INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

The Right to Be Forgotten in The Context of Mobile Number Recycling

Motunrayo Adebayo

Indiana Wesleyan Univeristy

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1408000129

Received: 13 Aug 2025; Accepted: 20 Aug 2025; Published: 13 September

Abstract*:* Mobile phone number recycling, the process of reassigning deactivated numbers to new users after a designated period, is a necessary practice for managing the limited pool of available numbers in the face of growing demand. While efficient for mobile network operators, this process can leave residual links between the recycled number and its previous owner's digital footprint. These leftover risks can lead to the new owner receiving calls, messages, or notifications intended for the former owner of such mobile numbers, creating issues relating to privacy and security, such as identity theft and fraud. The aim of this work is to review security and regulatory provisions relating to mobile phone recycling, identifying gaps and proffering solutions to further protect privacy in this aspect.

Key words: Mobile number recycling, privacy, information security

I. Introduction

The need for recycling mobile numbers stems from the need of telecommunication companies to manage the finite supply of phone numbers amidst the growing demand for such numbers. However, when a phone number is recycled, the digital footprint of the former owner might still remain. This means the new user might receive messages or service attempts intended for the former user posing privacy and security concerns. This especially applies to businesses that heavily depend on mobile phone numbers for the purpose of identity verification and/fraud prevention.

A phone number is more than just a method of communication, it is an integral part of a person's personal and professional identity. The lifecycle of a phone number starts from when it is assigned to a user, being used for calls and other usages. Once the number is no longer in use, it goes to a dormancy period before reassignment. The dormancy period can last from a few months to many years and this depends on the policy of the service provider. While dormant, calls to the number typically receive a "no longer in service" message, allowing time for a clean separation between the former and future user. As a result of the huge demand for phone numbers, there is the issue of *phone number exhaustion.* As a result of the scarcity of numbers to pool from, NANPA in 2019 warned that by 2025, telecoms companies might run out of numbers to assign, and as a result , the need for phone number recycling (this applies globally). Carriers, especially the major ones have determined timelines between dormancy and reassignment of these numbers. For instance, Verizon may recycle a number after 30 days of dormancy, while AT &T waits up to 90 days. The Federal Communication Commission (FTC) on a regulatory level, enforces a number again period of up to 90 days for geographic numbers and 30 days for non-geographic ones before reassignment.

There are benefits to the reuse of mobile numbers. Telecommunications company's benefits from this by conserving the limited pool of available numbers, prevent or delay number exhaustion, and save cost involved with reassigning new phone numbers to people, such as infrastructure upgrades and network maintenance. There are also environmental benefits to this. It is therefore a necessity for these companies.

As stated already, the recycling process create serious security and privacy risks which can hram both new and old users. Of these, 8 types of attacks have been identified;

- PII Indexing
- Account hijackings (via recovery or without password reset)
- Targeted takeovers
- Phishing
- Persuasive takeovers
- Spam
- Denial-of service

When these attackers discover recycled numbers through carrier interfaces with minimal restrictions, they can impersonate old users, hijacking accounts or collecting sensitive information.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Upon testing 259 phone numbers from two major US carriers, it was shown that 83% were recycled and 66% were linked to personally identifiable information or some existing online accounts making them vulnerable to hijacking even if SMSM based tow factor authentication was enabled. In addition, 39% of these numbers were linked to breached passwords, allowing hijackers bypass 2FA (Lee & Narayanan, 2021).

In a honeypot experiment with 200 recycled numbers, **almost 10% received sensitive calls or texts within a week**, including one-time passcodes from major platforms and personal data such as medical or banking information. These findings highlight how quickly sensitive communications can reach unintended recipients, giving them opportunities for exploitation (Lee & Narayanan, 2021).

Some of the major causes of these vulnerabilities are linked to inconsistent information about number aging period, adequate public information as well as unlimited prepaid number queries. Solutions to these could include more transparency from carriers, limits on number queries and changes, proactive warnings before recycling and options for number parking to retain control. These should also be limit on how websites rely on SMS based authentication and subscribers should proactively remove old numbers to protect themselves (Lee & Narayanan, 2021).

