ISACA

# 5G Privacy: Addressing Risk and Threats

Privacy

# CONTENTS

# ABSTRACT

By 2025, there will be an estimated 1.8 billion fifth-generation (5G) wireless connections worldwide, with Asia and the United States leading the growth trend.[1]

Enterprises will have the option of building and controlling a private 5G network using their own spectrum or procuring a network slice from a provider's public 5G wireless network. It is estimated that by 2030, more than 1,000 businesses and government organizations will have deployed private 5G networks.[2]

5G is designed to greatly increase the speed and responsiveness of wireless networks to connect virtually everyone and everything—including machines and devices. 5G wireless technology delivers data and services at higher bandwidths than earlier-generation wireless technologies, and with ultra-low data latency, massive network capacity, increased availability, and a more uniform user experience.[3] Along with these advantages, 5G networks add new privacy concerns to those already impacting users of cellular networks. To build trust among consumers, regulators, government agencies and businesses, both emerging and existing privacy issues must be addressed.

This paper reviews 5G network architecture with special attention to its privacy features. This examination includes a high-level review of 5G architecture and a discussion of existing and emerging privacy threats. It also highlights some new 5G privacy features that can mitigate those threats.

[1] Scarsella, A.; P. Solis; J. Leigh ; "U.S. 5G Smartphone Forecast, 2021-2025," https://www.idc.com/getdoc.jsp?containerId=US48244821#:~:text=The%20U.S.%205G%20smartphone%20market,in%20a%20CAGR%20of%2036.3%25

[2] Ferguson, K.; "5 Predictions About 5G Adoption in 2022 and Beyond," TechTarget, 22 February 2022, https://www.techtarget.com/whatis/feature/5-Predictions-about-5G-Adoption-in-2021-and-Beyond

[3] Qualcomm, "Everything you need to know about 5G," https://www.qualcomm.com/5g/what-is-5g

# Introduction

5G technology's new capabilities can transform the experience of its users. They include:

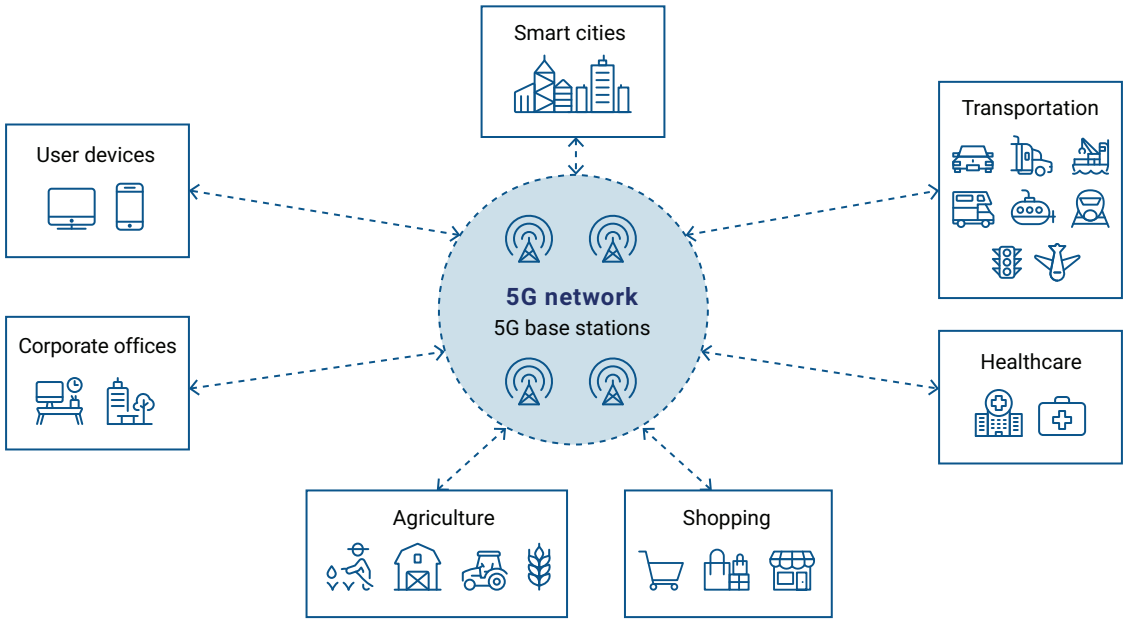
- Providing a faster network with greater capacity and less delay, compared with previous technologies
- Supporting many diverse types of static and mobile Internet of Things (IoT) devices
- Decreasing network energy usage
- Meeting technical and services requirements of specific customers/market segments via the 5G network slicing function
- Revolutionizing industries with many new possibilities

These capabilities are further detailed in **figure 1**. 5G provides services that power applications used in several industries, including those shown in **figure 2**. Examples of industries that stand to be transformed by 5G adoption include retail, healthcare and manufacturing.

**FIGURE 1:** 5G Capabilities

| 5G Capabilities | Description |
|---|---|
| Provides a faster network with greater capacity and less delay, compared with previous technologies | Higher capacity with faster processing improves the connectivity needs of the IoT ecosystem by eliminating lags in transmitting data across the network. Extremely fast speeds provide low latency of 1 millisecond. The faster 5G speed means faster download of a high-definition (HD) film compared to the time required for a 4G network. |
| Supports a variety of static and mobile IoT devices | Allows flexibility by supporting IoT devices with a diverse range of:<br>• Speeds<br>• Bandwidth<br>• Quality-of-service requirements |
| Decreases network energy usage | 5G technology can reduce network energy usage by as much as 90% and provide up to 10 years' worth of battery life for low-powered IoT devices. |
| Helps revolutionize businesses by offering endless possibilities with virtually no limits | Supports and promotes other technologies/applications with its high speed, low latency and massive capacity:<br>• Drone deliveries<br>• Cloud-connected traffic control<br>• Emergency response<br>• Next-level gaming and entertainment |
| Meets technical and services requirements of specific customers/market segments via its network-slicing functionality | Creates multiple unique logical and virtualized network infrastructures via its network-slicing functionality. Each network slice is an isolated end-to-end network tailored to fulfill specific requirements requested by a particular application. |

**FIGURE 2:** Industries Impacted by 5G Technology



## Retail Industry

The retail industry will greatly benefit from the rollout of 5G, especially in populous areas where coverage is expected to flourish. 5G will complement other smart retail technologies, such as shelf sensors, cashier-less checkouts and QR codes.

Brick-and-mortar retailers could use 5G in conjunction with ultra-high definition (UHD) video, virtual reality and augmented reality as a way of competing more effectively with online shopping and providing enhanced in-store digital interactions with customers.[4]

According to Forrester, 5G communications will boost retail supply chain transparency and efficiency as IoT sensors become ubiquitous. Further, GSMA Intelligence estimated that the IoT market in North America will account for 5.9 billion connections by 2025.[5]

## Healthcare Industry

5G is expected to revolutionize every aspect of healthcare, from supply chain optimization to remote diagnostics to electronic medical records management. 5G-compatible devices may be used to monitor bed occupancy levels, the movement of physicians, nurses and patients around the hospital, and wearable medical devices.[6]

The biggest 5G transformational change is likely to come through haptic communications and the tactile Internet. The tactile Internet is a service that combines ultra-low latency with extremely high availability, reliability and security.[7]

This type of Internet connectivity will enable a physician to perform a procedure on a remote patient. A surgeon's movements at one site would be recreated instantaneously by computerized equipment at the other site. This innovation will particularly benefit patients in rural areas or other locales where surgeons specializing in complex procedures may not be readily available.[8]

A surgeon's movements at one site would be recreated instantaneously by computerized equipment at the other site.

