Finding You

The Network Effect of Telecommunications Vulnerabilities for Location Disclosure

By Gary Miller and Christopher Parsons

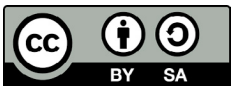
OCTOBER 26, 2023
RESEARCH REPORT #171

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright



Electronic version first published by the Citizen Lab in 2023. This work can be accessed through https://citizenlab.ca/2023/10/finding-you-telecommunications-vulnerabilities-for-location-disclosure/.

Document Version: 1.1
- Figure 7 was updated with additional redactions.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

About the Authors

Gary Miller contributed to this report while a Researcher at the Citizen Lab. He is currently the Founder of the Mobile Intelligence Alliance, a US-based non-profit mobile security research organization, a former mobile network security executive, and regarded as an expert in mobile network espionage. He received his BA in Economics from the University of Washington and is a contributor in mobile espionage investigative journalism research with major global news outlets.

Christopher Parsons contributed to this report while he was a Senior Research Associate at the Citizen Lab, in the Munk School of Global Affairs & Public Policy at the University of Toronto. He received his Bachelor's and Master's degrees from the University of Guelph and his PhD from the University of Victoria. He is currently an A/Manager, Technology Policy at the Information and Privacy Commissioner of Ontario.

Acknowledgements

We would like to thank civil society organizations, investigative journalists, and mobile network security experts who graciously agreed to contribute their insights and share forensic artifacts in the course of developing this report.

We want to specifically thank Siena Anstis, Kate Robertson, Jakub Dalek, Celine Bauwens, Levi Meletti, and Mohamed Ahmed for their thoughts and expertise, edits, and peer review of this report.

Additionally, we would like to thank Mari Zhou for her design and publishing assistance and Snigdha Basu for her communications support. This report was undertaken under the supervision of Professor Ronald Deibert.

Corrections and Questions

Please send all questions and corrections to: inquires@citizenlab.ca.

Suggested Citation

Gary Miller and Christopher Parsons. “Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure,” Citizen Lab Research Report No. 171, University of Toronto, October, 2023.

Information Boxes

Contents

Introduction

The information collected by, and stored within, mobile networks can represent one of the most current and comprehensive dossiers of our life. Our mobile phones are connected to these networks and reveal our behaviours, demographic details, social communities, shopping habits, sleeping patterns, and where we live and work, as well as provide a view into our travel history. This information, in aggregate, is jeopardized, however, by technical vulnerabilities in mobile communications networks. Such vulnerabilities can be used to expose intimate information to many diverse actors and are tightly linked to how mobile phones roam across mobile operators' networks when we travel. Specifically, these vulnerabilities are most often tied to the signaling messages that are sent between telecommunications networks which expose the phones to different modes of location disclosure.

Telecommunications networks have been designed to rely on private, though open, signaling connections. These connections enable domestic and international roaming, where a mobile phone can seamlessly pass from one company's network to another. The signaling protocols used for this purpose also allow networks to retrieve information about the user, such as whether a number is active, which services are available to them, to which country network they are registered, and where they are located. These connections and associated signaling protocols, however, are constantly being targeted and exploited by surveillance actors with the effect of exposing our phones to numerous methods of location disclosure.

Most unlawful network-based location disclosure is made possible because of how mobile telecommunications networks interoperate. Foreign intelligence and security services, as well as private intelligence firms, often attempt to obtain location information, as do domestic state actors such as law enforcement. Notably, the methods available to law enforcement and intelligence services are similar to those used by the unlawful actors and enable them to obtain individuals' geolocation information with high degrees of secrecy. Over the course of this report we will generally refer to all of these actors as 'surveillance actors' to refer to their interest in undertaking mobile geolocation surveillance.

Despite the ubiquity of global 4G network penetration and the rapidly expanding 5G network footprint there are many mobile devices, and their owners, who rely on older 3G networks. This is particularly the case in the regions of Eastern Europe, the Middle East, and Sub-Saharan Africa where 3G subscriber penetration is 55% according to the GSMA[1], an organization that provides information, services, and guidelines to members of the mobile industry. Further, at the end of 2021 the UK-based mobile market intelligence

1 Kenechi Okeleke, Harry F. Ballon, and James Joiner. (2023). *The Mobile Economy 2023*. https://data.gsmaintelligence.com/research/research/research-2023/the-mobile-economy-2023

firm Mobilesquared estimated that only a quarter of mobile network operators worldwide have deployed a signaling firewall[2] that is designed to impair geolocation surveillance. Telecom insiders understand that the vulnerabilities in the SS7 signaling protocol used in 3G roaming have enabled the development of commercial surveillance products that provide their operators with anonymity, multiple access points and attack vectors, a ubiquitous and globally-accessible network with an unlimited list of targets, and virtually no financial or legal risks.

This report provides a high-level overview of the geolocation-related threats associated with contemporary networks that depend on the protocols used by 3G, 4G, and 5G network operators, followed by evidence of the proliferation of these threats. **Part 1** provides the historical context of unauthorized location disclosures in mobile networks and the importance of the target identifiers used by surveillance actors. **Part 2** explains how mobile networks are made vulnerable by signaling protocols used for international roaming, and how networks are made available to surveillance actors to carry out attacks. An overview of the mobile ecosystem lays the foundation for the technical details of domestic versus international network surveillance, while the vectors of active versus passive surveillance techniques with evidence of attacks shows how location information is presented to the actor. **Part 3** provides details of a case study from a media report that shows evidence of widespread state-sponsored surveillance, followed by threat intelligence data revealing network sources attributed to attacks detected in 2023. These case studies underscore the significance and relevance of undertaking these kinds of surveillance operations.

Deficiencies in oversight and accountability of network security are discussed in **Part 4**. This includes outlining the incentives and enablers that are provided to surveillance actors from industry organizations and government regulatory agencies. **Part 5,** makes clear that the adoption of 5G technologies will not mitigate future surveillance risks unless policymakers quickly move to compel telecommunications providers to adopt the security features that are available in 5G standards and equipment. If policymakers do not move swiftly then surveillance actors may continue to prey upon mobile phone users by tracking their physical location. Such a future paints a bleak picture of user privacy and must be avoided.

2 Mobileum, Mobilesquared. (2021). The State of the Signaling Firewall Landscape November 2021. https://www.mobilesquared.co.uk/wp-content/uploads/2023/04/Mobileum_Security-Research_Nov21-FINAL-VERSION.pdf

1. Roaming, SIMs, and Services 101

Mobile users expect their phones to work wherever they travel beyond the borders of their home country. However, it is when individuals are traveling abroad that they are most vulnerable to network-based geolocation tracking.

When an individual travels internationally with a mobile phone, the phone continues to operate outside of its home mobile network (i.e., the domestic carrier with which it is associated). This ongoing operation is accomplished through a series of global inter-connections and agreements between network operators around the world. These interconnections and agreements are often unique to each network type (3G, 4G, and 5G) and these networks have historically been bridged by telephony signaling protocols which have been developed since the 1970s to form the Signaling System Number 7 (SS7 network), and subsequently the Long Term Evolution (LTE/4G) network which uses the Diameter signaling protocol.

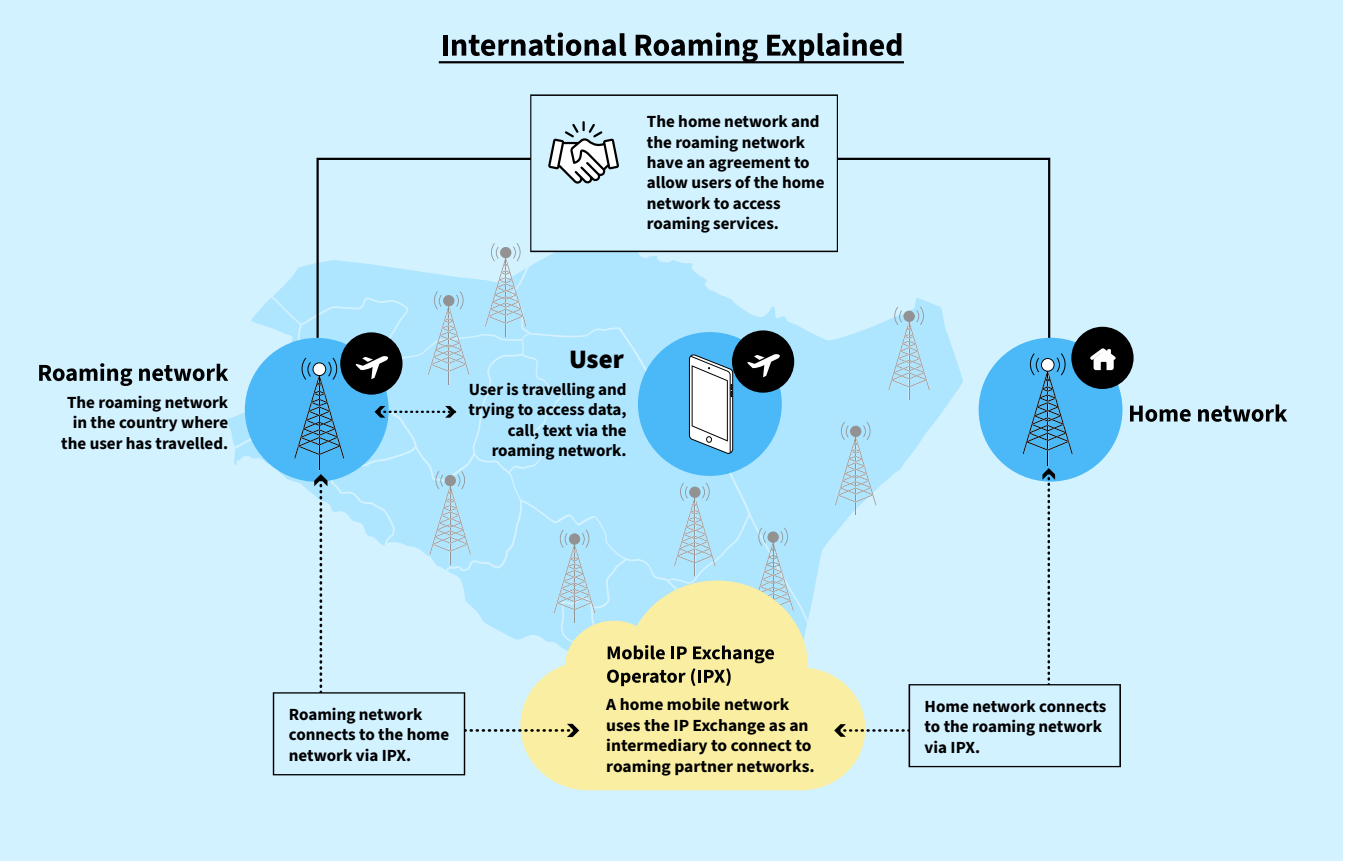


Figure 1: International roaming process flow.