The purpose of this paper is to explore the security, privacy and compliance issues related to phone number recycling which is the regulated proactive of reassigning deactivated numbers to new users. Looking at the security issue here, such numbers are still linked to online accounts of old owners which can cause issues like PII Indexing, account hijacking via SMS recovery, and account hijacking without password reset. Privacy risks are heightened when recycled numbers appear on people search services, exposing sensitive personal information of former owners and enabling impersonation, fraud, and further data exploitation.

These risks are enhanced by carriers' operational weaknesses, such as lack of query limits, **prepaid number change interfaces** and the public display of full numbers before reassignment, enabling attackers to easily identify and obtain vulnerable numbers. With an estimated **one million recycled numbers available at any given time** and approximately 35 million numbers disconnected annually in the U.S., the attack surface is both large and constantly replenished.

These paper discusses and emphasizes best practices when it comes to telephone recycling eg unlinking numbers before deactivation, using number parking services to maintain control and making use of stronger authentication methods instead of SMS or telephone based authentication methods

How Mobile Number Reallocation Works

Amongst telecommunications companies, there is a structures process followed to ensure an inactive number can be reassigned to a new person; The main stages are:

Deactivation

A customer stops using the number for reasons such as changing providers, upgrading devices, defaulting on payments, account closure or just inactivity (for a determined period of time with no payment) and then the Mobile Network Operator deactivates it.

Dormancy Period

This is the period after deactivation where the number enters a ***holding period*** **(also called or dormancy or aging period)** .It cannot be reassigned during this period and gives the original user the chance to reclaim the number. This period varies from one region to another and also based on the telephone carrier itself. for example, UK operators like EE, Vodafone, and O2 typically use 30–90 days, while high-demand markets may have shorter timelines.

Data Clearing

This is when MNOs make attempts to reset or clear data associated with the number in their systems. However, there might be data remnants especially in third party platforms such as social media, banking apps or messaging services and these can remain tied to the number leading to unintended account access, identity confusion and privacy breaches.

Reassignment

After the dormancy period, the number is added back to the pool of available numbers. The new owner receives the fresh SIM card but same number. However, if third party accounts are still linked to it, they may receive messages, calls or authentication codes intended for the former owner.

This process is the same globally but might be different in how they are executed. If the dormancy period is too short in a high demand area, it increases privacy risks and some jurisdictions have regulatory provisions concerning this (e.g., the FCC in the U.S. mandates a minimum 45-day aging period before reassignment). The regulations are stronger in some regions compared to others. For instance, UK and Germany emphasize strict transparency, while others might not be that structured. This leads to inconsistent timelines.

Dormancy periods are intended to reduce the risk of misdirected communications and account takeovers by ensuring that old data connections fade before a number re-enters circulation. In the U.S., the **Federal Communications Commission (FCC)** mandates

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

a **minimum 45-day aging period** before a number can be reassigned. Carriers often extend this to **45–90 days**, depending on region, operator policy, and demand. In high-demand area codes, this timeline can be shorter, sometimes just weeks, especially in areas with limited number availability leading to higher risks.

While reassignment is going on, the number is given to a new user many times without their own knowledge of prior ownership. This is the point at which security and privacy vulnerabilities become most serious, as online accounts, verification systems, and communications may still link the number to its former user.

