:** As Solo VPN integrated a broader range of third-party services over time, its connectivity pattern became increasingly distinct from those of Snap Master and SuperNet, while still retaining substantial overlap with the other apps. Solo VPN's unique links reveal connections to global advertising and payment ecosystems, including InMobi (India), Yandex (Russia), TradPlus and ZMaticoo (China), Bigo (Singapore), and Paypal, Chartboost and Unity (US). In 2025, the app also introduced connections to Alibaba Cloud services and Huawei app store, reflecting the growing role of Huawei's mobile ecosystem and its HarmonyOS as a potential competitor to Google's Android and Apple's iOS;[17]

- **Beyond core services:** In 2021, the VPNs included the same set of Google API permissions, including Google Fitness and Google Play Games services. While these permissions do not demonstrate data collection, they indicate these apps are allowed to request access to users' health, body measurement, and gaming data — revealing potential integration with third-party services that are not typically associated with VPN functionality.

[17] https://www.thebritishacademy.ac.uk/documents/6277/The_realignment_of_tech_supply_chains_lessons_from_US_trade_sanctions_against_Huawei.pdf



The addition of historical back-end connectivity data from Janus extends insights about the known VPN family beyond what front-end records alone can reveal and identified back-end links between Autumn Breeze and entities previously only associated with the Qihoo 360 family through business filings. When combined with open-source evidence, these findings led to another family-related company — expanding the previous cluster of VPNs from 16 to 27 apps. Qihoo 360's VPN apps are among the most popular in the world by downloads — at the time of this research, its 12 operating apps collectively accounted for 12.8 million downloads across the Google Play and Apple App stores, according to Sensor Tower data.



Source: Authors' analysis based on Janus findings, app stores metadata, Sensor Tower records, and Wayback Machine archived pages; with data from the Tech Transparency Project and VPNpro

These patterns do not, on their own, establish common ownership, but they do demonstrate how back-end connections can add depth and nuance to investigations by revealing different levels of technical relatedness between apparently distinct VPN services.

Case study II: Adding nuance to investigations of popular VPNs in Myanmar

In Myanmar, ecosystemic analysis can add depth to risk assessments and research on user adoption of VPNs in controlled environments. In 2021, a military coup led to high levels of internet censorship and government control on all modes of communication, leaving the local population reliant on VPN applications to access blocked online services like Facebook. Comparing three VPN applications developed by different providers and operating under distinct business models using back-end connectivity reveals differences in the external services and infrastructure to which user traffic may be directed.

Background

After the Myanmar military, known as the Tatmadaw, overthrew the civilian government in February 2021, the new regime blocked several internet sites including independent media websites, secure messaging app Signal, and services from Meta such as Facebook, Instagram, and WhatsApp. These restrictions have had a significant impact on daily life, as a large population only access the internet using mobile phones, and Facebook is used by millions of people in various social, political, and economic functions. In response, many ordinary users started using various VPN applications.

In May 2024, the regime set up a technology to block most types of VPNs as part of its intensified crackdown. Reportedly, this was based on technology from Jizhi (Hainan) Information Technology Company Limited, also known as Geedge Networks,[18] which has been known to provide blocking technology for authoritarian regimes.[19] In offline settings, the authority personnel have been checking civilians' phones for VPNs as a way to extort money, and arbitrarily detain users.[20] In 2025, the regime passed a Cyber Security Law[21] that allowed authorities to formally imprison citizens for using VPNs. In addition to these risks associated with using VPNs, inside Myanmar there is also a general concern that the military regime may be able to intercept users' data even while using a VPN.[22]

---

[18] https://www.accessnow.org/myanmar-vpn-ban/

[19] https://advox.globalvoices.org/2025/09/18/how-a-chinese-company-exports-the-great-firewall-to-autocratic-regimes/

[20] https://www.irrawaddy.com/news/burma/myanmar-junta-searching-phones-for-vpn-use.html

[21] https://connectontech.bakermckenzie.com/myanmar-cybersecurity-law-enacted-on-1-january-2025/

[22] https://www.irrawaddy.com/in-person/interview/war-on-citizens-how-juntas-vpn-ban-is-strangling-communication-in-myanmar.html