When roaming on different foreign networks, those networks charge differing rates for voice, data, and messaging services in exchange for the services provided to users roaming on their networks. To enable these services, the involved network operators open their networks to one another so they can interoperate. It is this interoperation

that allows individuals to seamlessly make calls, send text messages, or use data while roaming on a foreign network.

Generally speaking, wholesale roaming agreements, such as the information included in the GSMA framework,[3] are used to establish the commercial and operational aspects of sending and receiving signalling messages for service exchange between network roaming partners. Signaling messages are operator-to-operator messages that are used to authenticate and manage user mobility. Functionally, operators use signaling messages to establish and maintain sessions providing services to users. However, while security best practices state that mobile network operators should reject messages sent by non-roaming partners or prevent abusive messages from exposing users to location tracking, these practices are not mandatory or enforced. This voluntary aspect of operator-to-operator signaling message security provides surveillance actors with an entry path into the target network. Further, networks typically connect to at least two network operators per country (and often many more) to minimize roaming costs and maximize network resiliency. While these open connections are a prerequisite for roaming service enablement they have also presented risks to geolocation tracking.

1.1. From SIM to Services - Creating the Path to Network Surveillance

Understanding the points of vulnerability that surveillance actors exploit to track user geolocation requires an understanding of how users are globally and uniquely identified on mobile networks. These identifiers play a critical role in the process of routing and delivering the malicious geolocation tracking messages from the surveillance actor's software to the network of the target phone, and returning the information back to the actor.

A starting point for understanding the identity of a user's phone is when the mobile network operator issues the SIM card. While we are accustomed to inserting the ever-smaller cards into mobile devices, these physical cards are rapidly being displaced by a software-based eSIM. Both physical- and software-based SIM cards use a unique identity called the Integrated Circuit Card ID (ICCID). Mobile network operators then use the ICCID to assign a globally unique network identity that is specific to that network operator, known as the International Mobile Subscriber Identity (IMSI), during service activation. This globally unique and network-specific IMSI is the crucial element in the context of delivering services to the phone from any global roaming network. The IMSI is, also, central to the targeting methods that are used in geolocation tracking operations that are sourced from foreign networks.

3 Relevant GSMA international roaming agreements include AA.12, AA.13, and AA.14

After the SIM or eSIM is provisioned to the user account, a phone number—which is referred to by the telecommunications industry as the Mobile Station International Subscriber Directory Number (MSISDN)—is also mapped to the IMSI that is defined by the network operator. This combined information—the MSISDN and the IMSI—is integrated into the network operator's service delivery, authorization, and authentication systems. Key to these systems is the 3G/4G Home Subscriber Service/Home Location Register (HSS/HLR) and 5G Unified Data Manager (UDM), which are collectively master databases containing the rules to authorize services associated with the subscription plan an individual has purchased on a monthly or pay-as-they-go basis.

Having fully assigned and provisioned the SIM, the mobile device can communicate with the operator's network for phone calls, text messages, and application data that can be routed globally. It is, also, at this point that malicious signaling messages can be directed towards the device with the effect of exposing its geolocation.

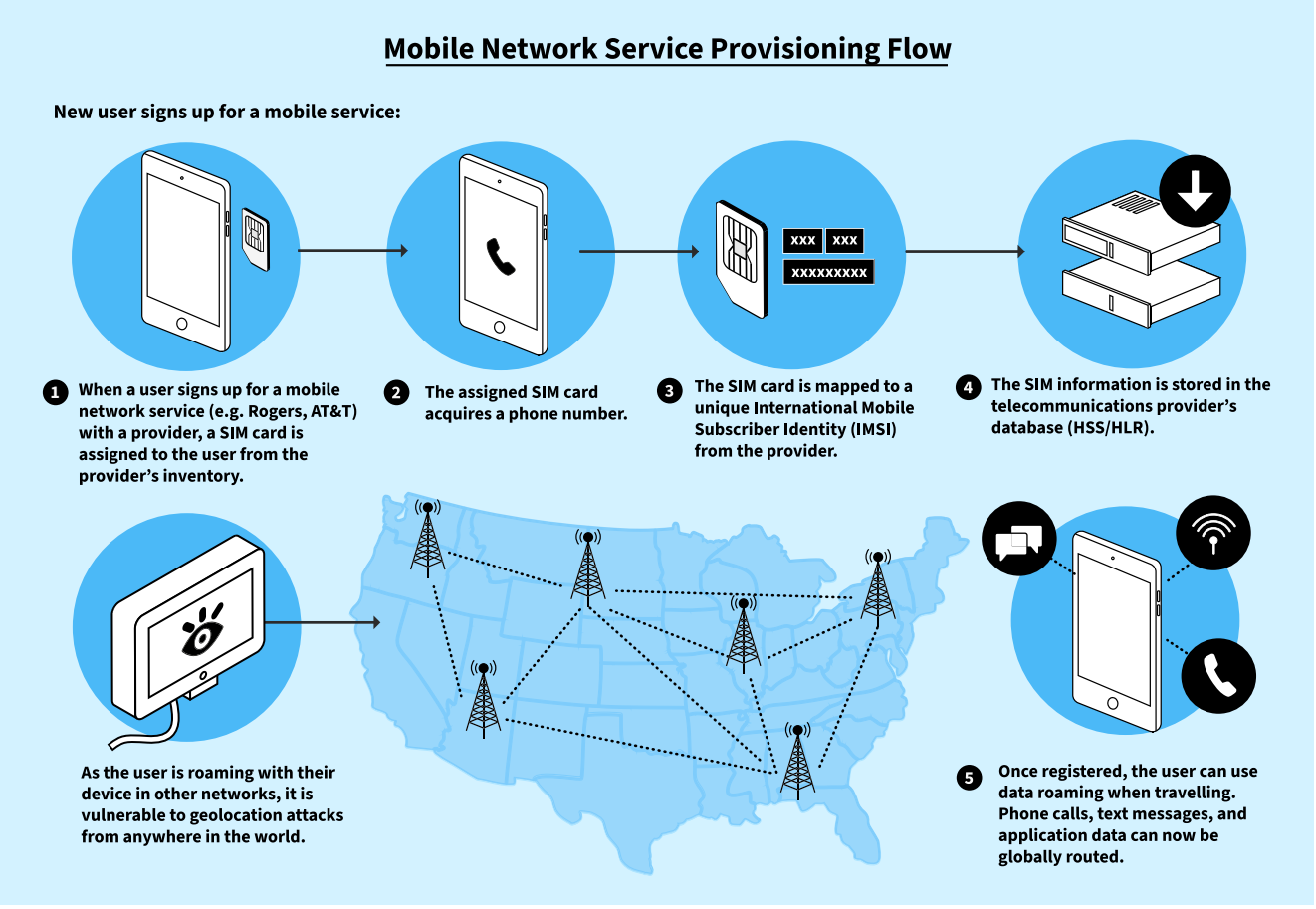


Figure 2: How mobile identities are provisioned to enable surveillance operations.

The IMSI of the target phone is a critical information element for conducting surveillance and is frequently seen in the initial procedure of the operation to locate its Cell ID, which

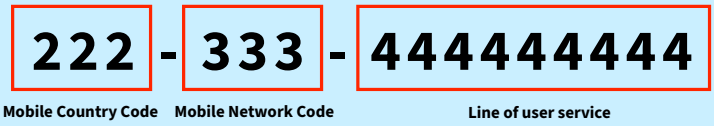
is the unique number used to identify a base station tower of a given network. The Cell ID can then be correlated to a location using one of many Cell ID database services.[4]

Information Box 1: The IMSI Network Identifier Explained

Networks use either 3G/4G identities or 5G identities. 3G and 4G networks use the IMSI, which typically include 15 digits, such as the following example:

- 222-333-444444444
- The first 3 digits (222) are the mobile country code (MCC)
- The next 2–3 digits (333) are the mobile network code (MNC).
- The remaining digits (444444444) identify the line of the user service.

International Mobile Subscriber Identity (IMSI)



In contrast, 5G networks have defined the Subscription Permanent Identifier (SUPI) instead of IMSIs. The SUPI is equivalent to the IMSI to ensure compatibility with 4G network infrastructure. Such compatibility is particularly important because 4G network infrastructure underpins a majority of current 5G international roaming.

5G adds a security feature called the Subscription Concealed Identifier (SUCI), with an encryption scheme to prevent the open transmission of the user network identity over the radio interface. This has the effect of foiling surveillance actors who have physical proximity to a mobile device and use tools such as IMSI Catchers to intercept radio communications in order to forcibly reveal a device's IMSI number. IMSI Catchers are used by a variety of actors, including law enforcement, security, and foreign intelligence agencies, as well as criminals, to obtain the network identity of users for surveillance purposes.[5]

4 Many commercial and public Cell ID database services are available: https://en.wikipedia.org/wiki/GSM_Cell_ID.

5 For more about IMSI Catchers, see: Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada." *Citizen Lab and CIPPIC.* Available at: https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf.

2. Geolocation Attacks Against Telecommunications Networks

This report principally focuses on geolocation threats that result from targeting mobile signaling networks. Surveillance actors can utilize either active or passive surveillance methods to obtain information from mobile signaling networks, with the effect of exposing a user's location. In some cases they may combine multiple methods to accomplish this goal.

The distinction between the two approaches is notable. Active surveillance implies that an actor uses software to engage with a mobile network to elicit a response with the target phone location, whereas passive surveillance uses a collection device to obtain the location of phones directly from the network. When it comes to active attacks, an adversarial network uses software to send crafted signaling messages to vulnerable target mobile networks to query and obtain a current geolocation of the target phone. Such attacks are possible where the targeted networks do not have properly deployed or configured security controls. Further, an actor accessing a network through a lease arrangement can only use active surveillance methods unless they have the ability to install, or otherwise access, passive collection devices located in networks around the world.

There is, however, the possibility that a mobile operator or other actors could be compelled to undertake both active and passive surveillance. In this situation, the network operator may either be legally compelled to facilitate surveillance or, alternately, suffer from a hostile insider who is accessing mobile systems illicitly or illegally. Further, should a third-party gain access to the operator or provider, such as by compromising VPN access into the targeted network systems, they may be able to obtain location information of targeted users in both active and passive modes.

2.1 Active Attacks

In cases of active attacks, a domestic or foreign surveillance actor uses software to issue signaling messages which are directed at the target user's mobile phone identity (commonly the IMSI) by manipulating the network signaling data to trigger a response from the target user's home network. Such surveillance measures can be used to facilitate other communications interception, location disclosure, or service interruption. In this section, we discuss how actors may gain access to networks for geolocation tracking as well as some of the vulnerabilities that can subsequently be exploited by surveillance actors that are undertaking active surveillance operations.