If organizations rely on phone number as the only source of authentication or account recovery, the timeline duration becomes important as it indicates need for real time number verification and ownership change detection to reduce fraud, privacy breaches and compliance risks. This is why there should be an adequate dormancy period to avoid privacy and security issues. In the US (FCC), Nigeria (NCC), Uk (Ofcom) all being used as case studies, we can see regulations requiring that a database be updated by telecoms companies so people can check such phone numbers to see if they have been reassigned before using it to contact a person, for authentication and so on. We also see set durations of cooling periods before such numbers are reassigned. In the USA, there is a RND database for this purpose (**Reassigned Number Database).**

Regulations vary globally. For instance in Nigeria, the Nigerian Communications Commission (NCC) enforces a 90 days dormancy rule which aligns with SIM registration requirements under the SIM Registration Regulations 2011 and in the UK the Ofcom Numbering Plan governs allocation, with providers encouraged to allow a 90-day gap before reissue, though not mandated by law. Ofcom also enforces General Condition C7 on number portability and accuracy of subscriber data, helping mitigate risks from reassignment. In the European Union it is guided by the European Electronic Communications Code (EECC) and the aging period is around 90 days as well. Some countries within the EU such as Germany are also commended for having strong rules affecting telephone recycling. However, there is no unified EU system as regards phone recycling which can affect cross border data transfers.

Empirical work shows that most recycled numbers observed in carrier inventories still connected to existing online accounts or to people-search records, enabling receipt of password-reset codes and other sensitive communications intended for prior owners (Lee & Narayanan, 2021a; 2021b). In a controlled measurement, nearly 10% of recycled "honeypot" numbers received one-time passcodes, medical reminders, or bank alerts within a week mainly because services still trusted the phone number as a login or recovery factor (Lee & Narayanan, 2021a). SMS remains a trust anchor, thereby routing authentication requests to the wrong person **(Telesign, 2025).** These inadvertent deliveries enable account access whenever the opportunity arises for malicious actors, through processes like password resets via SMS, data leakage (bank or health messages) and impersonation (the new owner stealing the identity of the old one) **(Lee & Narayanan, 2021c).**

These create legal consent and direct marketing pitfalls. In the US, the TCPA has a requirement of receiving consent before calling or texting a customer. However when these calls go to the new assignee by mistake, there is already a breach and can trigger liability (Manatt, 2021; JD Supra, 2025). In the **EU**, the **ePrivacy Directive** (2002/58/EC) generally prohibits unsolicited electronic communications without consent, making misdirected marketing to a newly assigned number a compliance risk unless a valid legal basis applies (EUR-Lex, 2002; Wikipedia, n.d.). UK guidance on direct marketing and number management further stresses provider due diligence and appropriate controls around assigned numbers (Ofcom, 2025; Ofcom, 2022).

Asides obtaining consent for marketing, **data-protection duties** are implicated when services continue treating a recycled number as if it still identifies the same person. Under the **GDPR**, controllers must observe **data minimization** (collect and retain only what is necessary), **accuracy**, and **storage limitation**; continuing to route security codes to an incorrect person undermines accuracy and necessity (GDPR, Art. 5(1)(c); ICO, n.d.; GDPR-Text, n.d.). It is also imperative that controllers implement appropriate security and authentication measures; if SMS 2FA is retained without verifying ongoing number ownership, residual risk rises (FTC, 2015; FTC, 2021).

In the U.S., the **CCPA/CPRA** provide a **right to delete** personal information (Cal. Civ. Code § 1798.105), which can intersect with recycled numbers: consumers may demand removal or correction where identifiers (like a phone number) cause misattribution or misdirected communications (California DOJ, n.d.; FindLaw, 2023; IAPP, 2020; Osano, n.d.; Spirion, 2020). Broader state privacy trends (e.g., California's **Delete Act** for data brokers) further press organizations to purge stale identifiers and downstream copies when ownership changes, limiting spillover to new assignees (BCLP, 2023; Privacy Rights Clearinghouse, 2024).

The data involved is usually very sensitive. From studies, new owners receive bank alerts, health notifications, school messages and OTPs which are enough for an account takeover without needing any specialized skills. High demand regions can however experience privacy harm blending operational and legal risks. misdirected communications may violate sectoral duties (e.g., health privacy), breach marketing-consent rules (TCPA/ePrivacy), and contravene data-protection principles (GDPR/CCPA) if controllers fail to verify that a number still belongs to the intended data subject (EUR-Lex, 2002; GDPR-Info, n.d.; California DOJ, n.d.).

