Choosing a Secure eSIM for International Travel

The Problem:

Many modern smartphones are moving away from physical SIM cards and increasingly rely on eSIM technology. Even devices that still include a physical SIM slot typically support eSIMs as well. This shift makes it easier for users to switch mobile carriers or add temporary cellular service when traveling internationally.

However, the growing number of low-cost eSIM resellers has created uncertainty about how user data is routed. Recent research indicates that many of these resellers do not own their own network infrastructure. Instead, they rely on centralized breakouts and sponsor networks, which may route traffic through locations far from the user. In some cases, traffic is routed through China or other parts of Southeast Asia even though the user is far from that part of the world. Additionally, becoming an eSIM reseller often requires little more than an email address and a credit card, with no identity verification process in place which can lead to the proliferation of low-quality and untrustworthy eSIM resellers. (See Resources below.)

The Concern/Risk:

The primary concern is that governments who do not respect privacy rights could work with local telecommunications providers in other countries to monitor communications by routing cell traffic from local eSIM resellers through infrastructure that enables monitoring. This could include intercepting data, reading text messages or listening to phone calls. While this risk of intercepting data (through either lawful or unlawful methods) is generally understood locally in any given country, the growth of eSIM resellers adds an additional layer of uncertainty because there is little transparency about which countries a user's data is routed through. The fact that cellular network traffic may be routed through China or other Southeast Asian countries may raise concerns for some users.

Additional concern stems from reports that China has had success in hacking foreign telecommunications companies for many years, a pattern which may be repeated by other governments. (See Resources below.) Beyond broad surveillance, there is the possibility that hostile governments could track specific individuals by referencing their IMEI numbers (the unique identifiers assigned to each mobile device) allowing targeted monitoring of communications or location tracking even on infrastructure outside of their direct control.

Recommendations:

We recommend purchasing eSIMs directly from major Mobile Network Operators (MNOs), because they typically operate their own core networks and maintain established points of presence worldwide. As a result, they are less likely to rely on virtual arrangements that route data through arbitrary and unspecified jurisdictions.

If purchasing an eSIM through a reseller, users should select providers that demonstrate a clear commitment to transparency in data routing practices and strong safeguards for data privacy and security. We strongly suggest against purchasing eSIMs from cheap resellers, such as the many popular ones like Airalo, Holafly, Nomad, Yesim, BNESIM, etc.

By Corey Keating
C.Keating@EriciusSecurity.org

List of Suggested eSIM Providers:

1) **eSIM providers focused on transparency, privacy, and security:**
   a) **Saily**: saily.com - Owned by a Lithuanian company; traffic routed regionally and through Western nations. From creators of NordVPN. Uses 1GLOBAL (formerly Truphone) as network provider. Includes privacy tools like a virtual location feature, an ad blocker, and web protection.
   b) **Ubigi**: cellulardata.ubigi.com - Owned by a French company; traffic routed through France and Japan (higher privacy jurisdictions). Allows a client side "Country of Residence IP" (selected during registration). It allows the user to choose where their cell-network traffic will appear to be coming from.
   c) **GigSky**: www.gigsky.com - Owned by a US company; traffic routed regionally and through US.
   d) **Roamless**: roamless.com - Owned by a US company; traffic routed regionally and through US.
2) **If you have an international data plan through your primary mobile provider based in the US, UK, or EU**, it likely maintains established agreements with local and regional MNOs to handle roaming traffic. This means your data should be routed through defined network pathways between the country where you are located and its destination, rather than being redirected through an unspecified third country. This should be adequate security for most people. However, there is little transparency required surrounding this topic, so there are no guarantees.
3) **Global Mobile Network Operators that offer eSIMs to travelers:**
   These global Mobile Network Operators (based in the UK or EU) operate in a higher-privacy jurisdiction, subject to GDPR. As mentioned above, they most likely have established agreements with local operators and traffic should be routed accordingly, not through an unspecified third country. Purchasing eSIMs through these companies should provide adequate security for most people.
   a) **Orange (Travel)**: https://travel.orange.com/en - Owned by a French company.
   b) **Vodafone**: https://travel.vodafone.com/ - Owned by a UK company.

Resources:

1) **News Articles**: These two news articles, summarize the "eSIMplicity …" research report listed below. Adequate for overview without reading entire report:
   a) "Study Exposes How Travel eSIMs Reroute Data Through China — and Let Anyone Become a Reseller" alertify.eu/silent-esim-connections/
   b) "Travel eSIMs secretly route traffic over Chinese and undisclosed networks: study" www.itnews.com.au/news/travel-esims-secretly-route-traffic-over-chinese-and-undisclosed-networks-study-619659
2) **Research**: The full report where these news articles are coming from: "eSIMplicity or eSIMplification? Privacy and Security Risks in the eSIM Ecosystem" (Aug. 2025)
   a) Slides (as a summary): www.usenix.org/system/files/sec25_slides_motallebighomi.pdf
   b) Full Report: www.usenix.org/system/files/usenixsecurity25-motallebighomi.pdf
3) **Telecom Hacking by China**:
   a) "China used three private companies to hack global telecoms, U.S. says" (Aug. 2025) www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543 -- "An FBI spokesperson told NBC News that Salt Typhoon has hacked more than 200 companies across 80 countries."
   b) "Singapore says China-linked hackers targeted telecom providers in major spying campaign" (Feb. 2026) therecord.media/singapore-attributes-telecoms-hacks-unc3886
   c) "At least 8 U.S. telecom firms were hit by China's hacking campaign, White House says" (Dec. 2024) www.pbs.org/newshour/world/at-least-8-u-s-telecom-firms-were-hit-by-chinese-hacking-campaign-white-house-says