2.1.1 How Actors Access Networks For Geolocation Tracking

Network-based geolocation tracking most commonly involves three interlinked elements:

1. specialized surveillance software;
2. a signaling address that is used to route malicious messages to the target network(s) so as to extract the targeted device's geolocation data;
3. network connectivity to the global 3G SS7 and 4G Diameter network.

This global SS7 or Diameter network backbone is known as the IP Exchange (IPX). The purpose of the IPX is to facilitate interconnection between mobile operator networks for the transport of signaling messages according to agreed interoperable service definitions and commercial agreements.[6] Further, the IPX architecture states that only service providers that are mobile network operators can connect to the network.[7] Therefore, third-parties who are not part of the mobile network operator community should not be allowed to connect and send mobile signaling messages, where vulnerabilities can expose mobile users to unauthorized geolocation surveillance.

Connections by surveillance actors to the IPX network are generally accomplished through covert commercial arrangements with a mobile operator, intermediary IPX transit, or other third-party service providers, such as SMS messaging providers, private mobile network operators, or sponsored Internet of Things service providers that possess connections to the IPX. While the IPX is designed to enable network roaming between different operators' networks it can also be abused to enable surreptitious geolocation surveillance. The IPX is used by over 750 mobile networks[8] spanning 195 countries around the world.[9] There are a variety of companies with connections to the IPX which may be willing to be explicitly complicit with, or turn a blind eye to, surveillance actors taking advantage of networking vulnerabilities and one-to-many interconnection points to facilitate geolocation tracking.

It is possible for mobile telecommunications companies to 'lease' access to their networks. This has the effect of significantly expanding the number of companies which may offer access to the IPX for malicious purposes. Moreover, a lessee can further sublease access to the IPX with the effect of creating further opportunities for a surveillance actor to use an IPX connection while concealing its identity through a number of leases and subleases.

In more detail, telecommunications operators in a given country apply for, and are allocated, bulk telephone number ranges according to a numbering plan as administered

6 GSMA Document IR.34 - Guidelines for IPX Provider Networks, Section 3 "IPX Network Architecture"

7 GSMA Document IR.34, Section 3.5

8 *About the GSMA - Represents the interests of mobile operators worldwide.* (2023, June 12). About Us. https://www.gsma.com/aboutus

9 *Member States.* (n.d.). United Nations. https://www.un.org/en/about-us/member-states

by their national telecommunications regulatory authority. These ranges are often used for a variety of purposes such as fixed line telephones, mobile numbers, or toll free numbers. Once the operator is allocated numbers, they can assign and use a portion of numbers as addresses, known as Global Title Addresses (GT), to equipment in their networks that are needed to operationalize domestic and international roaming with other network partners. This includes equipment such as the Visitor Location Register (VLR), Home Location Register (HLR), and other core network equipment.

The operators may, also, assign these GTs to third-party lessees. A malicious lessee may:

- configure surveillance software to use the leased GTs to conduct their own surveillance;
- use the GTs in a cloud-hosted solution to provide a commercial surveillance service;
- further partition the GT's for subleasing to other surveillance actors.

Notably, a surveillance actor can potentially lease GTs from either a single telecommunications operator or a range of operators from different jurisdictions. In this latter case, the surveillance actor may rotate attacks between the various subleased GTs either to try and avoid detection or to increase the likelihood of a successful operation if attacks from some of the subleased GTs happen to be blocked by network firewalls.

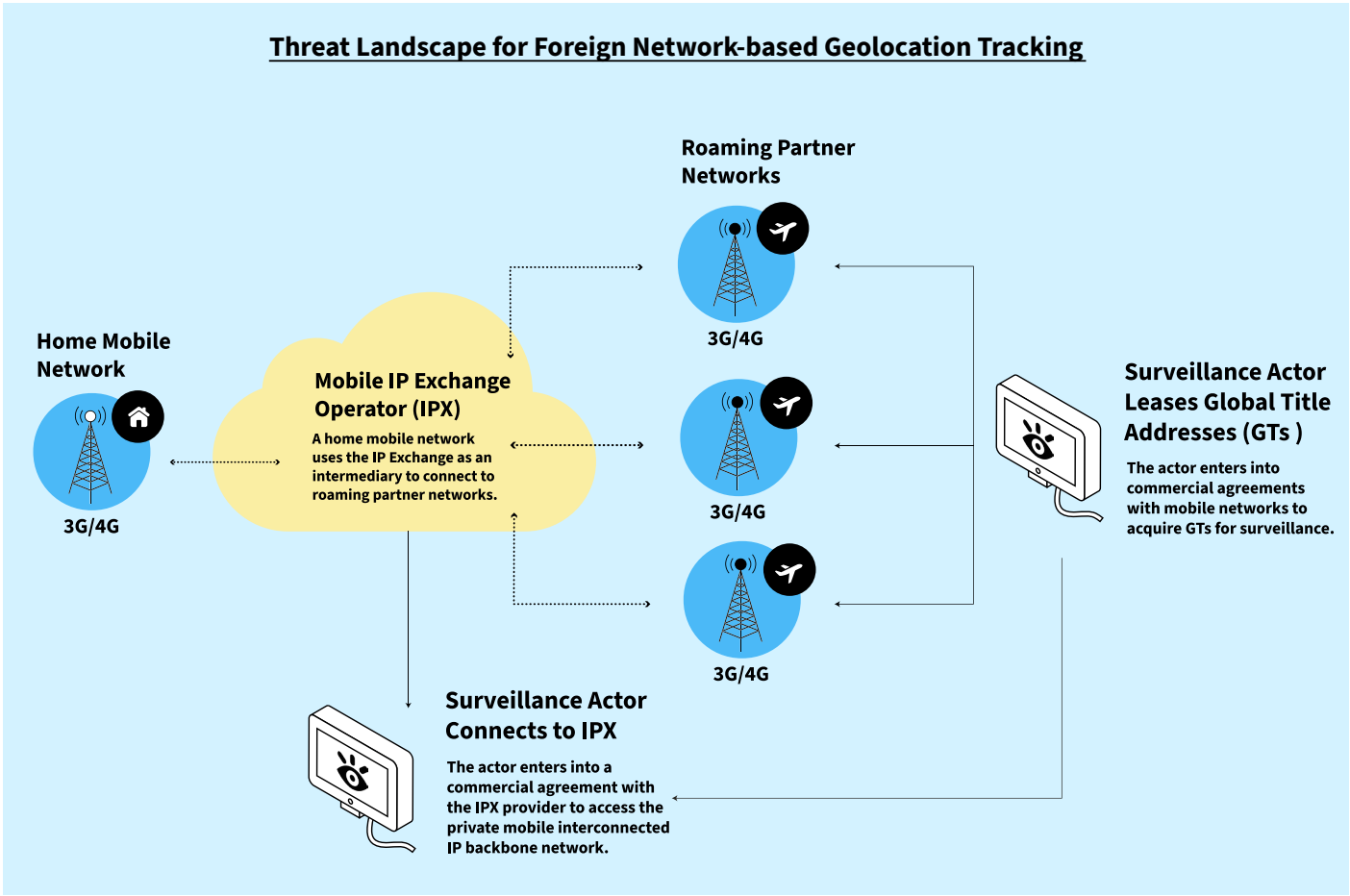


Figure 3: threat landscape for foreign network-based geolocation tracking.

Surveillance actors' operations are made possible due to the hub-and-spoke model that the IPX relies on to facilitate international roaming to other networks. In this model, while the IPX is responsible for routing and delivering messages between the home and roaming networks, it also connects other service providers, such as those delivering SMS messages, and other Value Added Service (VAS) providers that offer mobile number/HLR lookup, IoT mobility services, vehicle tracking, or hosted mobile virtual network operators (MVNO) that have agreements with IPXes. The end result is that a mix of third-parties have global access to mobile network operators' networks despite not having any direct commercial relationship with the foreign networks to which they can connect.

2.1.2. Vulnerabilities Tied to Home Location Register Lookup and Network Identification

One of the methods used to reveal network information associated with a mobile phone number entails using a commercial HLR lookup service. These kinds of commercial services enable organizations which are not telecommunications operators to check the status of a mobile phone number using the SS7 network without a mobile operator agreement. In this kind of situation, a surveillance actor would pay a fee to the HLR lookup provider based on the number of mobile number lookups it submitted to the service.

After receiving the phone numbers to lookup, the lookup service would issue a query using the SS7 network and retrieve a response from the network. That response would disclose information about whether the targeted number was valid and actively registered on a mobile network. If it is valid and active, the response will also disclose the network it was attached to and whether it was in a roaming state. Key information in the query will return the target IMSI associated with the MSISDN and the roaming network Visitor Location Register (VLR) address associated with the target phone. With this information in hand the actor can issue geolocation tracking requests with specific knowledge of the country, network, and the VLR used by the target phone.

Alternatively, if the surveillance actor already has access to the SS7 network under a leasing arrangement with a mobile network, they can perform the same HLR lookup, but without relying on an intermediary commercial HLR lookup service.

Information Box 2: Cross Protocol Signaling Attacks

3G vulnerabilities are particularly acute due to widespread address leasing arrangements,[10] though 4G networks can also assign and lease node addresses with the same effect. In some cases, actors will use 3G and 4G networks to simultaneously target the same user; these are referred to as "cross-protocol attacks."

The effect is twofold: first, the surveillance actors can directly request and receive geolocation information associated with the IMSI of the targeted device. Second, because the source address must be populated in signaling messages in order to route the message back to the source, it also leaves a fingerprint of the attack. This means that network firewalls operated by telecommunications providers can monitor the network from which the HLR lookup and location tracking messages were sent.

2.1.3. Domestic Threats—Innocent Until Proven Guilty

The risk of domestic location disclosure threats can sometimes be more concerning than those originating from foreign sources when third-parties are authorized by mobile operators to connect to their network. These can be particularly concerning in either low rule-of-law countries where domestic law enforcement or security agencies may abuse this access, or where state institutions in even high rule-of-law countries choose to exploit vulnerabilities in global telecommunications networks instead of working to actively secure and defend them.

Signaling firewalls used by telecommunications providers to prevent foreign operators, or surveillance actors, from illicitly querying the geolocation of their subscribers may be less effective against domestic threats. Specifically, if the signaling firewalls are not appropriately configured then attacks originating within the same network may be undetected because the activity—which is originating from within the operator's own network—is assumed to be trusted, and networks may not screen and block location tracking messages from sources within their own networks. The result is that the third-parties which are granted 3G and 4G addresses on home networks may, sometimes, have the ability to silently geolocate users without being noticed or filtered by the telecommunications provider.

In some countries, law enforcement and security agencies are allowed to connect directly to a home country network so that they can send location tracking messages domestically as well as internationally. In these cases, location tracking messages sent from that

10 Crofton Black, Stephanie Kirchgaessner, and Dan Sabbagh. (2020, December 16). Israeli spy firm suspected of accessing global telecoms via Channel Islands. *The Guardian.* https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands

domestic operator network address may be allowed to use networks in that country to track the location of users on other networks in-country or on foreign networks.