5G-enabled healthcare could generate US$250 billion to US$420 billion in global GDP by 2030. The total global financial impact of 5G by 2030 is predicted to reach US$1.3 trillion.[9]

## Manufacturing Industry

The use of analytics, artificial intelligence and advanced robotics in smart factories via low-latency and private 5G networks will have a major impact on overall plant performance by improving operational efficiency at every stage of production—both on single assembly lines and across multiple facilities. McKinsey estimates that the GDP impact of connectivity in manufacturing could reach US$400 billion to US$650 billion by the end of the decade.[10]

[4] IHS Markit, "The 5G Economy," November 2019, https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/the_ihs_5g_economy_-_2019.pdf
[5] *Op cit* Ferguson
[6] PwC, "5G in Healthcare," 2020, https://www.pwc.com/gx/en/industries/tmt/5g/pwc-5g-in-healthcare.pdf
[7] Fettweis, G., et al.; "The Tactile Internet," ITU-T Technology Watch Report, August 2014, https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000230001PDFE.pdf
[8] *Op cit* PwC
[9] Grijpink, F., et al.; "Connected World: An Evolution in Connectivity Beyond the 5G Revolution," McKinsey Global Institute, February 2020, https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/telecommunications/our%20insights/connected%20world%20an%20evolution%20in%20connectivity%20beyond%20the%205g%20revolution/mgi_connected-world_discussion-paper_february-2020.pdf
[10] *Ibid.*

# Privacy Concerns Associated With 5G

Along with its benefits, 5G's expanded surface brings new privacy concerns, including a very high risk of leaking personal data or exposing hints that could reveal sensitive personal information.[11]

Effective consideration of privacy issues is critical to building and maintaining the trust relationship between consumers and service providers.[12]

Privacy threats consist of the following:

- Existing threats to previous-generation (2G, 3G and 4G) cellular networks
- New and emerging threats to 5G networks

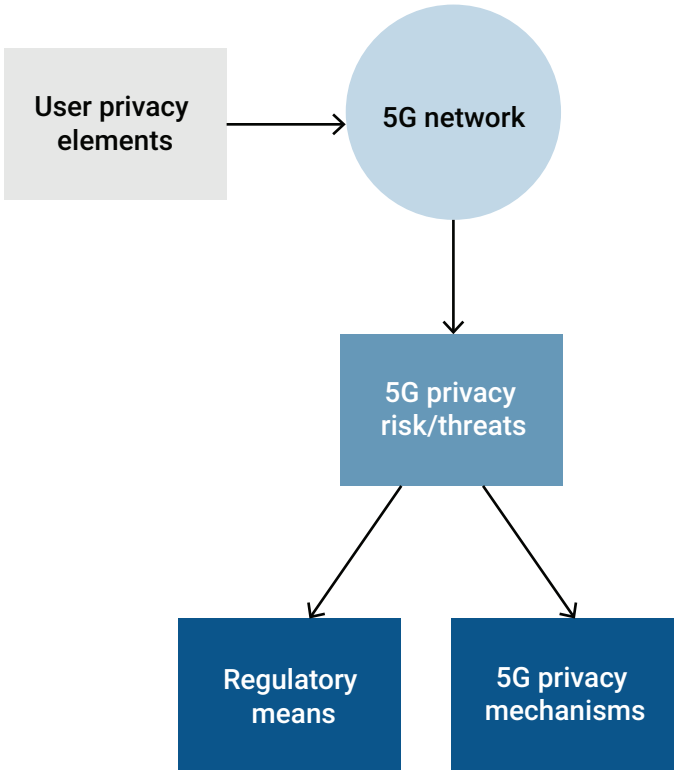
These threats can be understood and mitigated through a combination of two types of approaches:

- New 5G architectural enhancements
- Privacy laws and regulations[13]

Effective consideration of privacy issues is critical to building and maintaining the trust relationship between consumers and service providers.

This white paper reviews 5G technology from the privacy perspective, including user privacy elements related to 5G networks, 5G privacy threats, 5G privacy mechanisms and regulatory means to address these threats (**figure 3**).

**FIGURE 3:** Privacy Roadmap




[11] Liyanage, M.; J.Salo; A. Braeken; T. Kumar; S. Seneviratne; M. Ylianttila; "5G Privacy: Scenarios and Solutions," 2018 IEEE 5G World Forum (5GWF), 2018, https://ieeexplore.ieee.org/document/8516981

[12] Liyanage, M.; I. Ahmad; A. Bux Abro; A. Gurtov; M. Ylianttila; "User Privacy, Identity and Trust in 5G," in *A Comprehensive Guide to 5G Security*, Wiley, March 2018, https://ieeexplore.ieee.org/document/8341895

[13] Scientific Foresight Unit (STOA), STOA Options Brief "Privacy and security aspects of 5G technology," European Parliament, 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/697205/EPRS_STU(2022)697205(ANN1)_EN.pdf

# 5G Technology Explained

To understand the privacy considerations related to 5G technology, it is important to first have an understanding of the technology itself.

## Cellular Network Evolution

First-generation (1G) wireless network technology was based on an analog cellular network that transmitted voice communications using electronic pulses with varying magnitudes to send data. Its components were a mobile phone, cell towers and mobile switching centers. A cell tower consisted of an antenna and communication equipment placed on a tower to serve a small geographical area (cell). Phones running on 1G network had low battery life and poor voice quality and lacked security. Users usually experienced dropped calls.

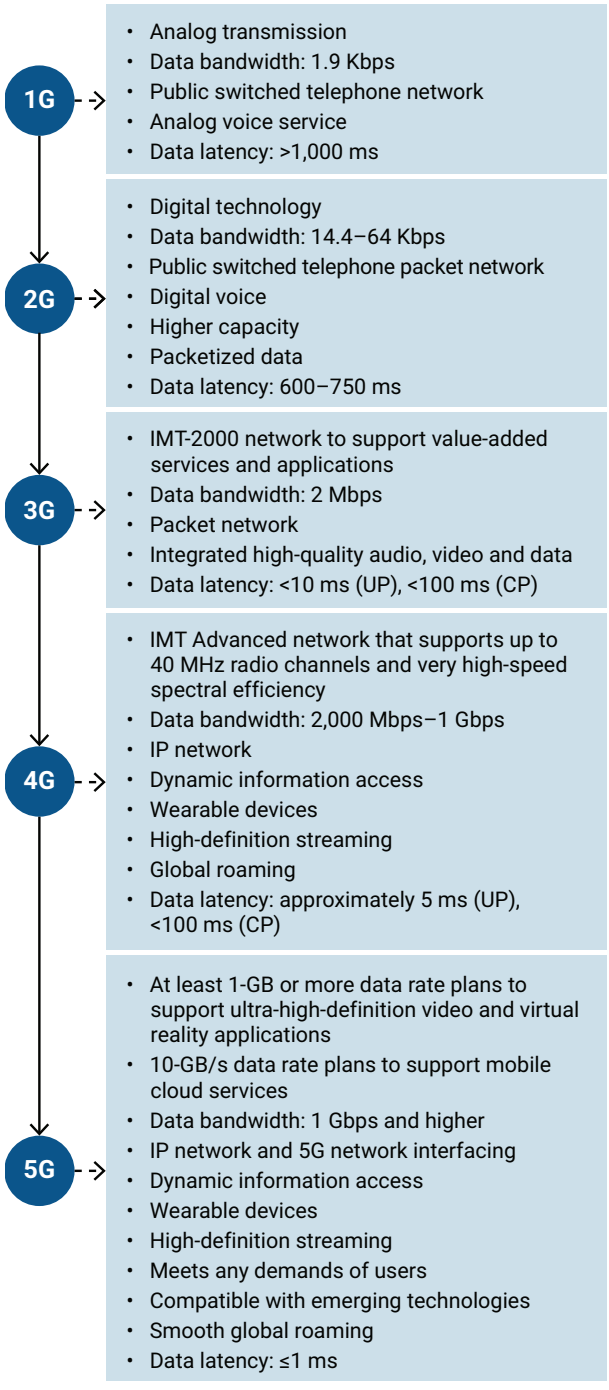
Second-generation (2G) and later-generation (3G, 4G and 5G) networks are all digital cellular networks. These digital networks are mobile communications networks that cover a specific geographical area with radio cells. These networks use radio waves to transmit signals to a network of base stations. The radio waves used by mobile devices are part of the electromagnetic wave spectrum and travel at the speed of light. The evolution of cellular technology from 1G to 5G is shown in **figure 4**.[14, 15]

Radio waves used by mobile devices are part of the electromagnetic wave spectrum and travel at the speed of light.