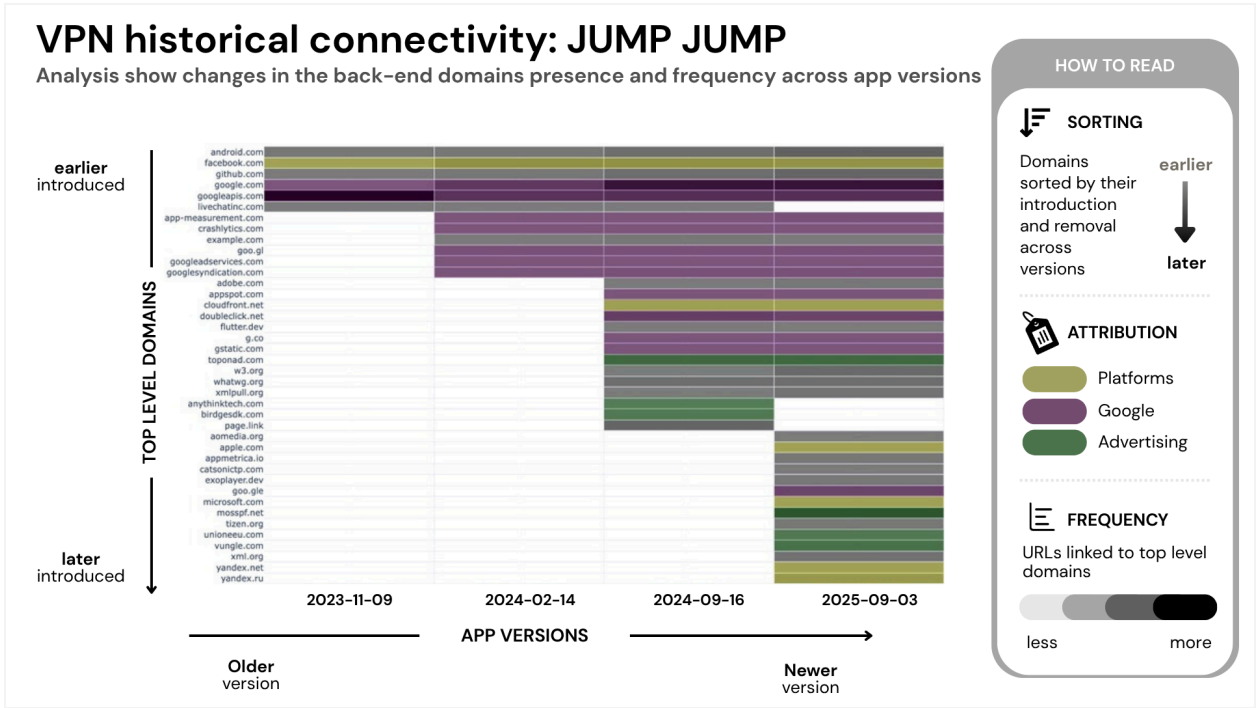
Myanmar: VPN Escalating Restrictions

- **Feb 2021**
  Following a military coup, major online platforms are blocked, driving widespread VPN use
- **May 2024**
  Regime deploys technology to block VPNs and begins inspecting citizens' phones for VPN apps
- **Jan 2025**
  A new Cyber Security Law introduces criminal penalties, including imprisonment, for VPN use
- **Today**
  Internet users continue to rely on VPNs that can still circumvent the regime's VPN block technology despite persecution

Users in Myanmar rely on VPNs to bypass censorship, and place considerable trust in providers to protect their privacy. Therefore, one of the most important questions for users assessing risks is: Do VPNs with different business models rely on different technical infrastructures, and where is user data potentially directed? Using Janus to compare the back-end connectivity of three of the most widely used VPN applications in Myanmar — Jump Jump, an ad-based freemium service that gained popularity after the coup; 1.1.1.1 Warp, a long-used commercial VPN; and Outline VPN, an open-source tool designed for activists and other high-risk users — to trace how dependencies evolved across historical app versions reveals significant differences that are not apparent from the apps' user-facing features alone.

Jump Jump VPN

Jump Jump VPN emerged as one of the widely used VPNs in Myanmar following the 2024 VPN ban and is, as of July 2026, ranked among the top ten apps on the Myanmar Google Play Store. Myanmar VPN Safety Guard, a local initiative that monitors VPN services available in the country, has flagged Jump Jump as insecure due to the lack of independent security audits and its freemium ad-based revenue model. The app is published by the Singapore-based Soon Bodywerkz Auto Pte Ltd, a company whose primary business is motor vehicle repair and maintenance, with software development listed as secondary activity. Besides Jump Jump, the company has published four apps on Google Play store: two other VPN apps, a video downloader and a game speed booster.