An example of the risks associated with state intervention of a telecommunications operator can be demonstrated by recent threat intelligence data showing location tracking attacks from the Vietnam mobile operator Gmobile, owned by GTel Mobile, which in turn is owned by the Vietnam Ministry of Public Security.[11] With a role of investigating national security matters, The Ministry of Public Security has been accused of various human rights violations including censorship and restrictions on internet freedom.[12]

From November 2022 to June 2023, five different SS7 GTs allocated to GTel/Gmobile were seen conducting surveillance operations targeting mobile users in African countries based on threat telemetry outputs from firewalls deployed in multiple mobile networks. Of the surveillance attempts seen from the data, a majority of the malicious signaling messages were associated with location disclosure.[13]

These conclusions emerge from data which is shown in Figure 4 and was derived from the Mobile Surveillance Monitor project, [14] which tracks surveillance activity from threat intelligence data sources. This data revealed that threats were detected and blocked by Cellusys[15] signaling network firewalls deployed at mobile operator networks. The charts show the distribution of various SS7 message operation types that were used by Gmobile in an attempt to track user locations from each of the source GT addresses which were, themselves, detected targeting phones in African mobile networks. As shown in the figure, various message types were used to attempt the location tracking operations. The technique of using different message types for location tracking is commonly used to try and either circumvent a signaling firewall or to enhance the chances of successfully geolocating the targeted devices.

11 Listed under Vietnam Enterprises Under the Ministry of Public Security (MPS): https://www.trade.gov/country-commercial-guides/vietnam-defense-and-security-sector

12 2022 Country Reports on Human Rights Practices: Vietnam (2022). U.S. Department of State. https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/vietnam/

13 Mobile signaling telemetry data was sourced from Cellusys and analyzed by Mobile Surveillance Monitor, a threat intelligence project operated by the author Gary Miller.

14 Tracking Digital Privacy Threats With Intelligence: https://surveillancemonitor.org

15 Cellusys: https://www.cellusys.com

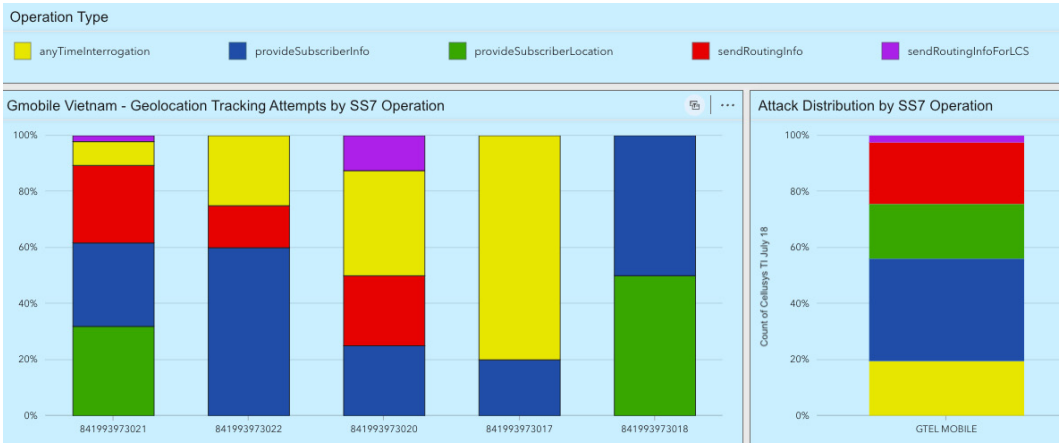


Figure 4: SS7 message types used by Gmobile Vietnam GT's to track user geolocation.

Gmobile was the only Vietnam network seen conducting targeted SS7 surveillance during this period of time. Given its ownership by the Ministry of Public Security the targeting was either undertaken with the Ministry's awareness or permission, or was undertaken in spite of the telecommunications operator being owned by the state.

2.2 Passive Attacks

Passive location attacks involve a domestic or foreign mobile network collecting usage or location information associated with a target mobile phone using collection devices installed in the network. The devices collect, and forward, communications and network data to a data warehouse or command and control facility which is operated by the surveillance actor.

2.2.1. Signaling Probes and Network Monitoring Tools

Signaling probes and network monitoring tools are typically placed into mobile networks by telecommunications companies for operational purposes, such as network trouble-shooting. These devices are generally placed in strategic network locations to capture network traffic at the user-level as it passes between network equipment. This process involves the probes ingesting raw signaling messages or IP traffic sent within a home network, or between the home and roaming partner networks where the user is currently registered. The network transactions are collected and provided to an upstream platform where they are processed and stored. Once in this platform, the messages can be aggregated to create operational Key Performance Indicators (KPIs) for analytics or saved in a format to trace user activity, such as a packet capture tool or analyzer such as Wireshark.[16] Because the probes intercept user signaling information they can track the general location of a mobile phone, even if the phone is not actively engaged in a voice call or data session.

16 Wireshark is a popular network analyzer tool, and is used to read and interpret captured network traffic.

2.2.2. Packet Capture Examples of Location Monitoring

The following figures (5 and 6) show examples of Packet Capture (PCAP) traces acquired from a mobile network. The traces are derived from an anonymous source to demonstrate how surveillance actors can extract location data from mobile signaling networks. The first two types of messages shown are Provide Subscriber Location (PSL) and Provide Subscriber Information (PSI). These are just two examples of the many types seen in location tracking operations. The final example seen in Figure 7 shows how a passive device capturing a user data session on the mobile network could reveal the location of the phone.

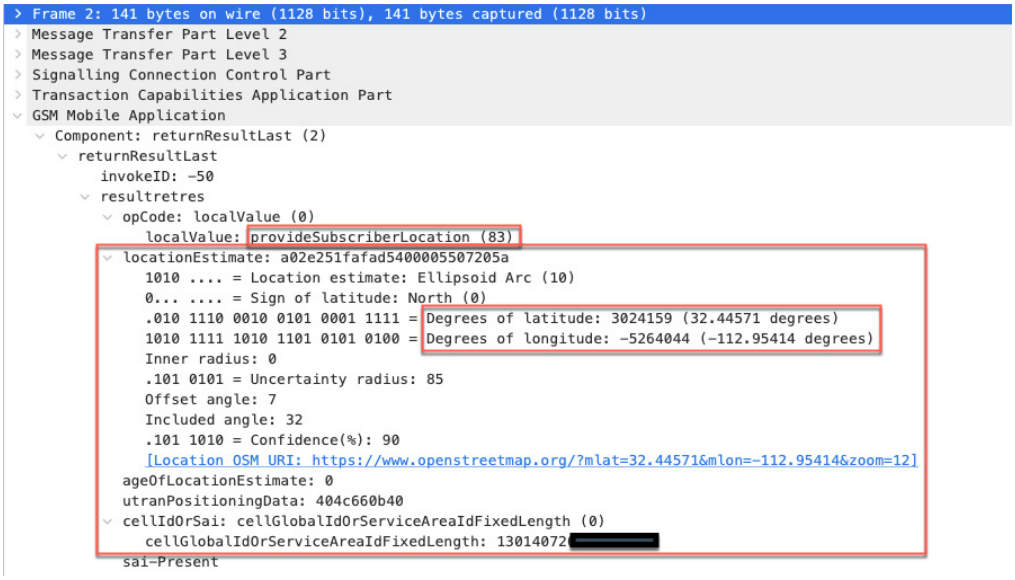


Figure 5: PSL signaling message active location tracking example.

In the PSL message response, the GPS latitude and longitude coordinates of the phone location is disclosed in the message sent back to the source GT, which could be operated by a surveillance actor.

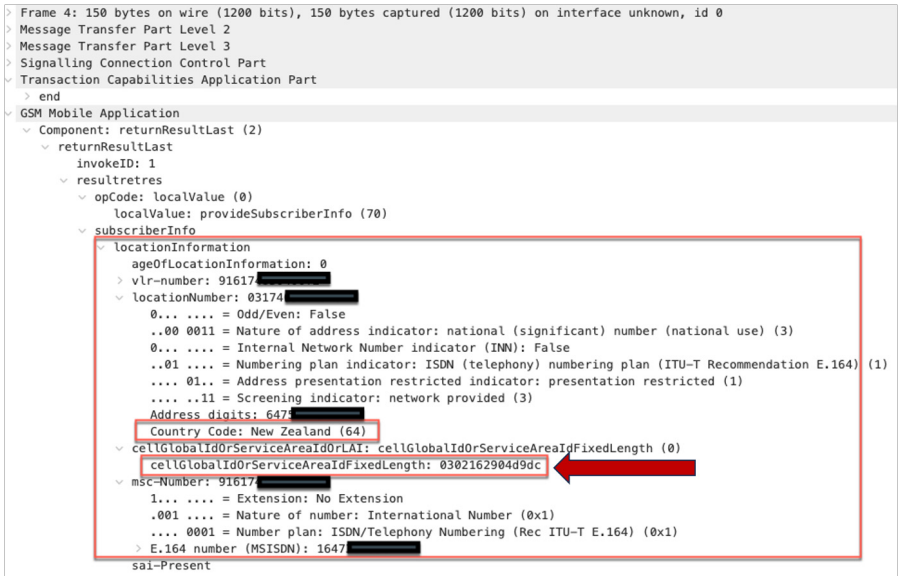


Figure 6: PSI signaling message active location tracking example.

In Figure 6, an international roaming user with a phone number based in Toronto, Canada has been located with a PSI message while using a mobile network in New Zealand. This has the effect of exposing the phone geolocation at the Cell ID level. The location information of the user is encoded in the cellGlobalIdOrServiceAreaIdFixedLength parameter,[17] which is an octet string including the current MCC, MNC, Location Area Code (LAC),[18] and Cell ID. In effect, with the octet string in hand it is possible to geolocate the mobile device.