## 5G Architecture

5G technology inherits improved versions of features found in existing 4G technology[16] and introduces new architectural and service-oriented enhancements.[17]

**FIGURE 4:** Cellular Technology Evolution




[14] Slalmi, A.; H. Chaibi; A. Chehri; R. Saadane; G.Jeon; N. Hakem; "On the Ultra-Reliable and Low-Latency Communications for Tactile Internet in 5G Era," *Procedia Computer Science,* vol. 176, 2020, https://www.sciencedirect.com/science/article/pii/S1877050920318925

[15] Net-informations.com, "1G Vs. 2G Vs. 3G Vs. 4G Vs. 5G," http://net-informations.com/q/diff/generations.html

[16] ISACA, "5G Security: Addressing Risk and Threats of Mobile Network Technologies," 2021, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoEFEA0

[17] *Op cit* Liyanage et al., "5G Privacy"

As shown in **figure 5,** 5G architecture consists of two components: 5G Core Network and 5G Radio Access Network (RAN).

## 5G Radio Access Network

The 5G RAN can be described as the arms and legs of the 5G network. As shown in **figure 6**, a RAN consists of the following:

- **User Equipment (UE)**—Includes cellphones and many Internet of Things (IoT) devices
- **Base station**—Includes radio unit (RU), antennas, baseband unit (BBU) and interfaces
  - Antennas receive digital radio signals from the UE operated by the users and pass the signals to the RU. When the RU receives signal information from the antennas, it uses the Common Public Radio Interface (CPRI) to communicate with the baseband unit (BBU). The BBU then processes the signal information so it can be forwarded to the core network. Data go back to the user through a reversal of this process.[18]
- **Access and mobility management function (AMF)**—A network function[19] that acts as a single-entry point for UE connections and, based on the customer's request transmitted via UE, selects and performs the requested functionality.[20] Available functionalities include access authentication and authorization, registration management and connection management.[21]

## 5G Core

5G Core (5GC) can be depicted as the brain of the 5G network.[22] It "utilizes cloud-aligned, service-based architecture (SBA) that spans all 5G functions and interactions including authentication, security, session management and aggregation of traffic from end devices."[23]

The core network is subdivided into three domains:

- Home network
- Serving network
- Transit network[24]

**FIGURE 5:** 5G Network with Components

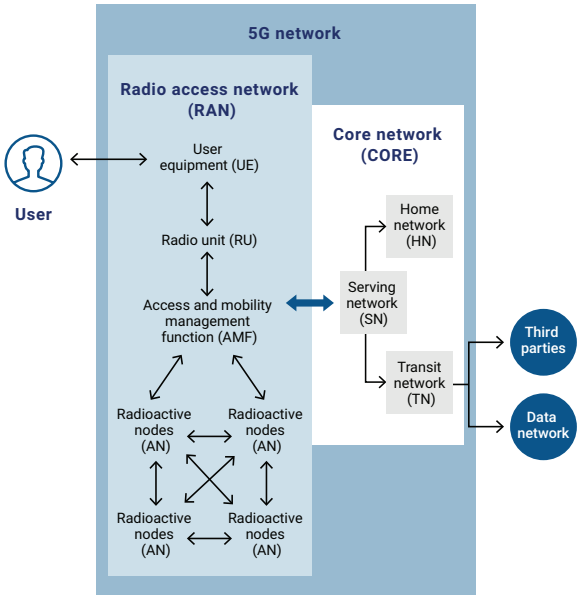
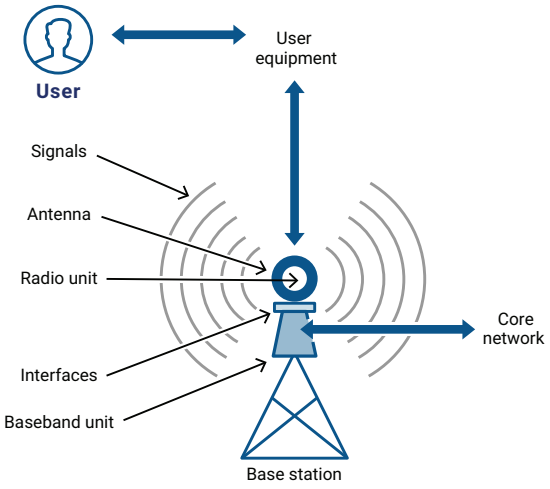



**FIGURE 6:** RAN—Base Station




[18] SDxCentral Studios, "What Is the Radio Access Network (RAN)?," SDxCentral, 17 January 2018, https://www.sdxcentral.com/5g/ran/definitions/radio-access-network, SDxCentral Studios
[19] *Op cit* ISACA
[20] Pathak, R.; "5G Core Network Architecture - A Beginners Guide," Rajarshi Pathak, https://www.rajarshipathak.com/2020/01/beginners-guide-for-5g-core-network-architecture.html
[21] *Ibid.*
[22] Purdy, A.; "Why 5G Can Be More Secure Than 4G," Forbes, 23 September 2019, https://www.forbes.com/sites/forbestechcouncil/2019/09/23/why-5g-can-be-more-secure-than-4g/#30194b6157b2
[23] Viavi, "5G Architecture," https://www.viavisolutions.com/en-us/5g-architecture
[24] ETSI 3rd Generation Partnership Project (3GPP), "Universal Mobile Telecommunications System (UMTS); LTE; General UMTS Architecture (3GPP TS 23.101 version 8.0.0 Release 8), 2009, https://www.etsi.org/deliver/etsi_ts/123100_123199/123101/08.00.00_60/ts_123101v080000p.pdf

The home network represents the core network functions conducted at a permanent location regardless of the user's access point. This network is responsible for retaining permanent user-specific data and managing subscription information via a Home Subscriber Server (HSS), which holds a database of all the operator's subscribers.[25] The home network also provides interfaces through which the serving network obtains authentication and other subscriber-related information from the HSS.[26]

The home network operator trusts the serving network operator to authenticate the UE using one-time authentication information that the home network provides. This information is used for authentication and session key generation. Note that the home network operator does not trust the serving network operator with the actual long-term credential for authentication (which is stored in the HSS's database). The long-term credential is used only as a fault recovery mechanism, which is needed to avoid lock-out of a mobile device when errors occur.

The serving network operator also trusts that the one-time authentication information provided via the HSS in the home network is sufficient to authenticate any unique UE associated with it.

In addition, the home network operator trusts the serving network operator to provide correct charging information related to the services used by the UE according to the roaming agreements between the two operators.[27]

The RAN connects to the serving network (a component of the core network) to provide users with access to network functions. The serving network provides the actual connectivity and mobility. Before granting service, it authenticates the UE through a Mobile Management Entity (MME), a component within the serving network. The serving network also routes calls and transports data from source to destination by interacting with the transit network for non-user specific data or services purposes.[28]

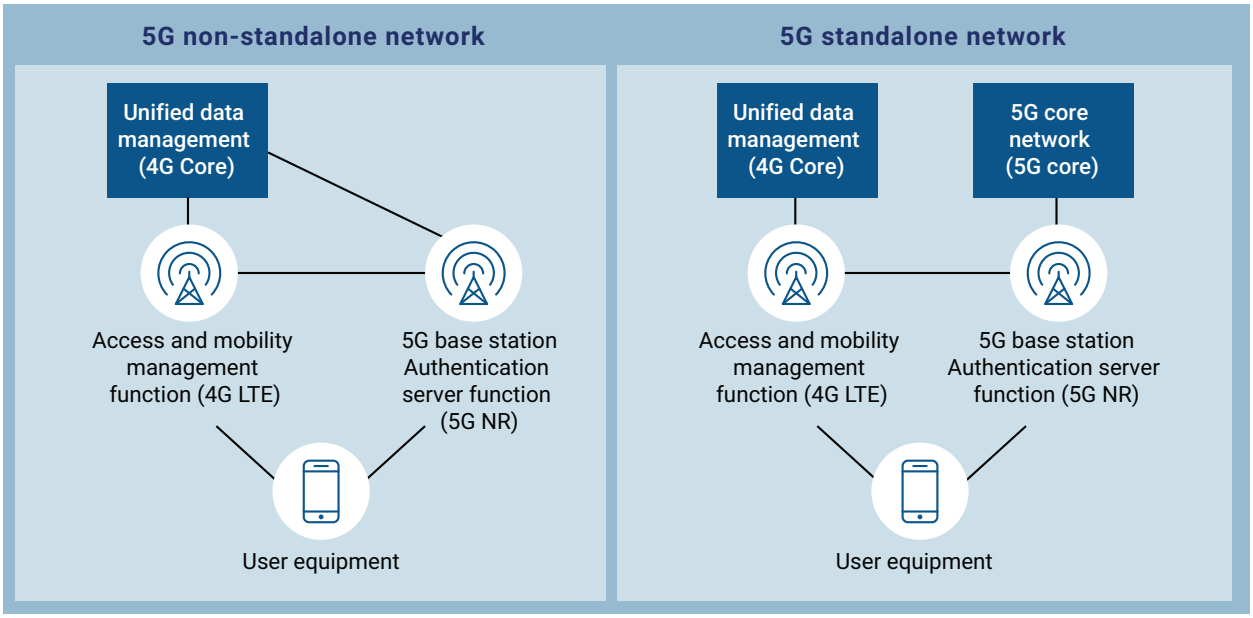
Finally, the transit network represents the core network section that provides communication between the serving network and remote parties.[29]