Our back-end connectivity analysis reveals that Jump Jump relies on a combination of standard Android components and web hosting packages along with platform services (highlighted in brown) from US big tech platforms such as Facebook, Apple, and Microsoft, as well as Russian social media Yandex. Google Services and its advertising domains are highlighted in purple. We also found many links hosted on Alibaba Cloud Computing such as anythinktech.com, birdgesdk.com, unioneeu.com, toponad.com, and mosspf.net, where some of them relate to the ad monetization services (green). In addition, we found vungle.com as another advertising monetization service.

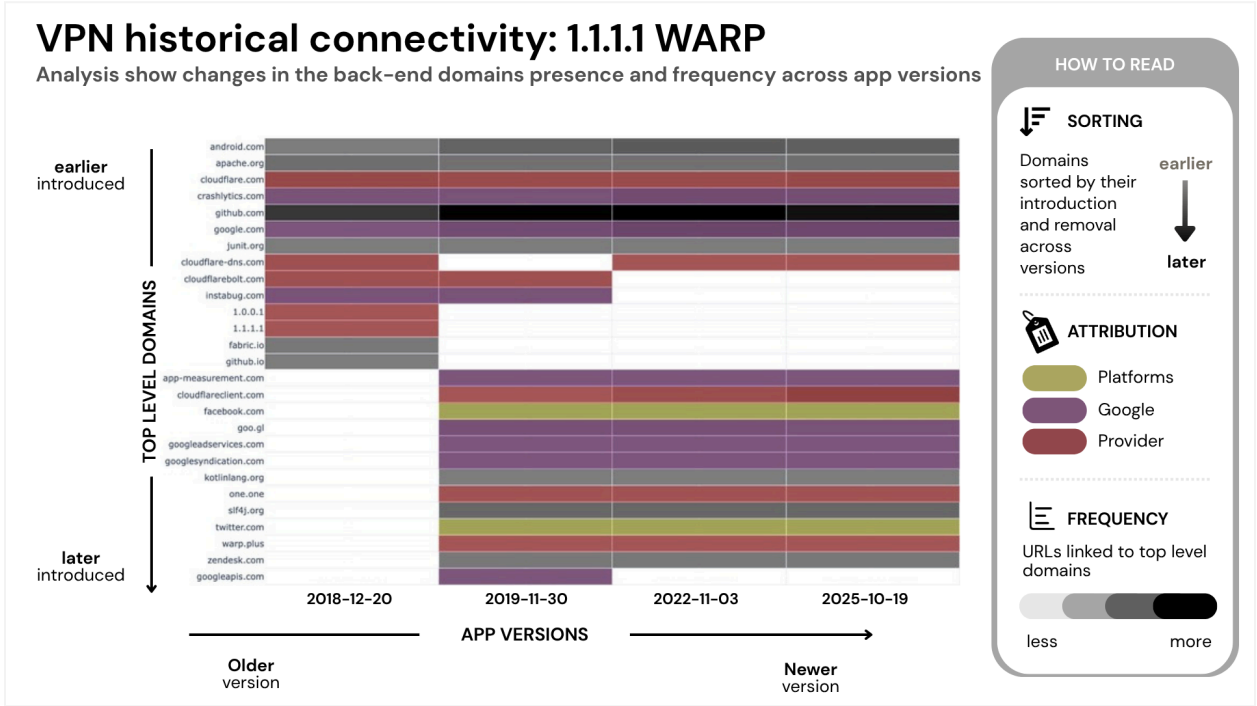
Jump Jump exhibits a diverse profile, with extensive dependencies on advertising, analytics, and social media services — characteristics consistent with its advertising-supported business model and contributing to its classification as insecure by specialist VPN monitoring initiatives. Back-end connectivity analysis reveals that Jump Jump relies on a combination of standard Android components and web hosting packages along with platform services from US big tech platforms such as Facebook, Apple, and Microsoft, as well as Russian social media Yandex and Alibaba Cloud Computing.
Critically, a historical view of back-end show Jump Jump's development trajectory toward ads-based revenue, implemented over three phases:

- **Phase I, Launch:** Launched as a free app with basic functionality in 2023.