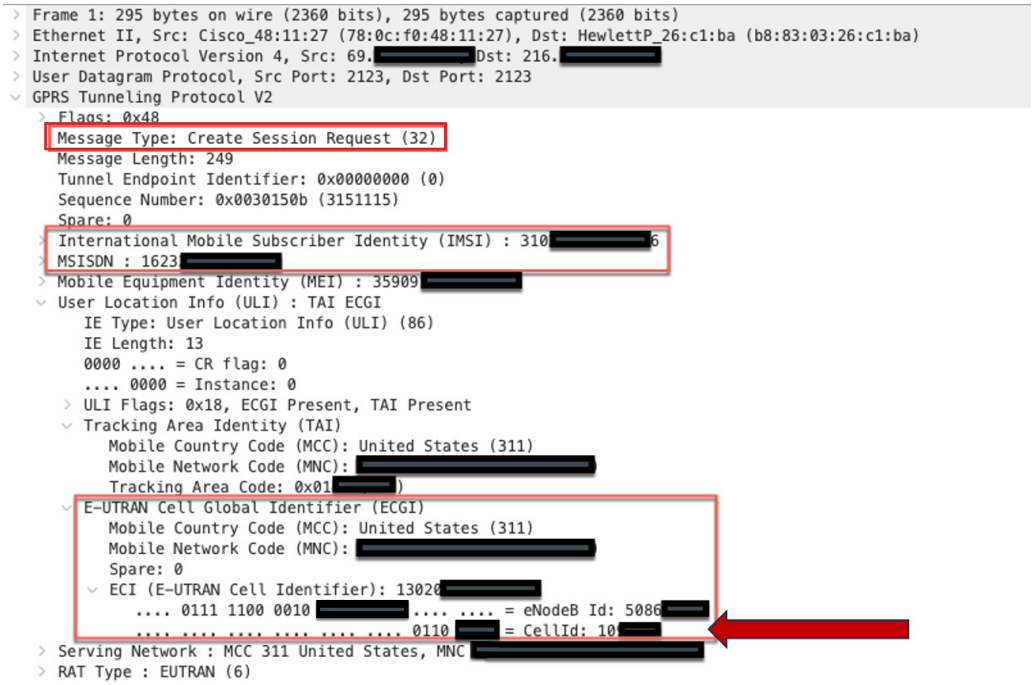


Figure 7: user location and identifiable information revealed in mobile data sessions (Note: Image was updated with additional redactions on November 8, 2023).

The packet capture shown in Figure 7 indicates that the IMSI, MSISDN, and IMEI of a mobile user has been revealed while attempting to establish a data session, as indicated by the GPRS Tunneling Protocol "Create Session Request" message. The request specifies the User Location Info (ULI), which provides the information necessary to derive the current global location of the user including the country, mobile network operator, base station, and Cell ID of registered user.

17 Defined in the mobile standards document 3GPP TS 23.003.

18 Defined in the mobile standards document 3GPP TS 24.008.

3. Case Studies and Statistics

The following case study reveals a tactic used to track the location of targeted users on a mobile network. It shows how a state sponsored surveillance actor can monitor the location of international traveler phones outside of their country.

3.1 Case Study - Saudi Arabia Tracking Travelers in the United States

The Guardian revealed a particularly notable example of likely state-sponsored geolocation tracking when it exposed activities which were likely conducted by the Kingdom of Saudi Arabia. The outlet reported that the country allegedly tracked the movements of individuals who traveled from Saudi Arabia to the United States and who were subscribers to Saudi telecommunications providers by exploiting the SS7 network.[19]

This surveillance was carried out by sending large volumes of Provide Subscriber Information (PSI) messages targeting the mobile devices that were roaming into the United States. These messages were issued by Saudi Arabia's largest three mobile operators, Saudi Telecom Company (STC), Mobily (Etisalat), and Zain KSA. When a network receives a PSI message, it will respond with the Cell ID (CID) of the targeted device and the CID, in turn, can uniquely identify the base station to which the device is registered at any given point. In effect, the United States network processed the PSI messages which had the effect of exposing the geolocation of the phones in the United States to the surveillance actors in Saudi Arabia. Surveillance actors can link the CID with a CID database to identify the GPS coordinates of the Cell ID. In aggregate, then, any PSI messages allowed into the network acted as a lynchpin to identify individuals' geolocation at the time of the surveillance and the duration of the targeted persons' travels in the United States. This would have had the effect of revealing the mobility patterns of residents of Saudi Arabia in the United States. This operation is described in the figure below.

19 Stephanie Kirchgaessner. (2020). Revealed: Saudis suspected of phone spying campaign in US. *The Guardian.* https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us

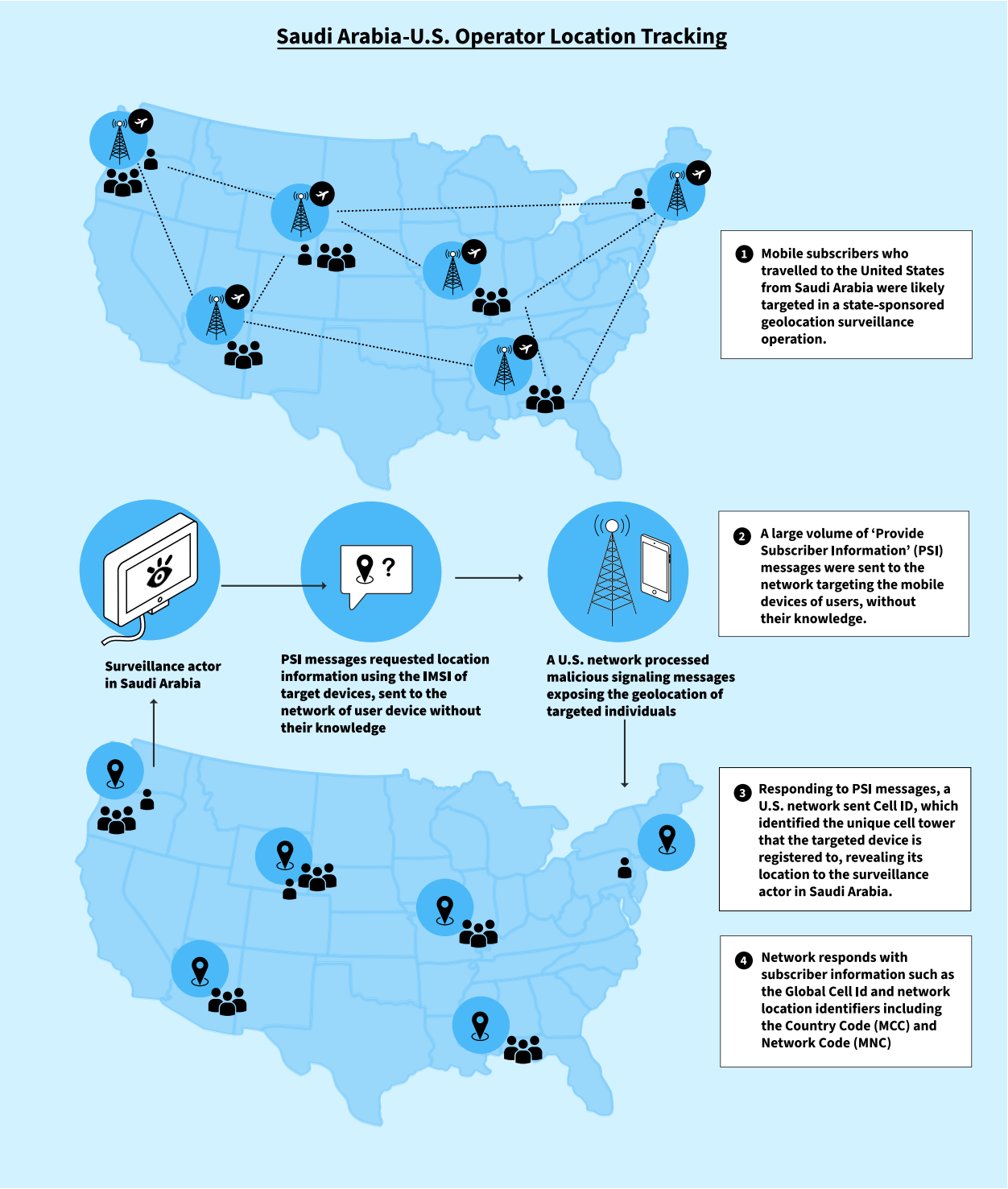


Figure 8: Location tracking of Saudi Arabian travelers in the United States.

The article noted that these messages were sent to each targeted Saudi phone many times per hour and that the anomalous activity could not be explained or justified under expected network operating procedures.

The transactions shown in Table 1 were aggregated over October to December 2019. They reveal the number of PSI messages that were sent from the three Saudi Arabia mobile operators to a specific United States mobile network, targeting IMSIs of Saudi phones

roaming on that network. The total IMSI count is the number of unique phones from the roaming partner seen on the network during the same timeframe.[20]

Roaming Partner Name	MCC, MNC	PSI Transactions	Total IMSIs
Saudi Telecom Company (STC)-SAUAJ	420,01	4,741,919	32,536
Etihad Etisalat Mobily-SAUET	420,03	2,821,709	11,362
Zain KSA-SAUZN	420,04	417,412	3,658
Total		**7,981,040**	**47,556**

Table 1: Saudi Arabia location tracking to United States mobile operator — Oct-Dec 2019

Data in Table 2 calculates the total number of tracking messages which were received from Saudi Arabia network operators during a 24-hour period, broken into hourly segments. Based on these single day statistics, each mobile phone was geolocated approximately every 11 minutes.

Event Date	PSI Transactions	Total IMSIs	Successful IMSIs	Requests Per Phone
29 Nov, 2019 00 hr	1750	265	262	6.60
29 Nov, 2019 01 hr	1469	242	241	6.07
29 Nov, 2019 02 hr	1491	223	221	6.69
29 Nov, 2019 03 hr	1469	214	212	6.86
29 Nov, 2019 04 hr	1199	209	207	5.74
29 Nov, 2019 05 hr	1441	250	247	5.76
29 Nov, 2019 06 hr	1231	222	222	5.55
29 Nov, 2019 07 hr	1249	270	266	4.63
29 Nov, 2019 08 hr	1125	229	229	4.91
29 Nov, 2019 09 hr	1523	306	303	4.98
29 Nov, 2019 10 hr	1260	290	288	4.34
29 Nov, 2019 11 hr	1358	304	304	4.47
29 Nov, 2019 12 hr	1325	298	297	4.45
29 Nov, 2019 13 hr	1677	368	367	4.56
29 Nov, 2019 14 hr	1567	380	378	4.12
29 Nov, 2019 15 hr	1684	406	403	4.15
29 Nov, 2019 16 hr	2191	443	439	4.95
29 Nov, 2019 17 hr	2560	507	504	5.05
29 Nov, 2019 18 hr	2426	484	484	5.01
29 Nov, 2019 19 hr	2368	467	465	5.07
29 Nov, 2019 20 hr	2363	422	417	5.60
29 Nov, 2019 21 hr	2196	407	402	5.40
29 Nov, 2019 22 hr	2397	409	400	5.86
29 Nov, 2019 23 hr	2387	354	348	6.74

Table 2. Saudi Arabia single day PSI location tracking targeting a United States mobile operator — Nov 29, 2019

20 In Table 1, the total unique IMSIs were observed over a three month timeframe. In Table 2, the total unique IMSIs were observed every hour.

Typically, PSI signaling messages from foreign networks are blocked by a network firewall. This defensive measure is intended to prevent unauthorized geolocation lookups. However, this did not occur in this case study because the targeted mobile phones were roaming on a United States network by their respective Saudi Arabia home networks. In contrast, had the messages been sent from a foreign network to a subscriber who did not belong to that same network, such as if a British operator had queried the same Saudi Arabian users while they roamed on United States networks, these messages should have been blocked.