## 5G Network Structures

As shown in **figure 7**, 5G network service providers offer two types of 5G network structures when transitioning from 4G to 5G technology: non-standalone network (NSA) and standalone network (SA).

While NSA is a suitable structure if the 5G service provider mainly intends to deliver high-speed connectivity to users of 5G-enabled devices, SA is a better choice for 5G service providers that intend to provide new services, such as smart factories.[30]

**FIGURE 7:** Two Types of 5G Network Structures




[25] *Ibid.*
[26] Norrman, K.; M. Naslund; E. Dubrova; "Protecting IMSI and User Privacy in 5G Networks," ACM, 12 December 2016, https://eudl.eu/doi/10.4108/eai.18-6-2016.2264114
[27] *Ibid.*
[28] *Ibid.*
[29] *Op cit* ETSI
[30] Ekström, H.; "Non-standalone and Standalone: two standards-based paths to 5G," Ericsson Blog, 11 July 2019, https://www.ericsson.com/en/blog/2019/7/standalone-and-non-standalone-5g-nr-two-5g-tracks

## Network Slicing

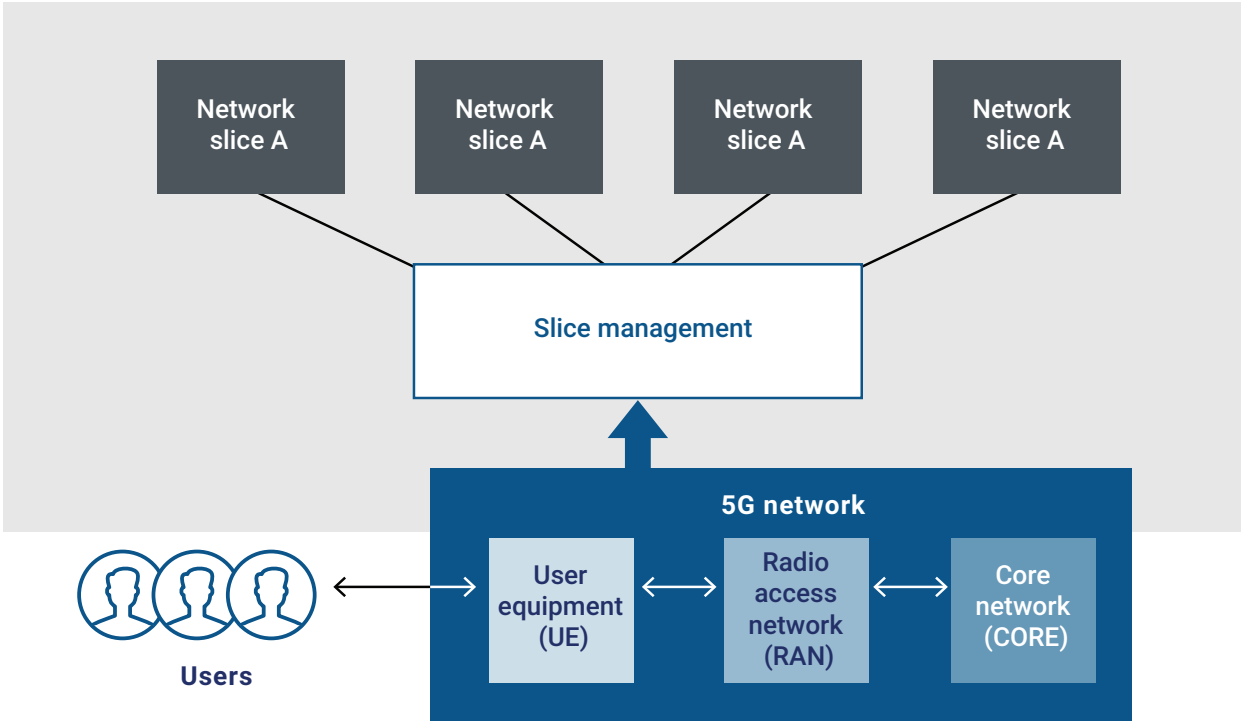
One of the most innovative aspects of 5G network architecture is network slicing, which allows an independent end-to-end virtual network to run on a shared physical infrastructure capable of providing services customized to a subscriber's specific requirements and based on a negotiated agreement between the 5G service provider and the customer, as shown in **figure 8**.

Essentially, network slicing entails running multiple virtual networks as independent business operations on a common physical infrastructure in an efficient and economical way. The segmentation of a single physical network into multiple virtual networks allows business customers with different and sometimes conflicting needs to enjoy connectivity and data processing tailored to specific business requirements, all while adhering to a service level agreement (SLA) with the 5G network provider.[31]

To a subscriber/user, a virtual sliced (i.e., logical) network appears as a single network. However, rather than an entirely separate and self-contained isolated network, it could be either a portion of a larger physical network or a combination of multiple separate physical networks.

A network slice can span multiple parts of the network (such as radio access network, core network and transport network) and be deployed across multiple 5G operators. It also can incorporate dedicated and/or shared resources (such as processing power, storage and bandwidth) and customized network capabilities (such as data speed, quality, latency, reliability, security and services).[32]