Mitigation patterns are emerging. On the **governance** side, organizations should: (1) **re-verify number ownership** at key risk moments (login recovery, high-value transactions, periodic account hygiene); (2) **de-emphasize SMS** in favor of app- or hardware-based MFA; and (3) implement **suppression and deletion pipelines** that propagate changes to processors and data brokers (FTC, 2015; FTC, 2021; BCLP, 2023). On the **telecom** side, expanding authoritative reassignment signals (RND-like feeds) and improving transparency on aging policies further reduce misdelivery (FCC, 2021; RND, n.d.). The evidence is consistent: unless

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

services continuously validate that a number still maps to the same person, **new owners will keep receiving old owners' data**—a privacy failure with consent, security, and statutory consequences (Lee & Narayanan, 2021a; Telesign, 2025).

Security Threats from Number Recycling

Account Takeover via SMS-Based Authentication

A major empirical study by Lee and Narayanan (2021) analyzed 259 recycled numbers from major U.S. carriers and found that 66% remained linked to active user accounts, while 39% corresponded with credentials exposed in previous data breaches. This study shows that new owners whether maliciously or accidentally can easily trigger password resets and intercept one-time passcodes (OTPs) which are meant for previous users (Lee & Narayanan, 2021). Despite these risks, industry reliance on SMS-based multi-factor authentication (MFA) persists. The NIST (NIST, 2024) has discouraged the use of SMS as an authentication method due to its vulnerability to interception and takeover and the European Union Agency for Cyber security (ENISA, 2021) has also given a similar warning of "inherent insecurity" of SMS- based 2FA when compared to app or hardware based authenticators.

Reverse Lookup and Identity Reconstruction

Reassigned numbers can be used to expose personal and eve sensitive information of people using platforms such as Reverse Lookup and Identity Reconstruction. Platforms such as BeenVerified can expose information of former owners. Attackers can reconstruct information using publicly available information and information available on social media which can enable identity theft and targeted phishing attacks. These methods capitalize on the diminished unlinking between a number and its prior owner's digital footprint.

SIM Swap Attacks Combined with Number Recycling

This is when fraudsters take over a phone number by tricking telecom providers into issuing new SIM cards. The FBI's Internet Crime Complaint Center (IC3, 2024) reports continued financial losses tied to SIM swaps. In combination with recycled numbers, this attack is amplified. ENISA (2021) notes that such attacks are facilitated by weaknesses in operator processes, insider collusion, and legacy SS7 protocol vulnerabilities.

Security Breach Reporting Obligations

As regards data protection laws, organizations do have legal obligations to report breaches caused by recycled numbers depending on the instance. Many privacy regulations mandates notification to authorities and affected individuals if personal data is compromised (eg GDPR Articles 33 and 34, CCPA and NDPR). These could be triggered if a recycled number results in unauthorized receipt of sensitive information (e.g., OTPs, banking alerts).

Case Studies & Industry Responses

Princeton University Study on Recycled Numbers in the U.S.

Researchers at Princeton University tested 259 numbers available for reassignment from two major USA carriers and found that 83% were previously assigned and vulnerable to at least one exploitation method, such as password resets or identity reconstruction (Lee & Narayanan, 2021). From the study, it was revealed that carriers might lack enough safeguards to prevent attackers from enlisting recycled and available phone numbers through online number changing interfaces, a process made easier through online number changing, a process made easier by the absence of query limits and the display of full candidate numbers.

WhatsApp and Rapid Reassignment Vulnerability

A known vulnerability in WhatsApp's account registration system, previously reported by The Verge (Newton, 2020) found that new owners could gain access to prior owners' WhatsApp account without password knowledge causing unauthorized access to contact, messages and media. This is because WhatsApp relies mainly on phone numbers for identity, the platform could automatically log the new number into the old account through SMS verification.

Meta and Other Tech Companies' Mitigation Measures

Meta acknowledged number risks in it help center guidance with a recommendation that users update contact information before deactivation of a number (Meta, 2023). A similar incident occurred with Google where security prompts were implemented encouraging users to add backup email addresses and secondary verification methods (Google, 2023).