- **Phase II, Monetisation:** The first wave of monetisation was added in 2024, where in the course of a few months we see different ad networks being added: Google Ads/Ad Sense, Google Syndication, TopOn Ad, AnyThink, DoubleClick, and Cloudfront.
- **Phase III, Expanded Connectivity:** In 2025, a new block of domains was added to the connectivity. unioneeu and mosspf are both registered to Alibaba; along with links to the Russian company Yandex, and Vungle.com (liftoff.ai), an advertising service for applications.

1.1.1.1 Warp

1.1.1.1 Warp is developed by the American tech solution company Cloudflare, Inc, which routes user traffic through its Cloudflare server. It was widely used in Myanmar after 2021 on account of its simple, easy interface, effectiveness, and free access, until the regime's VPN ban in May 2024, when it stopped working.

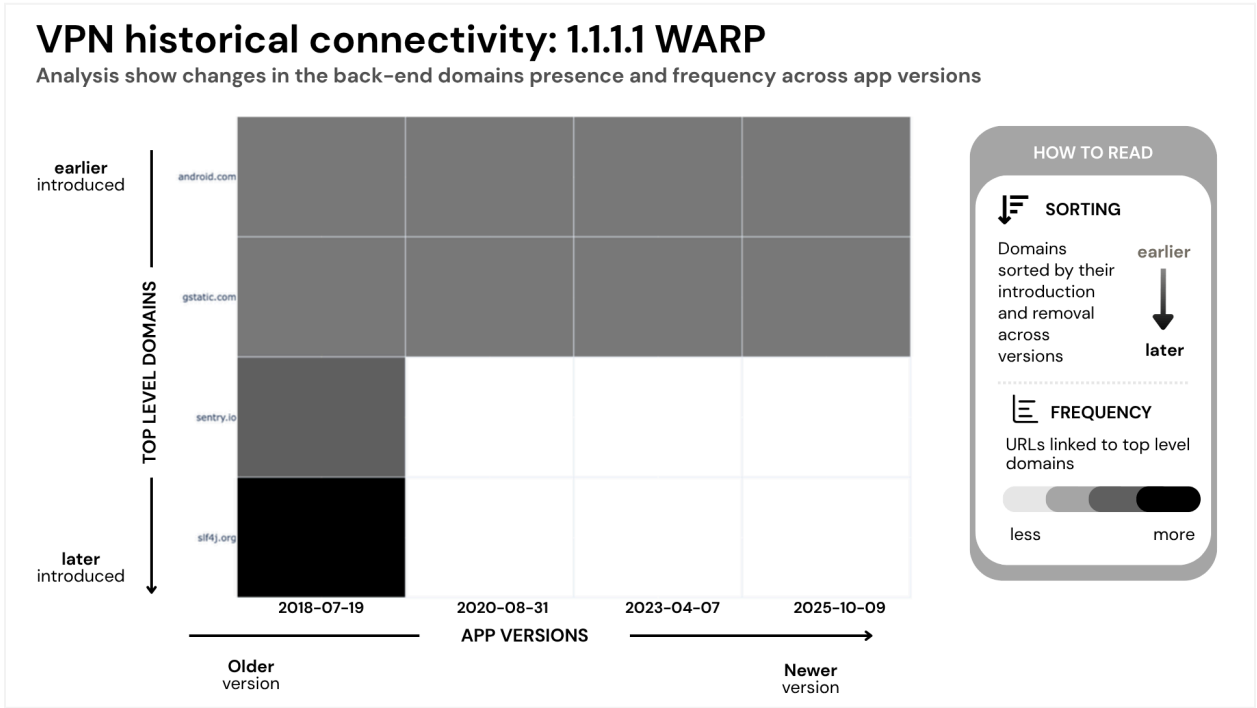


1.1.1.1 Warp relies primarily on provider-managed infrastructure, reflecting Cloudflare's mature and largely self-managed back-end ecosystem across its different versions over time. In contrast to Jump Jump, 1.1.1.1 Warp's back-end links lack services related to Chinese and Russian-based services such as Alibaba Cloud Computing and Yandex. Instead, the back end

links primarily to Cloudflare.com and Google services (including advertising), and relies on an ecosystem restricted to US technologies, analytics and advertising alongside open source software like Apache and GitHub.