The reason for the blanket surveillance outlined in this case study is not entirely clear. Nevertheless, we can conclude that this was likely state-sponsored activity intended to identify the mobility patterns of Saudi Arabia users who were traveling in the United States.

3.2. Current Statistics – Geolocation Tracking vs Other Threat Types

The failure of effective regulation, accountability, and transparency has been a boon for network-based geolocation surveillance. The figures below provide some context and offer a current view of the global mobile network landscape.

While some industry experts believe that mobile operators use firewalls to block a majority of geolocation tracking, with the effect of limiting the utility of using traditional SS7 surveillance methods, statistics provided by Mobile Surveillance Monitor indicate that geolocation disclosure is the most prevalent network threat type by a wide margin.

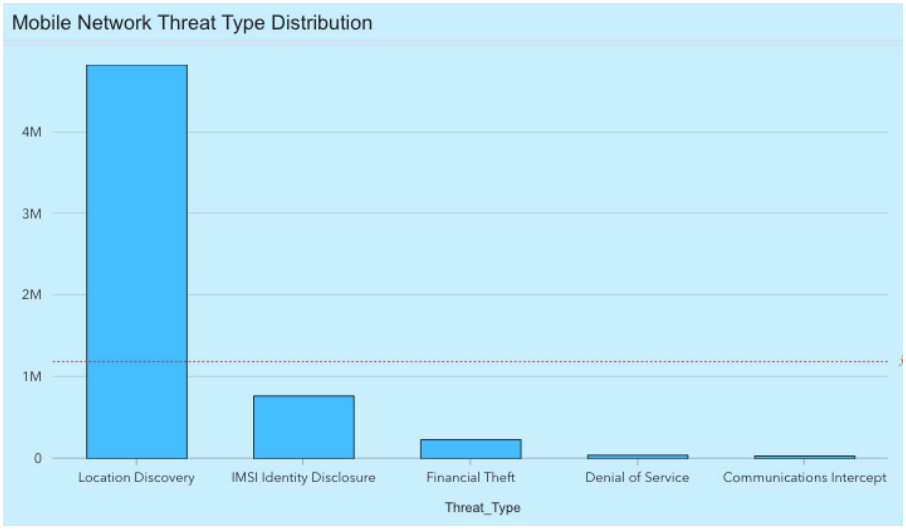


Figure 9: Network attack distribution by threat type.

Mobile Surveillance Monitor has also identified that approximately 171 networks from 100 source countries have sent targeted geolocation tracking messages to mobile operator networks located in Africa during the first half of 2023, indicating continued widespread

attempted SS7 surveillance activity. The top malicious networks from which these messages were sourced in 2023 are shown in Figure 10. The volume disparity between the top two network sources from the rest of the list indicates that GT's from Millicom Chad and Celtel DRC are likely attempting to harvest user location data. The activities by these GTs stand in contrast to other sources, such as Fink Telecom Services, which was exposed for selling targeted commercial phone surveillance services in the report "Ghost in the network" by the investigative journalism firm Lighthouse Reports.[21]

Network Threat Sources - Location Disclosure

Source Country	Source Network	Sum of Count (SUM)
Chad	MILLICOM CHAD	3,623,713
Congo DRC	CELTEL DRC	969,960
Zimbabwe	TELECEL ZIMBABWE	68,498
India	BHARAT SANCHAR NIGAM CELONE	53,436
Mozambique	MOCAMBIQUE CELULAR MOZAMBIQUE	35,614
Iceland	NOVA	16,979
Saudi Arabia	MOBILY ETIHAD ETILSAT	5,478
Jamaica	DIGICEL JAMAICA	4,884
Uganda	UGANDA TELECOM	3,784
Malaysia	CELCOM AXIATA BERHAD	3,773
Sweden	FINK TELECOM SERVICES	3,387
Italy	TELECOM ITALIA MOBILE	3,358
Saudi Arabia	ZAIN	3,141
Ghana	MILLICOM GHANA	2,699

Figure 10: SS7 network geolocation disclosure threats — ranking by source network.

21 Ghost in the network — Lighthouse Reports. (2023). *Lighthouse Reports.* https://www.lighthousereports.com/investigation/ghost-in-the-network/.
See also: Crofton Black and Omar Benjakob. (2023, May 14). How a secretive Swiss dealer is enabling Israeli spy firms. *Haaretz.com*. https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy-firms/00000188-0005-dc7e-a3fe-22cdf2900000

4. Incentives Enabling Geolocation Attacks

From an outsider's perspective, securing the perimeters of mobile networks would appear to be a straightforward process. Enterprises routinely place rigid security controls and filters at the edges of their networks using a firewall, so why would the same approach not be applied to mobile networks? And why not follow industry standards and widely accepted network security guidelines for mobile networks? In practice, security in mobile telecommunications is not as clear cut as it should be. A deeper look at some of the drivers in this critical infrastructure space can expose some controls which are more easily enforced than others.

Whereas domestic roaming policies can be mandated by the regulatory agencies of each country, such as the CRTC Telecom Regulatory Policies[22] or the UK Telecommunications Security Act,[23] international roaming is based on independent bidirectional negotiations and addressing information exchanges which are not regularly monitored or updated. At the industry level, technical interoperability and commercial aspects are facilitated by the GSMA Wholesale Agreements and Solutions (WAS) Working Group,[24] and the interoperability and addressing information that is exchanged between operators is maintained in documents called IR.21[25] and exchanged electronically using the Roaming Agreement Exchange (RAEX).[26] The network information in the IR.21 includes assignments of GT addresses or ranges to specific equipment in the operator network, with the purpose of informing each roaming partner for routing, interoperability, and security.

In the mobile telecommunications industry, the lack of strict requirements to maintain an inventory of address assignments to core network equipment has resulted in insufficient diligence by mobile operators around the world in updating their roaming address information. The effect of creating ambivalence about relying on RAEX and the network addresses listed in IR.21 ultimately reduces its reliability as a mobile security resource. The lack of an authorized and validated list of roaming partners with verified network information runs counter to the fundamentals of building a zero trust security posture.[27] If a system of strict compliance were properly maintained by each operator around the world, networks could use it to create better perimeter security controls.

---

22 Canadian Radio-television and Telecommunications Commission. (2021). Review of mobile wireless services. https://crtc.gc.ca/eng/archive/2021/2021-130.htm

23 Telecommunications (Security) Act 2021. (2021). https://www.legislation.gov.uk/ukpga/2021/31/enacted

24 Wholesale Agreements and Solutions Group — Working Groups. (2023, June 15). *Working Groups.* https://www.gsma.com/aboutus/workinggroups/wholesale-agreements-and-solutions-group

25 IR.21 GSM Association Roaming Database, Structure and Updating Procedures

26 RAEX IR.21 Management System – RoamSmart. (2019, June 18). *RoamSmart*. https://roam-smart.com/raex-ir-21-management-system/

27 According to the US National Security Telecommunications Advisory Committee (NSTAC), Zero Trust is described as "a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted." https://www.cisa.gov/resources-tools/groups/presidents-national-security-telecommunications-advisory-committee/presidents-nstac-publications

4.1. Economic Enablers

As mobile operators deployed analytics to monitor traffic exchanged between their roaming partner networks, it quickly became apparent that the trust model was broken. Millions of unauthorized messages from foreign networks were discovered[28] and this drove the industry to develop requirements for a signaling network firewall. While security guidelines and specifications have been designed and released by the GSMA's Fraud and Security Group (FASG)[29] there are, as of writing, no universal accountability or enforcement mechanisms. It is up to each respective mobile network operator—and perhaps their domestic telecommunications regulators and cybersecurity authorities—to decide whether, and how, they should protect their networks and subscribers.

Attention to unauthorized signaling messages became more acute following the presentation of the Carmen Sandiego Project at Blackhat 2010[30] and the presentation by Tobias Engel in 2014 at the Chaos Communication Congress.[31] The former revealed points of security vulnerability and the latter showed how basic software and SS7 network connectivity could enable limitless surveillance operations.

It was those presentations, and accompanying media attention, that drove vendors to begin developing and selling signaling firewalls. The adoption of these firewalls was often delayed, however, because some mobile network operators had already been leasing their networks to third-party Value Added Service (VAS) providers. This meant they were disincentivized to adopt a security posture which might negatively impact these business relationships and accompanying revenue. It was only after the GSMA finalized SS7 network security guidelines in 2017 that network operators began to deploy firewalls. However, by that time surveillance actors had been leasing GT's and deployed capabilities in mobile networks around the world, with the effect of mitigating some of the protections that signaling firewalls were meant to provide.

4.2 Industry Enablers

The mutually beneficial revenues associated with the vibrant GT leasing business has provided mobile networks around the world with significant sources of revenue. As of May 2023, network providers such as the Swedish telecommunications provider Telenabler AB, shown in Figure 11, continued to openly promote SS7 Global Title Leasing as a business offering.

28 Many discovered messages provided a phone's location, active calls, and more to the party that initiated the query.

29 Fraud and Security Group — Working Groups. (2023, March 23). *Working Groups.* https://www.gsma.com/aboutus/workinggroups/fraud-security-group

30 The Carmen Sandiego Project. *Blackhat* (2010, July 4). https://media.blackhat.com/bh-us-10/whitepapers/Bailey_DePetrillo/BlackHat-USA-2010-Bailey-DePetrillo-The-Carmen-Sandiego-Project-wp.pdf

31 Schedule 31. Chaos Communication Congress. (n.d.). https://fahrplan.events.ccc.de/congress/2014/Fahrplan/events/6249.html