Researchers have however noted that these measures are voluntary and inconsistently adopted, limiting their effectiveness (ENISA, 2021).

Telecom Operators' Policy Adjustments

Due to regulatory pressure and public incidents, some carriers decided to extend dormancy periods to reduce reassignment risks. An example is that of AT&T increasingly their standard of dormancy to 90 days. while UK operators such as Vodafone adopted a minimum 90-day buffer in compliance with Ofcom guidance (Ofcom, 2021). Although these adjustments are great steps, they do not fully address global inconsistencies in recycling timelines, which still range from 30 days in some parts of the world.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Regulatory & Legal Landscape: Privacy Protections During Phone Number Deactivation and Recycling

Telecommunications laws in various jurisdictions impose obligations on carriers to safeguard personal information throughout this process.

United States

The Federal Communications Commission, the principal regulator of telecommunications within the United States under U.S. Under **47 U.S.C. § 222** (Customer Proprietary Network Information, or CPNI rules), provides that carriers must protect the confidentiality of subscriber information, including details that can be linked to a phone number after it has been deactivated. Thereby ensuring that all data linked to a phone number such as call records, voicemails, and SMS are adequately deleted or disconnected from the phone number before assigning to someone else (FCC, 2023)..

The **Telephone Consumer Protection Act (TCPA)**, 47 U.S.C. § 227, adds another layer of privacy. It prevents having contact with customers without prior consent, which also applies to recycled numbers (Consent is attached to the person in question and not the phone number). This was the purpose of creating the FCC's **Reassigned Number Database (RND)** which became operational November 1st 2021, to reduce wrong number calling and unintentional disclosure of personal data to the wrong person and it is the duty of carriers to report permanently disconnected numbers every month to that platform making sure businesses can check the number status before contacting the subscriber (FCC, 2021).

Failure to follow these rules can result in significant penalties. In 2022, the FCC issued multimillion-dollar fines to carriers that mishandled disconnections and exposed personal data through misdirected communications (FCC, 2022).

United Kingdom & EU

Telecommunications companies are regulated by Ofcom in the UK. They also regulate privacy protections during the number reallocation process. Ofcom's **General Conditions of Entitlement** (Condition C7) obligates providers to manage phone number assignments in a way that protects user data and misdirected communications. Before reassigning a number, carriers must clear any network-level data linked to the number, including voicemail accounts and cloud-based services (Ofcom, 2021). In addition, the **UK GDPR** provides the legal duty on telecom operators to ensure personal data is accurate and up-to-date (Article 5(1)(d)) and to prevent unauthorized access (Article 32). This implies that when a number is deactivated, providers must "unlink" it from any active accounts and delete residual data to avoid accidental disclosure to the new user. Violations can result in fines of up to £17.5 million or 4% of annual global turnover.

European Union

In the EU, the **General Data Protection Regulation (GDPR)** applies to number recycling because a phone number is considered personal data when it can be linked to an identifiable individual. Under **Article 5 ,** the Data Minimization principle requires that personal data be erased when no longer in use for its original purpose. This means providers must delete numbers when they are no longer being used for the purpose for which it was initially collected.

Article 6 on lawful processing requires a valid legal basis for any continued processing of data tied to a deactivated number, which is unlikely to exist once the subscriber relationship ends. **Article 32** obligates providers to implement "appropriate technical and organizational measures" to secure personal data, including clearing SIM profiles, clearing voicemail systems, and preventing new users from accessing the prior owner's linked accounts.

In addition, **ePrivacy Directive** (2002/58/EC) also mandates confidentiality of communications, prohibiting interception or access to stored communications except under lawful authority. This includes preventing accidental access by new number holders.

Nigeria

In Nigeria, the regulatory body for telecommunications carriers is the **Nigerian Communications Commission (NCC)** which regulates this process under the **Numbering Plan Regulations 2019**, and requires a **minimum 180-day quarantine period** before a number is reassigned. During this period, operators must ensure that all personal data linked to the number is deleted or anonymized (NCC, 2019).