Outline VPN

Outline VPN is a free and open access tool that allows users to set up their own VPN server. It was developed by the Outline Foundation, a non-profit organisation from Jigsaw, an incubator from within Google. The civil society and digital security trainers recommended the tool to activists and high-risk individuals seeking a more secure VPN option, and has reportedly remained working in Myanmar despite the regime's VPN firewall. Outline claims its focus on small-scale providers makes its services harder for censors to identify and block, although this approach introduces practical challenges when providers seek to serve larger numbers of users.[23] According to Outline's website, the tool is independently audited for security by Radically Open Security (2018, 2022) and Cure53 (2018, 2024).



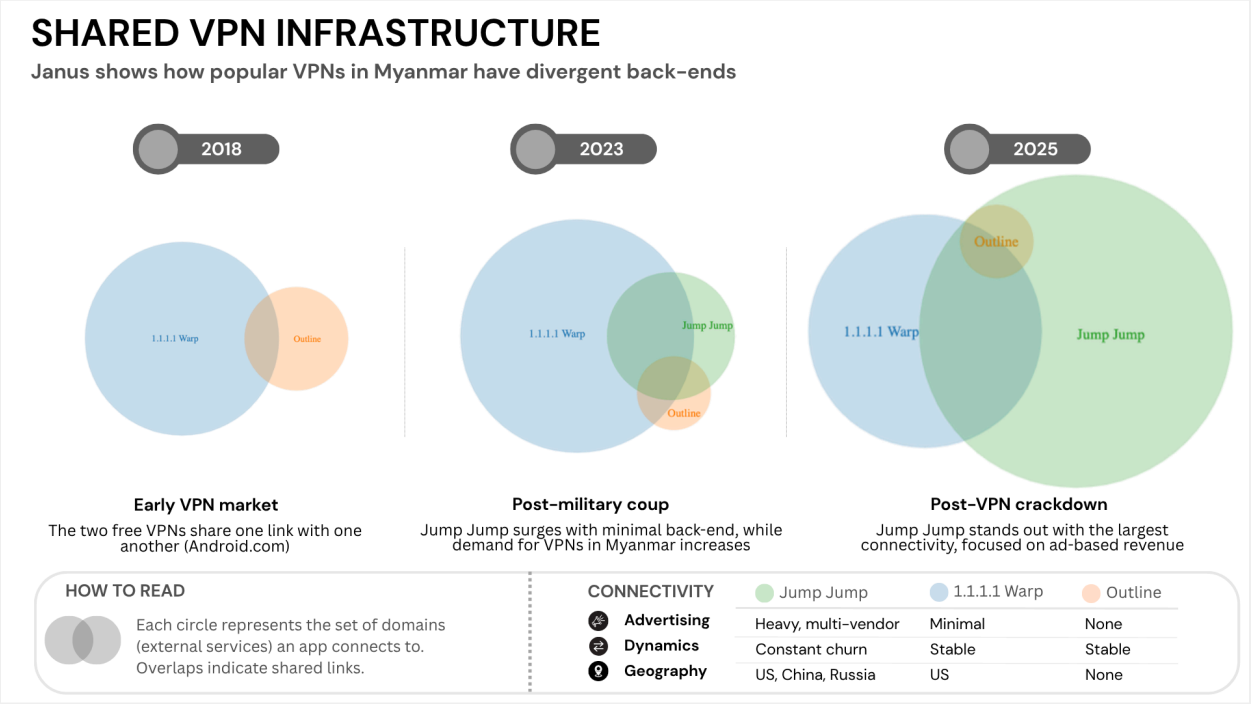
In contrast to the other VPNs analysed, Outline exhibits a significantly smaller and less complex back-end footprint. Janus analysis identified only four domains associated with the application, all related to Android software development. Therefore, it maintains minimal external dependencies, consistent with its privacy-oriented design. Unlike the other cases,

[23] https://okthanks.com/blog/2024/4/9/growing-with-the-people

any links to external big tech companies, analytics, or advertising do not exist. This simplicity suggests a lower risk of data leaks for a user.

Comparing VPN services

Taken together, these analyses of Myanmar's popular VPN apps reveal dependencies and suggest potential areas of risk. The back-end connectivity of the app versions in 2018, 2023, and 2025 illustrates how providers with different business models rely on markedly different technical ecosystems. Across the years, they share a core set of Android and Google components, yet their broader infrastructure diverges substantially. While Jump Jump is characterised by heavy use of ad Software Development Kits (SDK) from multiple vendors and a diverse geographical mix that expanded over time, 1.1.1.1 Warp presents a more stable and streamlined back-end profile, dominated by US-based providers and centred on 20 stable domains. Outline has the most minimal back-end footprint of the three, with its connectivity reduced to just two domains from 2023 onwards.