**FIGURE 8:** Network Slicing



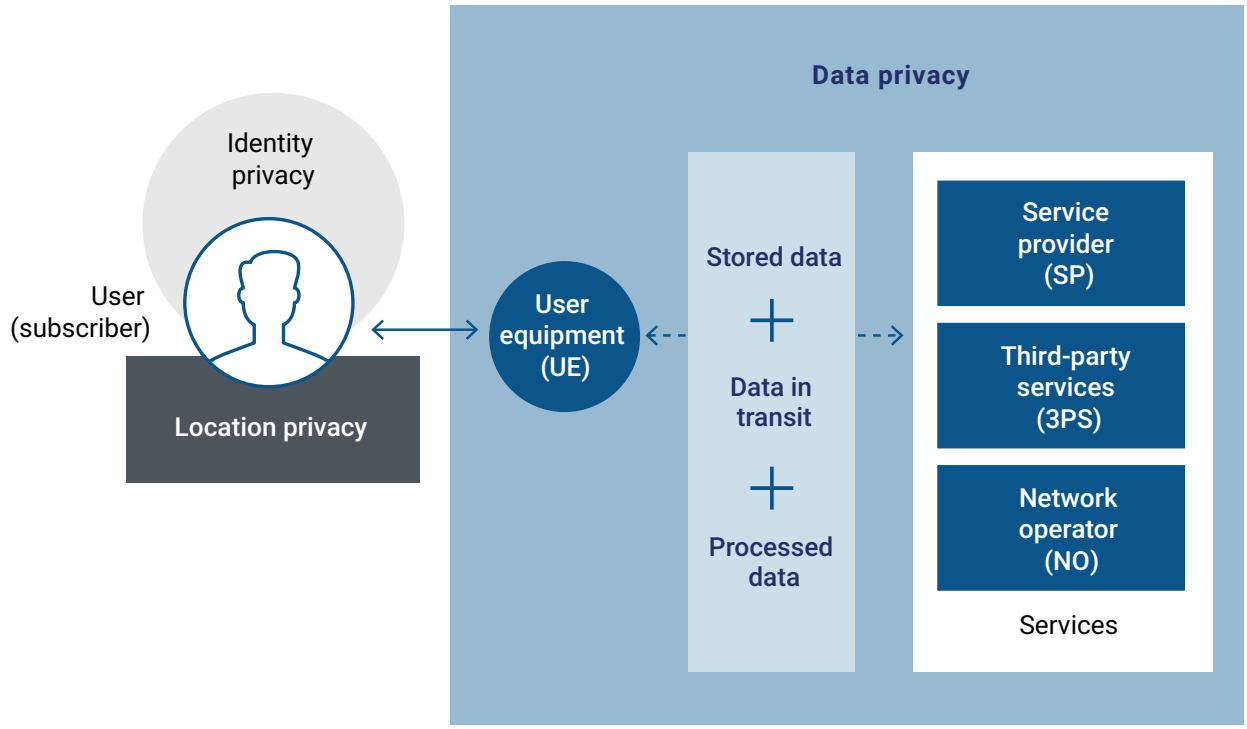

[31] *Op cit* ISACA
[32] GSMA, "An Introduction to Network Slicing," https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf

# User Privacy Elements

As shown in **figure 9**, privacy on the 5G network can be divided into three main categories:

- **Data privacy**—Data privacy refers to the confidentiality and privacy of stored data. With heaps of smart and heterogeneous devices residing on and connected to each other on a 5G network, the network will have a huge volume of data, including sensitive banking and financial information (e.g., data generated by the banking industry).
- **Location privacy**—With the introduction of 5G, several service providers constantly track the location of users who access services via the network. Through this tracking, these providers can infer the habits and routines of the users to improve existing services and offer new user-friendly services. However, if actors other than these providers continuously track users via devices embedded in the 5G network, serious location privacy issues could result. For example, MoviePass®, a movie ticketing subscription service, offered members the chance to see one non-3D movie a day for just US$9.95 per month. The service gained traction and its success was often credited to its use of big data being stored on the network. Although its privacy policy stated that MoviePass would only use customers' location data to help them find local theaters in their neighborhood, during a keynote at the Entertainment Finance Forum, CEO Mitch Lowe said "...we watch how you drive from home to the movies. We watch where you go afterwards, and so we know the movies you watch. We know all about you." This led to an uproar by customers who believed that MoviePass was tracking their movements without their consent.[33]
- **Identity privacy**—Identity-related information associated with a device, system or individual must be provided to and used by a 5G network to establish a connection.[34] When requesting digital services, users often prefer not to reveal their identity to other users or service providers on the 5G network. Numerous services, such as those that require online registration, may reveal the real identity of users and pose a possible threat to identity privacy.

**FIGURE 9:** User Privacy Elements



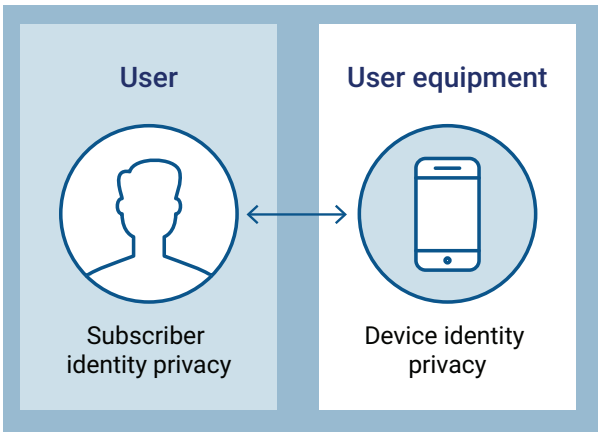

[33] Romano, A.; "MoviePass's fuzzy business model includes tracking users' locations," Vox, 7 March 2018, https://www.vox.com/culture/2018/3/7/17087048/moviepass-big-data-collection-tracking
[34] Khan, R.; P. Kumar; D. Jayakody; M. Liyanage; "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, 2020, https://ieeexplore.ieee.org/document/8792139

As shown in **figure 10**, identity privacy is made of the following components:

- Subscriber identity privacy: privacy of the user's personal identity on the 5G network
- Device identity privacy: privacy of the device used to connect to and request services on the 5G network

The identity-related information associated with a device, system or individual must be provided to and used by a 5G network to establish a connection.

**FIGURE 10:** Identity Privacy




# 5G Privacy Threats and Mitigating Mechanisms

This section addresses 5G privacy threats and some means to address them, including both privacy mechanisms that can be implemented via the 5G network and policies that can be adopted by the 5G network operators and service providers. **Figure 11** provides an overview of the 5G-related privacy threats and corresponding means to mitigate them.

**FIGURE 11:** Identified Threats and Mitigating Means

| Existing Privacy Threats and Mitigating Means | | |
|---|---|---|
| **Threats** | **Mitigating Controls** | |
| | **5G Privacy Mechanism** | **Regulations/Policies** |
| 1. Identity privacy exposure (user identity catching) | Subscription concealed identifier (SUCI) implementation | |
| 2. Risk of unauthorized data access and data breaches:<br>• High-level data transmission rate<br>• Responsibility ambiguity/loss of data ownership<br>• Trust objective issues<br>• Bidding-down attack<br>• Man-in-the-middle attacks<br>• Third-party issues | • Most advanced encryption system adoption<br>• Transport Layer Security (TLS) in 5G standalone deployment<br>• High-level alert system provision for data breaches<br>• Network authorizations<br>• Dynamic and continuous consent<br>• Processes/notifications<br>• Transparency and traceability mechanisms<br>• RAN data compromise risk<br>• Network slicing allocation | • Downward review of data breach timeline<br>• Personal data ownership or licensing structure implementation<br>• Data requests aligning with data protection regulations<br>• Clearly defined roles/responsibilities |
| 3. Issues in transboundary data flow (transborder privacy requirement differences) | | Adoption of:<br>• Transfer impact assessment (TIA)<br>• Hybrid data location storage |
| **Future Unaddressed Threats** | | |
| • Location identity exposure | | |
| • De-conceal SUPI identity using artificial intelligence | | |

# Threat 1: Identity Privacy Exposure

User identity exposure (user identity catching) is an attack that aims at revealing the identity and location of users by capturing their assigned unique identifier (TMSI or GUTI) using an International Mobile Subscriber Identity catcher (IMSI catcher).[35]

The TMSI is the user's temporary and unique identifier, used by networks such as GTM/ 3G prior to the arrival of the 4G Long-Term Evolution (LTE) network. GUTI (Global Unique Temporary Identifier) is the temporary identifier used by the LTE network. The IMSI is the permanent mobile subscriber identity assigned by the network provider to UE once the user registers it on the network. A TMSI is temporarily assigned to a UE for privacy purposes after the serving network has authenticated a user using the IMSI and is therefore the identifier for the specific UE in further communication.[36] These temporary identifiers consist of both the identity of the user and the home network the user is subscribed to and can be used to track the user's location.[37]

Despite TMSIs and GUTIs being used to hide user identities, attackers can still compromise user privacy. This is because TMSIs are reused by the network and GUTIs are reallocated infrequently—typically only when a GUTI reallocation event occurs in the network. In the meantime, an attacker can eavesdrop on the network and retrieve and use these identifiers to track a user's identity and location.

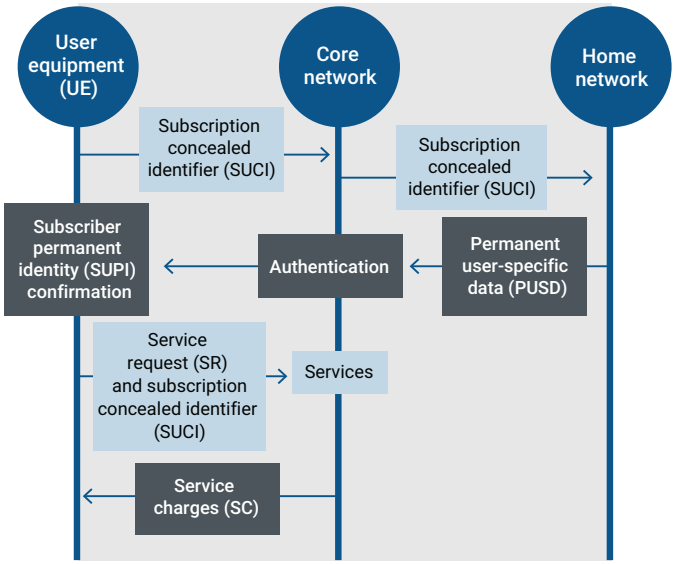
## Mitigating Mechanism for Identity Privacy Exposure and IMSI Catching

To mitigate the threats of user identity exposure (user identity catching), 5G provides enhanced subscriber privacy through a new feature, the subscription concealed identifier (SUCI). This feature replaces the IMSI used in previous mobile networks.