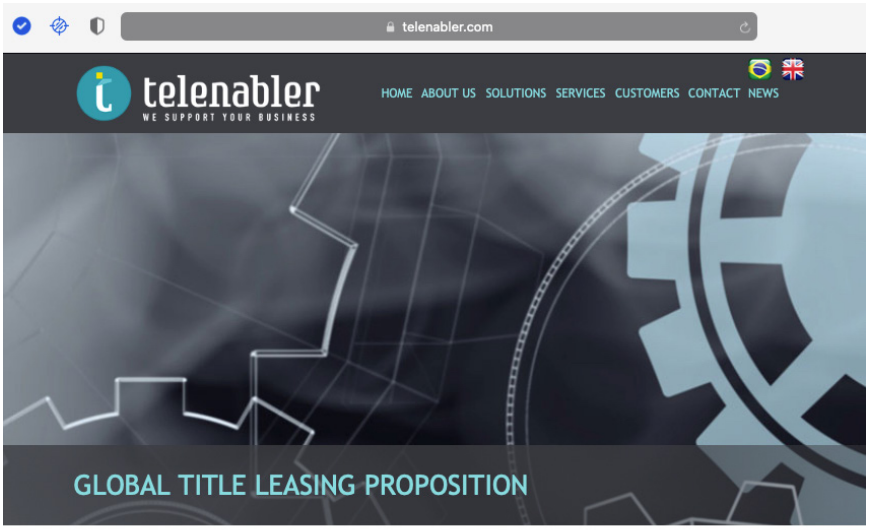
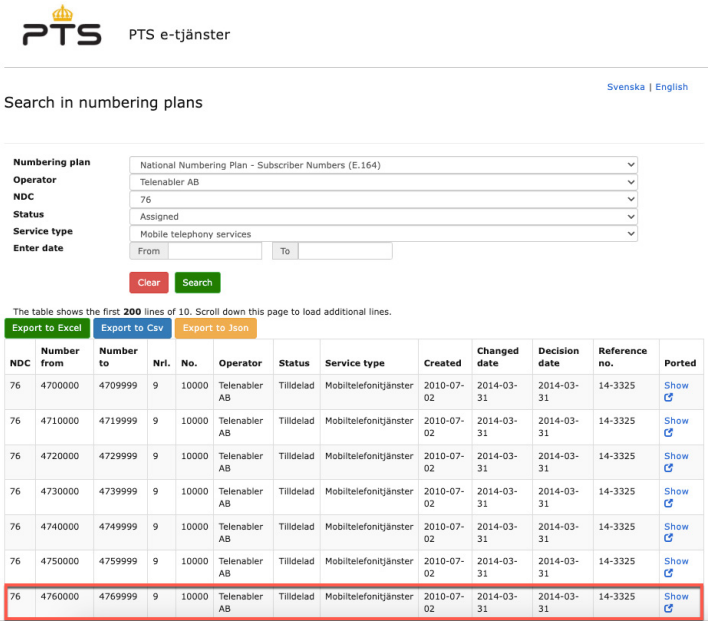


Figure 11: Telenabler Global Title leasing web page.

The point of GT leasing risks is made clear by examining GT's assigned to Telenabler by the Swedish Post and Telecom Authority (PTS) as shown in Figure 12 below. The outlined number range identifies a specific block of 10,000 numbers allocated to Telenabler, where a subset of those numbers were seen as the source of location tracking operations.



NDC	Number from	Number to	Nrl.	No.	Operator	Status	Service type	Created	Changed date	Decision date	Reference no.	Ported
76	4700000	4709999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4710000	4719999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4720000	4729999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4730000	4739999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4740000	4749999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4750000	4759999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show
76	4760000	4769999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2010-07-02	2014-03-31	2014-03-31	14-3325	Show

Figure 12: Swedish number range assigned to telenabler seen as the source of location tracking operations.

Four of the telephone numbers assigned to Telenabler were detected attempting geolocation surveillance up until June 29, 2023 as seen in Figure 13 below. Consistent with many surveillance actors, the source numbers used as GT's assigned to Telenabler are seen using multiple SS7 signaling message operation types, as seen in Figure 13. While different types of signaling messages were used, each had the objective of disclosing the geolocation of a target user's phone.

Mobile Network Threat Summary

Source Network	Source Node	Operation	Sum of Count SUM
TELENABLER AB	467647531812	anyTimeInterrogation	10
		provideSubscriberInfo	383
		provideSubscriberLocation	116
		sendRoutingInfo	37
	46764753182	anyTimeInterrogation	15
		provideSubscriberInfo	2
	46764753183	anyTimeInterrogation	27
		provideSubscriberInfo	33
		provideSubscriberLocation	17
		sendRoutingInfo	4
	467647531851	anyTimeInterrogation	35
		sendRoutingInfo	6
			Total 685

Figure 13: Location surveillance threat events attributed to telenabler leased GTs.

GT leasing rates have been removed from most websites due to the perceived negative implications of making networks available for a cost. However, the fees have traditionally been in the $5,000-$15,000 per month range.[32] Global Title lessors assert that there are a number of benefits associated with their commercial engagements. First, they assert they can offer SS7 network access to third parties without the resources to obtain number ranges. Second, they claim they can offer access to MVNOs and Global SIM service providers with a core network when they may not otherwise be able to obtain them due to local regulatory requirements. And, third, they assert that by leasing GTs they can offer global connectivity to messaging and value added service providers to mobile networks with low barriers to entry. Regardless of the extent to which these benefits are realized they also open the door to malicious operators to make GTs available to surveillance actors to undertake surreptitious geolocation surveillance.

32 Global Title leasing (fixed price per month). (n.d.). Freelancer. https://www.freelancer.com/projects/network-administration/global-title-leasing-fixed-price

Information Box 3: The Future of Global Title Leasing

The practice of third-party network leasing by foreign mobile networks remains an unregulated and opaque practice in the mobile industry. Network operators cannot determine which networks and which addresses have been leased to third-parties. Further, they have no ability to check the legitimacy of those third-parties or whether they have additional subleasing arrangements with surveillance actors such as criminal groups or state-sponsored entities. As a result, there is little accountability in the event a foreign network operator knowingly or unknowingly sells network access to a surveillance actor who is targeting mobile users.

The current status quo, however, may be changing. In March 2023, the GSMA released the document entitled "Global Title Leasing Code of Conduct."[33] The document lists a number of issues and concerns related to the commercial practice of GT leasing, which we have detailed in this report, and goes on to state that "GT leasing has evolved through the emergence of commercial relationships that were built up over time without any industry standardization, specifications, or recommendations. As a result, there is no agreed framework governing the relationships between GT Lessors and the networks to which they are interconnected."[34] The document proceeds to state very clearly that, "GSMA strongly advises that GT Leasing should not be used."[35]

While this is only a recommendation, it represents a significant shift in the official position of the GSMA and makes clear that the Association is at least willing to alter its policy positions. However, it remains unclear whether this will affect the third-party network reselling business that directly results in millions of yearly location tracking events seen on the world's mobile networks.

The GSMA Global Title Leasing Code of Conduct, discussed in Information Box 3, assigns legal liability to the GT Lessor in the event of malicious signaling traffic that causes harm to the target operator. By placing legal liability on the GT lessor that enables malicious cyber activities, such as geolocation tracking, it is difficult to conceive that the benefits to the selling operator outweigh the security, operational, and financial risks. However, telecommunications regulation is a state affair and, as such, it can be challenging to develop uniform cross-national industry policies or mandates that restrict such activities. Consequently, each respective operator is required to maintain strict security controls and firewalls to protect their network and subscribers.

Historically speaking, the impact of industry organizations to encourage restrictions on GT leasing have proven insufficient. While industry working groups such as the GSMA FASG have been formed to create guidelines meant to encourage mobile network operators to deploy security controls, they do not provide enforcement, publicly disclose attack statistics, or offer relevant threat intelligence with active operator participation. The GSMA

33 GSM Association Official Document FS.52 Global Title Leasing Code of Conduct

34 GSMA Official Document FS.52, Section 2.4 Issues and Concerns with GT Leasing

35 GSMA Official Document FS.52, Section 3 Global Title Leasing Use Cases

provides the Telecommunication Information Sharing and Analysis Center (T-ISAC) as a threat intelligence information sharing hub with the intention of distributing information regarding cybersecurity attacks. However, the service is only available to GSMA members and access to this information thus requires an annual financial contribution. In 2023, this contribution was between $14,306-$136,460, effectively serving as a payment gate to access information of benefit to the security and privacy of civil society.[36]

Mobile operators can directly engage the offending mobile operator whose networks are seen as the source of malicious signaling messages targeting their subscribers. This process traditionally involves the targeted mobile operator contacting the operator that was the source of the malicious signaling messages and giving them notice that if they do not see any responsible mitigation that the targeted operator will block subsequent traffic sent by the offending source GT address. However, if the targeted network operator blocks signaling messages from the source operator GT the surveillance actor can simply shift to sending these messages using another GT leased from the same operator or others from which they have leasing arrangements. This process could continue, where the attacker cycles through the available leased GT's until they are exhausted. Alternatively, attacks may be spread evenly over multiple networks across the world as a detection avoidance technique. This process ends up being an operationally intensive game of whack-a-mole where the defending operator simply gives up or configures the firewall to block the message types used in the attacks.

4.3. Government Enablers

In addition to some network operators being financially motivated to engage in leasing arrangements to surveillance actors, and the industry being largely unable to self-regulate, governments have generally taken a "hands off" approach to mobile network security. This may be linked to a lack of clear authorities conferred on telecommunications regulators, to assuming that mobile operators are best situated to solve security issues in their networks and, in other situations, to some government agencies benefitting from mobile network vulnerabilities and the state of weak operator security protocols.

In the first case, some domestic regulators are starting to take more active roles in demanding mobile network security standards. Critical infrastructure legislation is being passed and cybersecurity agencies are becoming more active in requiring telecommunications operators to provide details of how they secure their systems.[37] It remains to be seen, however, whether the wave of legislation that is being passed will necessarily

36 See: Membership Categories & Contributions — Membership. (2023, March 20). Membership. https://www.gsma.com/membership/membership-categories-contributions/

37 See: UK Telecommunications (Security) Act 2021, UK (DRAFT) Telecommunications Security Code of Practice

lead to effective government action or if, instead, it will just provide a range of powers and tools which governments are either ill-prepared to use or which could lead to insufficiently accountable government interference in telecommunications networks.[38]

In the second case, as states become more assertive in the kinds of security that telecommunications operators must adopt, the telecommunications operators can push back. They might oppose new government activity on the basis that proposed standards and requirements are overly intrusive, generally unneeded, or are simply inappropriate to the contemporary threat environment. In countries such as Canada there have long been voluntary forums wherein mobile operators and the government establish high-level standards that are accompanied by security review processes by government agencies.[39] Such measures may be insufficient given the current state of network insecurity.

In the third case, and perhaps more ominously, intelligence and security agencies that rely on mobile networks for surveillance may balk at the idea of heightening domestic telecommunications networks' security postures. They may also have an upper hand when it comes to determining what kinds of security elements are most appropriate, on the basis that they can effectively veto cybersecurity solutions that would impede their abilities to conduct surveillance domestically and abroad. While intelligence and security agencies may be most likely to understand how to exploit telecommunications networks for geolocation tracking, policymakers should also be mindful of the potential for law enforcement agencies to similarly misuse access to telecommunications networks, particularly in cases where domestic law enforcement agencies have a history of inappropriately exercising their powers absent suitable oversight and judicial authorization.

38 Christopher Parsons. (2022). "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act," *Citizen Lab*. Available at: https://citizenlab.ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act/

39 Canadian Security Telecommunications Advisory Committee (CSTAC). (2020, June 30). https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/committees-and-stakeholders/committees-and-councils/canadian-security-telecommunications-advisory-committee-cstac

5. Geolocation Tracking in 5G Networks and Unimplemented Defensive Measures

Surveillance actors have an ongoing interest in mobile networks and so they will adapt their methods according to the capabilities of the target network. While mobile telecommunications technologies and standards continuously evolve, many of the underlying principles and functionalities of the network architecture and surveillance methodologies remain the same.