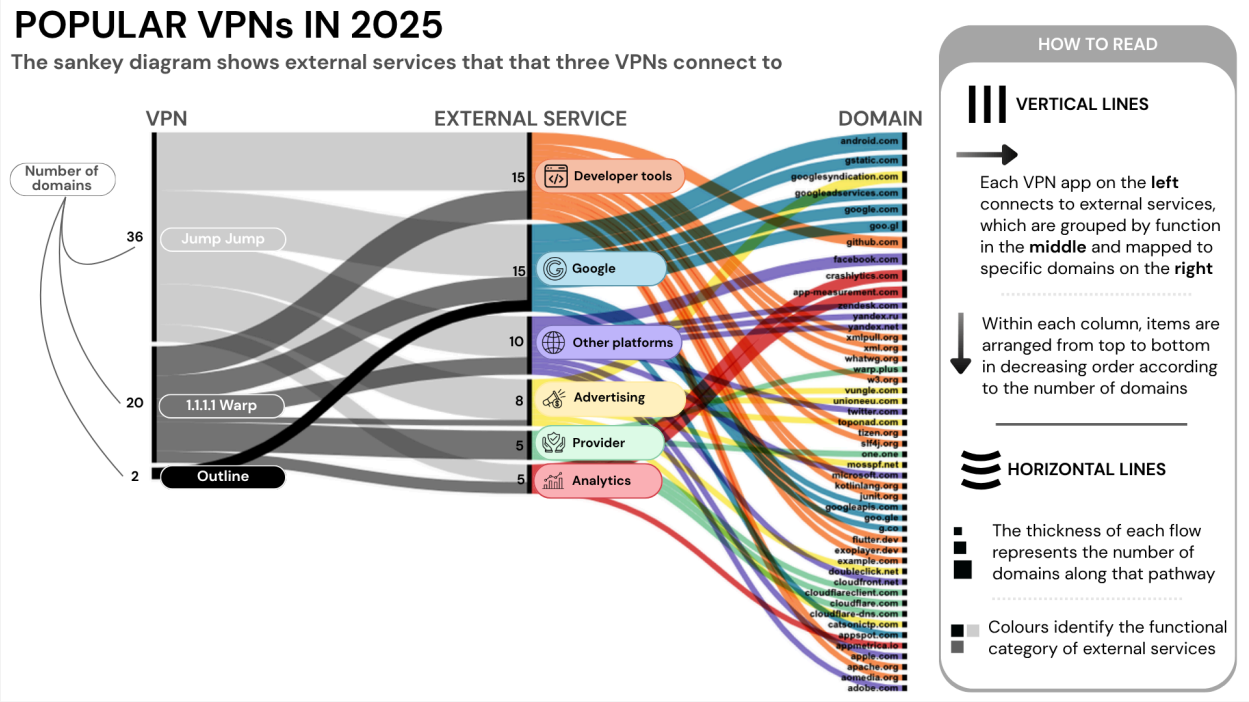


A closer view of the apps in their 2025 versions further illustrates the difference between the apps. In the sankey graph below, the middle vertical axis groups external services by function, showing how much each VPN (on the left) relies on specific domains (on the right), indicating how much a VPN might depend on third parties beyond its core functions.

On the one hand, we see developer tools and Google core services — which support the development, operation, and updating of the apps — as the most common categories of external connections across the three apps, which is unsurprising for Android applications.

On the other hand, the prevalence of platform services including social media and advertising, extensively linked in Jump Jump, raises questions about what data may be exposed to, or processed by, companies outside the VPN provider. The presence of connections to the provider's own infrastructure may also indicate a more mature service, while its absence, as in the case of Jump Jump, may point to higher dependency to third parties. Together, these signals offer more information with which to assess a VPN beyond its stated privacy claims. Although the changes that are happening at the back end of these

VPNs may not be directly related to the political events in Myanmar, we can draw connections between how different apps rise in popularity among users and how their back-end ecosystems evolve over time.



For users and digital security researchers, the ability to compare back-end connectivity profiles in this way opens up opportunities for further inquiry into the risks and benefits of

different kinds of VPNs — knowledge that can be invaluable in high-risk situations like Myanmar.