Users connect to the 5G network via RAN using UEs. A UE represents a subscriber's mobile device, such as cellphone or tablet. Each UE is assigned a subscriber permanent identity (SUPI), which uniquely identifies a device connected to the 5G network. Unlike a GUTI, which is a temporary identifier, a SUPI is a never-changing permanent identity.

As shown in **figure 12**, once connected, the UE provides the SUPI in temporal concealed form, known as subscription concealed identifier (SUCI), and transfers this concealed permanent identity over the air via a 5G network.

**FIGURE 12:** SUCI Implementation




[35] *Op cit* Norrman et al.
[36] *Ibid.*
[37] Hong, B.; S. Bae; Y. Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier," Network and Distributed Systems Security (NDSS) Symposium 2018, February 2018, https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_02A-4_Hong_paper.pdf

The SUCI is an encrypted identifier generated via SUPI encryption schemes, which are ECIES Profile A and ECIES Profile B.[38] This mechanism requires users' devices to identify themselves during the network connection process using the SUCI identifier.[39]

This concealment implements identity privacy and ensures that the user's geographical presence and mobile connections are untraceable to eavesdroppers. This unlinkable temporary ephemeral privacy-preserving SUCI makes it infeasible for it to be used to deduce the subscriber's permanent identity.[40]

## Threat 2: Unauthorized Data Access Threat and Data Breaches

Following are examples of threats related to data access and data breaches:

- **High-level data transmission rate**—5G is a platform on which various business applications reside, and therefore it supports multiple stakeholders—such as operators, service providers, enterprises and new technologies—with new business models that continuously use, store and process a high volume, variety and velocity of personal data from consumers. This means that more of users' personal data go through the hands of multiple providers[41] and therefore are vulnerable to privacy breaches.[42] This could negatively impact data-sharing consent processes, data rectification and erasure rights, and early data breach notification policies to avoid business reputation damage

When part of the 5G network is migrated to the cloud, stakeholders have distinct trust objectives based on their own policies and/or regulations.

- **Shared environment/responsibility ambiguity/loss of data ownership**—The 5G network consists of shared network infrastructure or virtual networks on which applications owned by various organizations interact with each other. Even though these applications have multiple application controls, there may be an existing risk of unauthorized data access and exchange resulting from an access control gap due to the shared nature of the network. In addition, if a threat occurs leading to personal data loss on the shared network infrastructure, there will be difficulty in identifying which stakeholder is responsible for such loss since the ownership of the data in transit from one application to another within the shared 5G network has not been defined.
- **Different trust objectives/privacy goals and interest issues**—When part of the 5G network is migrated to the cloud, stakeholders have distinct trust objectives based on their own policies and/or regulations. These policies allow a user in one network domain to access resources in another network domain based on the latter domain trusting that the authority of the other domain has authenticated its users.

Concealment implements identity privacy and ensures that the user's geographical presence and mobile connections are untraceable to eavesdroppers.

The issue is that these implemented trust policies might not consider all aspects of consumer data privacy, resulting in unauthorized access to personal user data.[43]

[38] Tea, V.; "Unmasking Concealed 5G Privacy Identity with Machine Learning and GPU in 12 mins," TechRxiv, 4 November 2020, https://doi.org/10.36227/techrxiv.13187636.v1
[39] *Op cit* ISACA
[40] *Op cit* Tea
[41] *Op cit* Liyanage, et al., "5G Privacy"
[42] *Op cit* Khan et al.
[43] *Ibid.*

- **Different privacy/commercial/national security interests—** These are subject to different regulations and have related obligations to provide legal communications to law enforcement bodies in different regions. Such obligations could lead to privacy issues.[44]

5G technology providers should continuously embrace the most advanced encryption systems. These systems should guarantee encrypted communications from one 5G network to another and protect 5G procedures and data transmission.

- **Bidding-down attack—**This is a form of cryptographic attack that falsely represents that the network does not support a high-quality feature such as an encrypted authentication/authorization connection. It thereby forces user devices (and the network entities they connect to) to accept a lower-quality mode of operation, such as a cleartext authentication/authorization connection, which makes it easier for an attacker to retrieve personal data for malicious purposes.
- **Man-in-the middle attacks—**Hackers can use their status as trusted network nodes to carry out man-in-the-middle attacks, which involve sending malicious commands to connected devices to force the use of a lower-quality mode of operation, such as a cleartext authentication/authorization connection. An attacker can then illegally retrieve users' personal data more easily.[45]
- **Third-party issues—**5G network deployment will lead to an explosion of new services and a significant increase in agents of device manufacturers, network operators and service providers (i.e., application designers and those who might be involved in the deployment of new 5G applications) who will be granted permissions to access the 5G network and may be involved in personal data processing activities.[46] This access might lead to unauthorized disclosure or to selling extracted personal user data. For example, the US Health Insurance Portability and Accountability Act (HIPAA) allows the sharing of an individual's health data in specific contexts. The information-sharing rule in a cloud network can significantly invoke data-privacy issues.[47] In addition, this could lead to ambiguity problems regarding responsibility for data being processed or in transit since responsibility for each of the parties could be diluted.[48]
- **RAN data compromise risk—**The radio units (RUs), distributed units (DUs) and central units (CUs) of base stations in the RAN are collocated or distributed in various configurations and deployed as virtual network functions (VNFs). Both RUs and DUs sit at the edge of the network, so network operators can deploy them in unmanned locations with minimal security. This produces the risk of leaving sensitive data vulnerable to physical attacks if they are sent through the RUs/DUs unencrypted or if the RUs/DUs possess keys used to decrypt them.

## Mitigating Controls for Unauthorized Data Access Threat and Data Breach

Based on 5G's higher speeds and data rate, the time limit for notification of a data breach should be reduced.

### Preventive controls include:

- 5G technology providers should establish advanced dynamic and continuous consent processes and notifications that guard users' rights to rectification, erasure and notification.
- 5G technology providers should continuously embrace the most advanced encryption systems. These systems should guarantee encrypted communications from one 5G network to another and protect 5G procedures and data transmission. Currently, 5G implements 256-bit encryption, which is a substantial improvement over the 128-bit standard used by 4G.
- As shown in **figure 13**,[49] 5G implements the Transport Layer Security (TLS) protocol, which employs encryption to provide end-to-end security of data sent from one 5G network function to another, ensuring that eavesdroppers and hackers cannot see private and sensitive data sent and therefore promoting data integrity.[50]

[44] Agencia Espanola Proteccion Datos (AEPD), "Introduction to 5G Technologies and Their Risks in Terms of Privacy," https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf
[45] *Op cit* ISACA
[46] *Op cit* Agencia Espanola Proteccion Datos
[47] *Op cit* Khan et al.
[48] *Op cit* Agencia Espanola Proteccion Datos
[49] Henda, N.; M. Wifvesson; C. Jost; "An overview of the 3GPP 5G security standard," Ericsson Blog, 17 July 2019, https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview
[50] *Ibid.*

- Organizations can allocate different parts of their 5G network to accommodate various data privacy needs. For example, a hospital could slice its network into dedicated segments for protected health information, payment data, other personally identifiable information and less sensitive data (**figure 14**). The hospital could then tailor security and privacy controls for each network slice based on the sensitivity of data and other compliance requirements.[51]