The **Nigeria Data Protection Regulation (NDPR)** adds privacy-specific obligations:

Article 2.1(1): Requires that personal data be processed lawfully, fairly, and in a transparent manner.

Article 2.2(3): Mandates the secure destruction of data when no longer necessary.

Article 2.6: Imposes security measures to protect personal data against unauthorized access, alteration, disclosure, or destruction relevant when preparing a number for recycling.

Violations can attract fines up to 2% of annual gross revenue or ₦10 million, whichever is greater.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Privacy Implications Beyond Recycling

A phone number is a ***persistent identifier*** and even when it has been assigned to someone new, it can still be used for ad targeting and profiling even to the new person. Modern adtech routinely "matches" people across sites and devices by hashing stable identifiers most commonly emails and phone numbers to generate universal IDs that can be passed around the programmatic ecosystem. Hashing doesn't truly anonymize these identifiers (they're guessable and reversible at scale), and frameworks like UID2 explicitly rely on hashed phone/email to build trackable tokens for bidding. In practice, that means the *same* number can continue to anchor a profile long after its reassigned. (Federal Trade Commission, Policy Review, Clearcode)

Major platforms such as Meta also encourage the direct use of phone numbers for audience targeting. Meta's custom audiences lets advertisers upload customer lists which include phone numbers which Meta then links with user accounts for targeting and look-alikes creating a durable bridge between the offline world (a CRM or checkout record) and online identity, even if a consumer never typed that number into Facebook themselves. Similar "customer list" uploads appear across ad stacks and third-party tools, reinforcing the role of phone numbers.

Phone numbers are also directly linked with online accounts and social graphs, and many companies have consistently blurred the lines between marketing and security, using numbers collected for the purpose of 2FA or account recovery for marketing as well, even if that wasn't the initial intent of the person giving the number, a practice that has drawn enforcement. Twitter paid $150M after U.S. regulators alleged it used 2FA numbers and emails for advertising; the FTC has also warned that hashing such identifiers doesn't cure the problem. These incidents show how a phone number initially provided to *protect* an account can become a lever for profiling and ad delivery. (Federal Trade Commission, Axios)

Data brokers and "clean rooms" further entrench phone-based linkability. Brokers routinely compare hashed lists from brands and publishers to find the "same person" across datasets; recent U.S. proposals even describe hashed-identifier matching as part of standardized opt-out and deletion workflows. Once matched, downstream actors can infer interests, demographics, or high-risk inferences (credit "propensity," health interests, etc.) and push those back into targeting pipes. Even if a number is later recycled, the identifier may remain embedded in legacy datasets, raising risks for both the previous and the new owner. (advocacy.consumerreports.org).

Research has shown how easily identifiers (and behaviors) can be linked across platforms. Studies have shown that number recycling is linked to a realistic attack path where attacks take over via SMS resets and inadvertent exposure of previous owners' communication, revealing that only a phone number is enough to expose a person's expansive digital footprint. Separately, work on identity linkage and cross-site profiling shows that seemingly "anonymous" accounts remain linkable once a stable handle (like a phone number) is in play. (recyclednumbers.cs.princeton.edu)

Regulatory Limits on Profiling

GDPR. EU law defines profiling broadly and restricts decisions *based solely on* automated processing (including profiling) that produce legal or similarly significant effects (Article 22). Controllers must offer meaningful information about the logic involved and allow data subjects to contest decisions. Even outside Article 22 scenarios, profiling requires a valid legal basis and transparency, and DPA guidance stresses careful assessment when using stable identifiers for cross-context tracking. If you're matching on phone numbers, expect to justify your legal basis (often consent) and provide an easy way to object. (GDPR, gdpr-text.com, ICO)