Information Box 4: Equivalent Signaling Message Types Used to Query Mobile Device Location

In the case of user location lookups, each of these messages perform a similar action and could be exploited by an adversary; an adversary could even use all of these vectors simultaneously to target a single user if telecommunications operators expose these vectors as a result of how they have configured their networks.

Network Type	Sending Node	Example Message
2G/3G SS7	HLR	MAP_Provide-Subscriber-Information (PSI)
4G Diameter	HSS	Diameter Insert_Subscriber_Data_ Request (IDR)
5G	UDM	Namf_Location_ ProvideLocationInformation (NPLI)

Given the historical exposure of users to location tracking by adversaries, and the emergence of new services in 5G such as connected cars, smart homes, smart grids, and healthcare, it is critical that mobile network operators take a holistic and all-encompassing approach to protecting their networks if they are to limit the vulnerabilities which surveillance actors will otherwise exploit and abuse.

5.1. Subscriber Identity Privacy Enhancements

New security features which are available in the 5G standards take a significant step towards preventing network-based location surveillance. Whereas 3G and 4G networks use the IMSI as the user network identity, which has been exposed to adversaries and obtained over the years to conduct geolocation tracking attacks, 5G provides privacy enhancements. These enhancements have the ability to obfuscate the network identity

of the user and their device, and they come in the form of the following identifiers:

- **Subscription Permanent Identifier (SUPI) -** The globally unique identifier that is allocated to each 5G subscription
- **Subscription Concealed Identifier (SUCI)** - The encrypted equivalent of the SUPI that includes the Mobile Country Code (MCC) and Mobile Network Code (MNC), and the Mobile Subscription Identity Number (MSIN)
- **Globally Unique Temporary Identifier (5G-GUTI)** - The temporary identifier used in 5G networks to identify a mobile device and its associated subscription information

Implementing security features, however, is highly dependent on telecommunications operators adopting correct network configurations and taking advantage of the available 5G security features. There is a risk that some operators may not adopt these configurations on the premise that doing so increases the costs of deploying 5G infrastructure. Moreover, users have no ability to determine whether available privacy or security measures have been implemented. This customer-harmful business judgment on implementing privacy or security features should be avoided on the basis that, in doing so, businesses may be placing themselves in legal or regulatory jeopardy should individuals seek recompense for a failure to adequately protect their privacy, or regulators should impose fines on companies that have deliberately failed to protect their customers' personal information.

5.2. International Signaling and Interconnect Security Enhancements

The ability for foreign networks to target international users with signaling messages to reveal geolocation constitutes the most prevalent known attacks on mobile networks. Despite this being well known within the telecommunication industry the question remains as to whether operators are protecting their customers from these threats.

In fully-compliant, cloud-native 5G deployments,[40] international roaming signaling messages transit foreign networks with a new interface called N32 and use a network function called the Security Edge Protection Proxy (SEPP). This function was introduced into the 5G network architecture to add protection to the historically vulnerable communication between foreign network operators. The SEPP provides much needed encryption, integrity, and authentication at the border edge between roaming networks.

However, to provide privacy protection, networks on both ends of the roaming interface must implement the SEPP function. Getting all roaming partners to implement SEPP may

40 Fully-compliant refers to the 3GPP 5G Standalone (SA) defined in Technical Specification 29.573 (TS 29.573)

be extremely challenging; of the 351 network operators reported to have launched 5G services, only 41 have launched 5G cloud-native architectures according to the Global Mobile Suppliers Association (GSA) as of April 2023.[41] The remaining 310 operators are still using the Non-Standalone Architecture (NSA) for 5G, which lets mobile operators bypass the SEPP feature in 5G roaming while still providing the improved speed and reduced latency benefits of the 5G radio access network.

According to interviews with telecommunications security vendors at the Mobile World Congress (MWC) conference in March 2023,[42] only a handful of operators have deployed SEPP, let alone are actually using it. The effect is that many operators are not integrating the security and privacy benefits of the 5G standards when they are deploying 5G networks.

Many network vulnerabilities are specific to a given mobile network operator's implementation of telecommunications standards. However, given that many operators have shown a willingness to sell access to third-parties, there is a serious concern that surveillance actors will have software code in place to probe and test the integrity of foreign 5G networks. This will let surveillance actors adjust their tactics, techniques, and procedures for various network type vulnerabilities across each target network implementation. Historically, surveillance actors have quickly learned to modify their attacks to disguise traces and circumvent firewalls, and the slow pace of operator security deployments reduce the challenge that such actors will have in finding and exploiting obvious vulnerabilities.

The slow pace of operator security deployments over the most vulnerable attack vectors should be a wake up call to country regulators. To counter attacks quickly, adherence to 5G security guidelines and standards are imperative, in addition to adequate tools for threat detection. Without these measures, the ways in which 5G networks have been deployed may only be marginally better at protecting users from surveillance actors' attacks than the prior 3G and 4G networks, if at all.

41 GSA — 5G Public-Networks April 2023 Summary Report https://gsacom.com/paper/public-networks-april-2023-summary-report/

42 HardenStance Briefing — MWC23: Taking Stock of Telco Security https://www.hardenstance.com/wp-content/uploads/2023/03/HardenStance-Briefing-MWC23-Taking-Stock-of-Telco-Security-FINAL.pdf

6. Conclusion

Based on historic, current, and forward-looking assessments of mobile network security, geolocation surveillance should continue to be of significant concern to the public and policymakers. Exploitable vulnerabilities exist in 3G, 4G, and 5G network architectures and are expected to remain, absent forced transparency that exposes bad practices, and accountability measures that compel operators to correct such issues. If anything, the availability of all three network types provides multiple options for surveillance actors. If nation states and organized crime entities can actively monitor the location of mobile phones domestically or in foreign countries, then such vulnerabilities will continue to represent a security risk to the safety of not only at-risk groups, but also corporate staff as well as military and government officials.

The past four years reveal that surveillance originates from networks operating within nations with high internet freedom rankings, small remote island countries, and ostensibly neutral countries. Current vulnerabilities of mobile networks are systematically exploited as a source of intelligence gathering or espionage by surveillance actors, law enforcement, and organized crime groups who exploit vulnerabilities for their own purposes. Threat activity that is emergent from small Caribbean countries, as well as attacks from eastern European and African countries, point to widespread abuse of many telecommunications networks' Global Title leasing arrangements.

In light of the existent threats, what can be done? While this report does not offer comprehensive policy recommendations or technical suggestions, there are a series of interventions that should be prioritized.

First, attacks which often occur during international travel suggest the likelihood of third-parties sharing private user IMSIs. There should be active efforts by law enforcement and security services to prevent trafficking in such information, such as through the dark web.

Second, network and other third-party service providers, such as those who provide IPX and inter-carrier billing settlement, should be required to encrypt the unique details of a phone's IMSI and its accompanying mobile data files. Such activities should be accompanied by a strict and regular schedule of compliance audits. These protection and accountability measures would prevent malicious actors within the networks from illicitly monetizing or otherwise leveraging such retained information. Such audits might be undertaken by data protection authorities, privacy commissioners, telecommunications regulators, or consumer rights regulators.

Third, the prospect of inappropriately allowing third-party access to the private IPX network, or brokering information it obtains when exchanging signaling traffic, raises the likelihood for significant malicious surveillance capability.[43] Specifically, surveillance operators could connect and monitor traffic from international signaling hubs between foreign networks and play a key role in the ability to execute these attacks. Telecommunications, cybersecurity, data privacy, and consumer rights regulators should all assess whether mobile participants in their jurisdictions are engaged in questionable business practices that endanger individuals' security, privacy, and consumer rights. Legislators, too, should be attentive of whether they should provide additional powers to regulators to discipline bad actors or mobile industry participants that are prioritizing revenues over protecting their subscribers.

Fourth, the increasing frequency of geolocation attacks using 4G networks indicates an increased level of sophistication amongst surveillance actors and an evolutionary trend that is elevating espionage risks as the world moves into the 5G era. 5G deployments are already fully launched in many developed nations and geolocation surveillance activity is seen from some of these same countries. This calls into question the security of future roaming partnerships with networks of western countries. While a great deal of attention has been spent on whether or not to include Huawei networking equipment in telecommunications networks, comparatively little has been said about ensuring non-Chinese equipment is well secured and not used to facilitate surveillance activities.[44] Policy makers, telecommunications regulators, cybersecurity agencies, and legislators alike should move to develop a vendor- and platform-neutral set of mandatory security and privacy standards. They should, also, work to actively enforce these standards and attach significant penalties to companies that are found deliberately not adhering to them.

Consumers might rightfully assume that their telecommunications provider has deployed and configured security firewalls to ensure that signaling messages associated with geolocation attacks, identity attacks, or other malicious activity are not directed towards their phones. Unfortunately this is not often the case. Decades of poor accountability and transparency have contributed to the current environment where extensive geolocation surveillance attacks are not reported. This status quo has effectively created a thriving geolocation surveillance market while also ensuring that some telecommunications providers have benefitted from turning a blind eye to the availability of their

43 Jon Brodkin. (2021, October 6). Company that routes SMS for all major US carriers was hacked for five years. *Ars Technica.* https://arstechnica.com/information-technology/2021/10/company-that-routes-sms-for-all-major-us-carriers-was-hacked-for-five-years/

44 For more, see: Christopher Parsons. (2020). "Huawei and 5G: Clarifying the Canadian Equities and Charting a Strategic Path Forward." *Citizen Lab.* Available at: https://citizenlab.ca/2020/12/huawei-5g-clarifying-the-canadian-equities-and-charting-a-strategic-path-forward/.

network interconnections to the surveillance industry. While it is implausible to expect that all telecommunications networks will adopt security and privacy postures to protect against all threats, the low-hanging geolocation threats detailed in this report should be addressed post-haste.

Operators should be required to: adopt and act to attain and demonstrate compliance with cybersecurity guidelines and frameworks such as zero trust; report when they experience attacks; accept accountability for when their networks are abused by surveillance actors; work towards buiding security agreements and accreditations; and undertake penetration tests to identify and remediate vulnerabilities. In cases where operators decline to undertake these activities willingly, then regulators should step in to compel corporations to undertake these kinds of activities.

Today, surveillance actors use geolocation to reveal intimate and personal information. It is used to track human rights defenders, senior business leaders, government officials, and members of militaries. In the future, with the blossoming of smart cities, the internet of things, and the growth of internet-connected systems, the capabilities and potentials for attack will only grow. If organizations should fail to act, then advocates in civil society and the broader business community will have to pressure regulators, policy makers, and politicians to actively compel telecommunications providers to adopt appropriate security postures to mitigate the pernicious and silent threats associated with geolocation surveillance.