**FIGURE 13:** 5G Transport Layer Security (TLS)

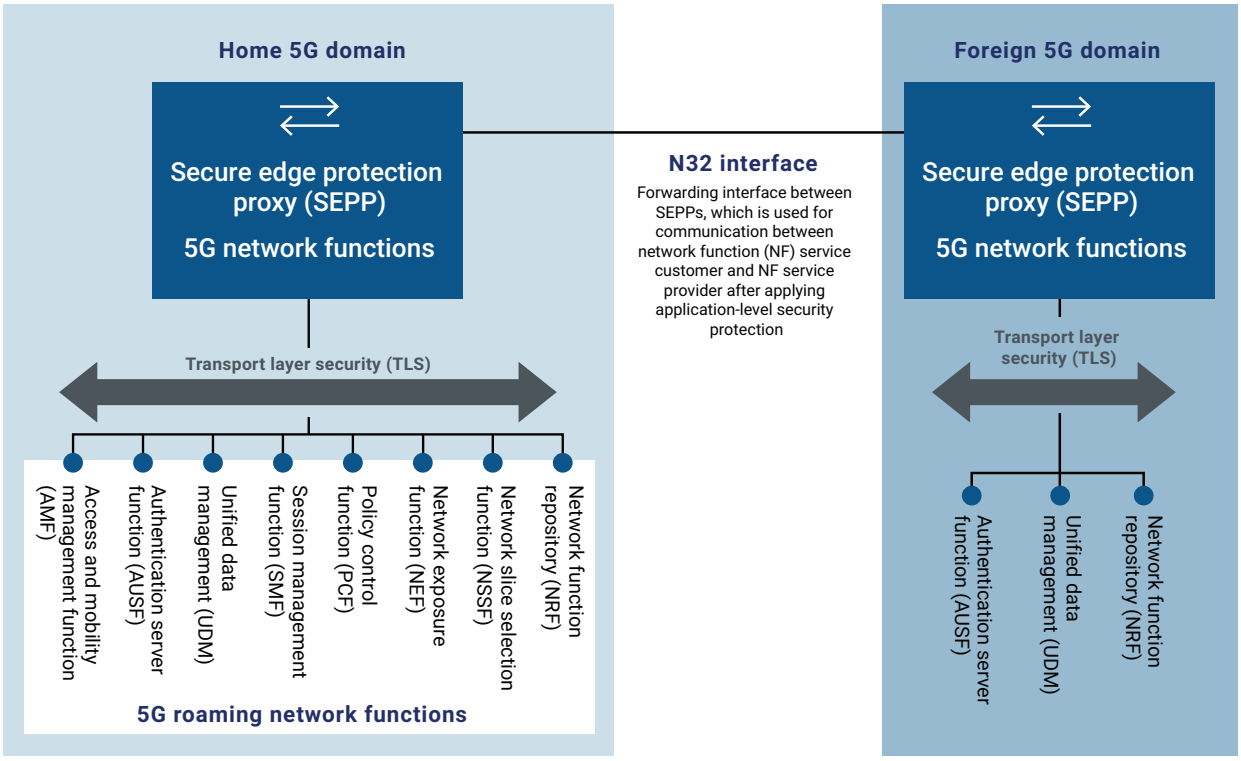
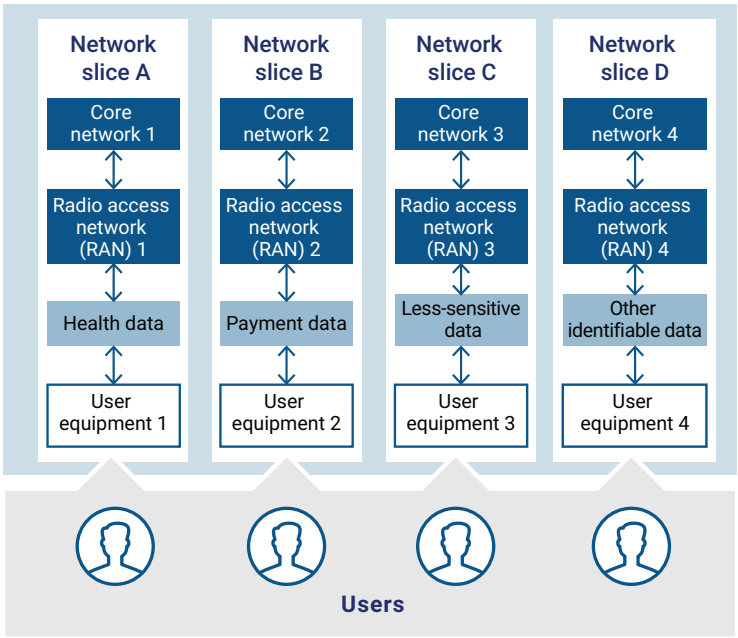



**FIGURE 14:** A Hospital's 5G Network Slicing Allocation




[51] Fancher, D.; W. Frank; S. Dayekh; P. Jyoti; D. Alvarez Molina; "5G Security, Privacy Improvements to Build Network Trust," *The Wall Street Journal* and Deloitte, 11 June 2021, https://deloitte.wsj.com/articles/5g-security-privacy-improvements-to-build-network-trust-01623438054

- Responsibility for ownership or licensing of personal information must be clearly assigned/defined between the different stakeholders (i.e., mobile network operator, service providers and third parties).[52]
- During and after deployment of new 5G-based applications and services, all agent requests for access to user personal data must align with data protection regulations. Access requests must be clear and understandable regarding data controllers, the purpose of the requested data, and access and use of control measures by users.
- Roles and the corresponding scope of responsibility with respect to data protection should be carefully defined among developers, providers, operators and agents. [53]
- To mitigate the threat of data breaches, the 5G network implements network authorization as follows:
  - Serving network authorization by the home network: The UE home network authorizes a serving network before the serving network provides services to the UE.
  - Radio access network authorization: The serving network authorizes the UE's radio access network before providing services to the UE.

**Detective controls include:**

- 5G technology providers should establish a high-level alert system for data breaches.[54]
- Transparency and traceability mechanisms need to be implemented in both of the following cases:
  - Connection of devices to 5G services
  - Distribution processing

## Threat 3: Issues in Transboundary Data Flow

Due to global digitalization, personal data have become the lifeblood of the modern market, and will freely flow across borders. Because 5G captures a larger amount of data at a more granular level, if and when 5G-captured data cross boundaries, the amount of information crossing borders is magnified, and the risk of revealing sensitive information about a person may increase.

As data freely flow, it is crucial to mandate individual or government consent for data transfers, including how information may be processed and stored across borders.[55]

In this increasingly globalized world, where markets for goods and services span national borders, national safeguards and rules for personal data protection may not offer as much protection as intended, as technology allows data to be whisked out of a national jurisdiction at the click of a mouse. Once whisked off, data can be collected, stored and transmitted, then exchanged or sold. Therefore, the ability of individuals to control what information is known about them and by whom is compromised and ultimately could lead to the creation of a surveillance society.

In this increasingly globalized world, where markets for goods and services span national borders, national safeguards and rules for personal data protection may not offer as much protection as intended, as technology allows data to be whisked out of a national jurisdiction at the click of a mouse.

For example, the government of the Canadian province of British Columbia proposed to contract out the administration of its public health insurance, the Medical Services Plan, to a Canadian subsidiary of an American company. Opponents argued that doing so would give United States agencies, including the Federal Bureau of Investigation (FBI) the ability to obtain personal information about Canadians from American companies as a result of provisions in the United States Patriot Act. The dispute resulted in litigation, an amendment to Canadian legislation, and a comprehensive investigation by the office of the Commissioner of Information and Privacy for British Columbia.[56] This scenario illustrates how data that cross a border may be used or accessed

[52] *Op cit* Khan et al.
[53] *Op cit* Agencia Espanola Proteccion Datos
[54] *Op cit* Scientific Foresight Unit (STOA)
[55] *Op cit* Khan et al.
[56] Gunasekara, G.; "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows," *International Journal of Law and Information Technology*, Volume 17, Issue 2, Summer 2009, https://academic.oup.com/ijlit/article/17/2/147/914150

and that the data's country of origin may not be able to override processing practices in another country.