Connecting evidence

Digital forensic approaches provide valuable evidence for investigating VPN services, but no single method can establish ownership, trustworthiness, or privacy risks on its own. Instead, robust investigations combine multiple sources of evidence — each with their own strengths and limitations — as well as contextual knowledge that only expertise in the topic could provide, such as common practices in a given market, regulatory events driving changes, or insider information. Similarities in privacy policies or source code may result from copied documentation, shared third-party developers, or the re-use of open-source components rather than common ownership. Additionally, corporate registration or domain hosting in a particular jurisdiction does not necessarily indicate operational control from that country, although such evidence may become more significant when considered alongside other indicators discussed above. Furthermore, as the marketplace continues to expand in response to shifts in the regulatory environments, data sources might be available only under paywalls or deliberately obscured for public scrutiny.

The analysis of back-end connectivity also has important technical limitations. Its primary source of analysis is currently limited to Android applications, where APK installation files make hard-coded URLs accessible for inspection, whereas equivalent iOS application packages are not publicly available. Even for Android, historical coverage depends on the availability of archived APKs in open repositories such as Androzoo or user-contributed datasets.

Finally, APK analysis identifies the external domains, services, and software components an application is capable of communicating with, but it does not reveal what data is actually transmitted, whether those connections are actively used, or how information is processed once it reaches a third-party service. Some connections are only created while the app is running or in response to specific user actions, meaning they cannot always be identified through static analysis alone. Answering these questions requires complementary approaches, such as network traffic analysis or server-side investigation. Developers may also employ code obfuscation techniques that conceal back-end connections, although we did not observe such practices in the VPN applications analysed in this report.

Interpreting Janus Findings

Janus can reveal...

- Shared back-end infrastructure
- Third-party dependencies
- Historical changes in connectivity
- Technical relationships between apps
- New infrastructure appearing over time
- Static connections found in APKs
- Indicative patterns shared across Android app and its iOS counterpart

Janus cannot determine...

- What data are actually transmitted
- Whether a connection is actively used
- How providers process data after it reaches a domain
- Ownership from hard-coded URLs alone
- Intent or legitimacy of a provider
- Dynamic connections created when an app is running
- Connections that may exist only in iOS counterpart

Conclusion

As VPNs continue to play a critical role in protecting access to information in restrictive environments, the ability to investigate their technical ecosystems becomes increasingly important. Understanding VPNs requires looking beyond their user-facing interfaces to examine the broader ecosystems they are in, including market concentration and infrastructural dependencies that shape how these services operate.

Tools like Janus, which analyse back-end connectivity across historical VPN app versions, can complement corporate records, app-store metadata, privacy policies, and other open-source sources using technical evidence. In the Qihoo 360 case, back-end connectivity analysis uncovered technical relationships among seemingly independent VPN applications, revealing shared infrastructure and potential links between operators. Whereas in Myanmar, it provided evidence to substantiate recommendations about technology use within a specific market — helping assess the security implications of different VPN options.

Building on this report's findings, we recommend that practitioners incorporate back-end connectivity analysis into broader digital forensic investigations of VPN services by:

Treating VPNs as ecosystems:

- Considering related apps, developers, parent companies and shared infrastructure reveals connections between apparently independent VPNs;
- Comparing the back-end ecosystems of several VPNs provides a quicker way to identify patterns and outliers;

Using multiple signals:

- Combining app-store metadata, ownership records, privacy policies, back-end connectivity and security expert blacklists provides a stronger evidence base than relying on any single indicator;
- Identifying red flags in VPN services helps prioritise further investigation into clusters of apps and areas of concern. Extensive advertising infrastructure, unexplained third-party connections, changing ownership or publisher information, and links across large VPN families can indicate areas requiring closer scrutiny;

Tracking relationships over time:

- Observing changes in publishers, domains, infrastructure and third-party services reveals relationships that a snapshot of a current app would miss;
- Analysing historical app versions shows how VPN ecosystems and their dependencies evolve over time, supporting ongoing digital rights and regulatory work.

Ultimately, these signals provide a pathway from asking whether a service is trustworthy to investigating who operates it, what it depends on, how its infrastructure evolves, and what other risks may emerge around it. Beyond VPNs, the same approach can support investigations into emerging issues such as age-verification requirements, platform restrictions, and data protection regulations, helping us better understand the technologies and infrastructures that increasingly shape our everyday lives.





1 September 2026

Janus Report