California (CCPA/CPRA). California gives consumers the right to opt out of the *sale or sharing* of personal information, with "sharing" explicitly covering cross-context behavioral advertising—i.e., the cookie-less matching of hashed phone numbers to target ads across sites. Businesses that sell or share must post clear opt-outs ("Do Not Sell or Share My Personal Information") and honor choices via recognized signals. In practice, if you upload or receive phone-number-based audiences for cross-site ads, you're in "sharing" territory and must provide opt-outs and disclosures. (oag.ca.gov, Yes on Prop 24, InfoTrust)

Phone numbers should always be treated as high-risk identifiers. They exist over time, can be used to link offline and online data and are attractive for profiling even after recycling. Platforms and brokers use (often via hashing) use them for portable ad IDS; regulators increasingly view those uses as profiling and "sharing," triggering consent/opt-out duties and heightened transparency. If companies must use numbers for security, it is suggested that they keep them separated from marketing and if you profile for ads, build robust legal bases, user controls, and deletion/opt-out pipelines that cover hashed identifiers, too. (WIRED, Federal Trade Commission)

Technical Vulnerabilities & Research Insights

VoLTE/5G call- and presence-tracking. Regardless of 5G's upgraded crypto, researchers have shown that design/implementation flaws still give attackers the ability to infer when your phone is reachable and where it is. Attacks like **ToRPEDO** exploit predictable paging to link a soft identity (even a phone number) to a device and track it; later work found 11 additional 5G protocol flaws with downgrade paths back to weaker generations. In short: 5G is better but still leaky in practice. (NDSS Symposium, WIRED)

Signaling-layer location leaks (SS7/Diameter). The legacy SS7 network and 4G's Diameter core can be abused to query handset location worldwide with nothing more than a phone number. Civil-society labs and mobile-security vendors document active

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

exploitation; U.S. officials and advocates have urged carriers and regulators to treat this as an ongoing, not historical, threat. (Electronic Frontier Foundation, The Citizen Lab, Enea, epic.org, WIRED)

Carrier and platform missteps. Beyond protocol issues, real-world practices have amplified risk. In 2024 the FCC fined major U.S. carriers nearly **$200M** for selling real-time location data through aggregators without valid consent proof that location tied to your number can (and did) escape the network perimeter. (docs.fcc.gov, AP News, Axios, Ars Technica)

VoLTE/IMS stack weaknesses. Application-layer and IMS/VoLTE implementations have also exposed call privacy (e.g., eavesdropping via weak or misconfigured tunnels), reminding us that "5G privacy" lives or dies in deployments, not just specs. (Cellcrypt)

Anonymization is hard when the key is the number. Research shows that contact-discovery (the "upload your address book" feature in messengers) enables *enumeration* of vast swaths of users; hashing phone numbers doesn't solve it because the number space is small and guessable. Large-scale studies crawled WhatsApp/Signal/Telegram using only number patterns; follow-ups propose protocol changes or private set intersection to curb leakage. This dovetails with number-recycling work showing how new owners can inherit access paths to prior owners' accounts. (NDSS Symposium, ACM Digital Library, recyclednumbers.cs.princeton.edu)

Protocol evolution (progress, but not panacea). Formal re-assessments and proposals (e.g., 5G-AKA variants) aim to reduce linkability, yet active-attacker and deployment gaps keep re-identification in play. (USENIX, PMC)

Mitigations & Best Practices

For Telecom Carriers.

Extend dormancy before reuse to let account owners update records and to let call/SMS forwarding, voicemail, and OTT bindings expire. Pair this with **secure deletion** of any network-side artifacts (voicemail boxes, call-forwarding rules). Use the FCC's **Reassigned Numbers Database (RND)** so businesses can check before contacting a number that's been recycled. (Federal Communications Commission, reassigned.us)

Harden paging and signaling. Deploy SS7/Diameter firewalls, strict filtering, and anomaly detection; block unauthorized MAP/CAP/Diameter queries, and monitor for paging-occasion probing. Keep anti-downgrade defenses tight to prevent pushes to older, weaker RATs. (GSMA, Enea, telecomHall Forum)

Close 5G slice/IMS gaps. Follow industry guidance on slice isolation and IMS/VoLTE security; verify vendor implementations against known paging and registration issues. (Enea, NDSS Symposium)

For Businesses (app builders, platforms, marketers).