## Mitigating Controls for Transboundary Data Flow Issues

**Preventive controls include:**

- Standards that assess the impact of the exorbitant number of connected devices and services residing on the 5G platform, especially those devices and services provided within the media and entertainment sector, could help address cross-border data transfer issues. These standards should consider how data matching, correlation and information extraction should be performed to profile and track users through their devices.[57]
- Different regions/countries should establish a controller/processor within their jurisdictions and encourage legal departments to perform a transfer impact assessment (TIA). Conducted by a controller or a processor, a TIA is a written analysis of the impact cross-border transfers have on personal user data privacy.[58]
- A hybrid approach (hybrid data location storage) ensures that personal or sensitive data are stored locally, close to and within an individual's national boundaries (edge cloud), with less sensitive data stored in the international cloud.[59]

**SEPP ensures that wireless users (subscribers) maintain the same high level of security they have on their own carrier's network when they roam to another carrier's network, whether in their own country or while traveling abroad.**

- A third-party data transfer agreement should be established between associated parties with regard to personal data being transferred to or accessed in a third country. The agreement could be between a 5G network controller and a 5G data processor, a 5G data processor and a 5G data subprocessor, or any other combination of parties.

This agreement acts as a baseline for safeguards that address:

- Legality of the transfer itself
- Processing of personal data
- Compliance with established privacy regulatory requirements.[60]

- A new 5G network function, Secure Edge Protection Proxy (SEPP), secures interconnecting traffic between roaming partner networks by hiding network topology and traffic, exchanging certificates, and providing application security as needed.[61] Roaming refers to a user requesting services from a foreign network (i.e., a visitor network in a geographical region outside the area covered by the network to which the user is subscribed [home network]). SEPP has three features:
  - All traffic between networks is routed through security proxies.
  - Authentication between SEPPs is required to ensure effective filtering of traffic coming from the interconnect.
  - New application layer security solution on the N32 interface between the SEPPs provides protection of sensitive data while allowing mediation services throughout the interconnect.[62]

SEPP ensures that wireless users (subscribers) maintain the same high level of security they have on their own carrier's network when they roam to another carrier's network, whether in their own country or while traveling abroad. In addition, SEPP's cross-network authentication is performed within subscribers' home countries. SEPP permits better privacy procedures than the legacy signaling protocols used in 4G and 3G.[63]

[57] *Op cit* Scientific Foresight Unit (STOA)
[58] Zetoony, D.; "What exactly is a 'Transfer Impact Assessment' (TIA), and where the heck did it come from?," *The National Law Review*, 30 March 2022, https://www.natlawreview.com/article/what-exactly-transfer-impact-assessment-tia-and-where-heck-did-it-come#:~:text=The%20term%20has%20come%20to,afforded%20to%20the%20transferred%20data.
[59] *Op cit* Scientific Foresight Unit (STOA)
[60] Lyons, L.; T. Mackay-Temesy; "Data transfer agreements," TaylorWessing Global Data Hub, July 2018, https://globaldatahub.taylorwessing.com/article/data-transfer-agreements,
[61] *Op cit* Henda et al.
[62] *Ibid*.
[63] *Op cit* Fancher et al.

# Possible Future Unaddressed Threats

If the following remaining threats are not addressed, they will linger, possibly compromising privacy in the next-generation network, 6G.

- **Location identity exposure**—5G network technology intensifies the existing threat of location exposure. Anyone with access to a 5G base station (cell tower) will be able to track a subscriber's exact location far more precisely than possible with the 4G network because the 5G network's base station covers a smaller geographical area than that of the 4G network. This means that dozens of base stations will be placed close to each other within a geographical coverage area that just one 4G base station would have covered in the past.

**5G network technology intensifies the existing threat of location exposure.**

Each time a user connects to a base station within a cellular network, the network is aware that the user is within range of that base station. With a 4G network, the network provider can pinpoint the user's location only within a mile's accuracy, which means the user's precise location is obscure. But since more 5G towers exist within close range, the 5G network will be able to pinpoint a user's location much more accurately.[64]

- **De-conceal SUPI identity using artificial intelligence**—Although the 5G network protects Subscriber Permanent Identity (SUPI) privacy by concealing the user's permanent identity via encrypted unlinkable SUCI, research has shown it is possible to accurately link a SUCI-concealed identity to the unconcealed permanent SUPI. This can be done using artificial intelligence without having to de-conceal the SUPI identity. Eavesdroppers can monitor and capture all SUCIs at any given point in time and at multiple locations. Because only one SUCI concealing a unique SUPI can be sent at any point in time, it is easy to determine who and where a user is. Since SUCI is the 5G standard currently being used, this threat affects all 5G-compliant user equipment (e.g., cellphones, IoT devices and base stations) that utilize SUCI.[65]

# Conclusion

The full transformative potential of 5G technology and its successful implementation and acceptance depend on the earned trust of stakeholders. Therefore, it is mandatory that existing privacy threats be appropriately addressed. Identification and assessment of future privacy threats should be ongoing. Improved threat mitigation requires development of the means to address identified threats before they materialize.

[64] Grothaus, M.; "5G means you'll have to say goodbye to your location privacy," Fast Company, 1 March 2019, https://www.fastcompany.com/90314058/5g-means-youll-have-to-say-goodbye-to-your-location-privacy#:~:text=However%2C%20there%20is%20one%20major,today%20under%20our%204G%20networks.
[65] *Op cit* Tea

# Acknowledgments

ISACA would like to recognize:

## Lead Developer

**Ronke Oyemade**
CISA, CISM, CRISC, CDPSE, PMP
Strategic Global Consulting LLC, USA

## Expert Reviewers

**Srinivasan Chinnelli**
CISA, CDPSE, CIA, CRMA
JPMorgan Chase & Co., Philippines

**Joyce Chua**
CISA, CISM, CGEIT, CDPSE, CAEG (Professional), CFE, CIA, CIMP, CIPM, CIPP(A), CIPP(E), FIP, IRCA, ISMS Associate Auditor, ITIL, MCP, PMP
UOB, Singapore

**Blake Curtis, Sc.D.**
CISA, CISM, CGEIT, CRISC, CDPSE, COBIT, CISSP
Deloitte, USA

**Shamik Kacker**
Dell Technologies
USA

**Kanupriya Parab**
CISA, CISM, CRISC, CDPSE
Canada

## Board of Directors

**Pamela Nigro, Chair**
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

**John De Santis, Vice-Chair**
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

**Niel Harper**
CISA, CRISC, CDPSE, CISSP
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, Germany

**Gabriela Hernandez-Cardoso**
Independent Board Member, Mexico

**Maureen O'Connell**
NACD-DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

**Veronica Rose**
CISA, CDPSE
Senior Information Systems Auditor–Advisory Consulting, KPMG Uganda, Founder, Encrypt Africa, Kenya

**David Samuelson**
Chief Executive Officer, ISACA, USA

**Gerrard Schmid**
Former President and Chief Executive Officer, Diebold Nixdorf, USA

**Bjorn R. Watne**
CISA, CISM, CGEIT, CRISC, CDPSE, CISSP-ISSMP
Senior Vice President and Chief Security Officer, Telenor Group, USA

**Asaf Weisberg**
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

**Gregory Touhill**
CISM, CISSP
ISACA Board Chair, 2021-2022
Director, CERT Center, Carnegie Mellon University, USA

**Tracey Dedrick**
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

**Brennan P. Baybeck**
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

**Rob Clyde**
CISM, NACD-DC
ISACA Board Chair, 2018-2019
Independent Director, Titus, Executive Chair, White Cloud Security, Managing Director, Clyde Consulting LLC, USA

## About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its more than 165,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

### DISCLAIMER

ISACA has designed and created *5G Privacy: Addressing Risk and Threats* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

### RESERVATION OF RIGHTS



ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

**Phone:** +1.847.660.5505

**Fax:** +1.847.253.1755

**Support:** support.isaca.org

**Website:** www.isaca.org

**Provide Feedback:**

www.isaca.org/5g-privacy-risk-threats

**Participate in the ISACA Online Forums:**
https://engage.isaca.org/onlineforums

**Twitter:**
www.twitter.com/ISACANews

**LinkedIn:**
www.linkedin.com/company/isaca

**Facebook:**
www.facebook.com/ISACAGlobal

**Instagram:**
www.instagram.com/isacanews/