De-emphasize the phone number as a security anchor; treat it as *risk-bearing PII*. Prefer **phishing-resistant MFA** (FIDO2/WebAuthn) and device-bound authenticators over SMS OTP. Where SMS must be used, follow NIST 800-63B risk notes and offer a non-SMS fallback. (CISA, pages.nist.gov, NIST Technical Series)

Use API-based verification carefully. If you rely on carrier data or data brokers to "verify" a number, build consent, audit, and opt-out flows—remember that carriers were fined for location data sharing; don't recreate that problem in your stack. (AP News)

Rethink contact discovery. Replace naive hash-matching with privacy-preserving contact discovery (e.g., PSI/oblivious protocols), rate-limit queries, and block enumeration. (NDSS Symposium)

RND checks for outreach. Before SMS/call outreach (marketing, recovery, alerts), check the **RND** and honor opt-outs to avoid misdirected messages to recycled numbers. (Federal Communications Commission)

For Regulators.

Mandate pre-reuse notifications and grace periods. Require carriers to notify subscribers (e.g., via last-known email or in-app account) *before* number retirement; set minimum dormancy windows by risk category (consumer vs. enterprise lines). Complement with required RND queries for high-volume callers. (Federal Communications Commission)

Enforce signaling security baselines. Continue actions against unlawful location sharing and require measurable SS7/Diameter hardening and anti-downgrade controls. The 2024 FCC fines underscore why enforcement matters. (docs.fcc.gov, Ars Technica)

For Users.

Audit linked accounts any time you change numbers: rotate recovery channels, disable SMS-only 2FA, and set app-based or passkey MFA. (CISA)

Use virtual/burner numbers for sign-ups and public posts; keep a separate, stable number for banking and identity-critical services. (And set number-change alerts where available.)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Minimize contact upload. Opt out of "find friends" via address-book sync, or use messengers that offer private contact discovery. (NDSS Symposium)

Compliance alignment (GDPR, CPRA/CCPA, Nigeria).

GDPR – Data Protection by Design/Default (Art. 25). Treat phone numbers as high-risk identifiers: minimize collection, segregate security vs. marketing uses, and use privacy-preserving contact discovery where feasible. Regulators and scholarship emphasize embedding safeguards into the *means* of processing, not just policies. (edpb.europa.eu, Future of Privacy Forum, GDPR)

California – "Sale"/"Sharing" for cross-context ads. Uploading/receiving phone-number-based audiences for cross-site advertising is typically **sharing** under CPRA—triggering opt-out links and recognized signals. Build "Do Not Sell or Share" controls and contracts that truly constrain providers. (www.hoganlovells.com, Davis+Gilbert LLP, iapp.org)

Nigeria – NDPA 2023 (superseding NDPR). Nigeria's 2025 GAID clarifies NDPR is no longer applied post-NDPA; align number-based processing to NDPA principles (lawfulness, purpose limitation, minimization) and document risk assessments for contact discovery or profiling. (TEMPLARS, olaniwunajayi.net)

II. Conclusion & Policy Recommendations

Summary of risks and regulatory gaps.

While Mobile phone number recycling is important for managing the finite availability of numbers, it can create a constant chain of vulnerabilities. In both academic research and enforcement, numbers are stable identifiers that can survive recycling, thereby linking past owners to new ones through account recovery channels, adtech profiling and contact discovery. Technical flaws in VoLTE, 5G, and legacy signaling systems (SS7/Diameter) compound the risk, enabling call tracking and location leaks from nothing more than a number.

Existing regulatory frameworks GDPR, CCPA/CPRA, NDPA provide partial coverage but often lack explicit rules for number reuse. Enforcement has largely targeted downstream misuse (e.g., unlawful location sharing) rather than upstream policy gaps in recycling procedures. Few jurisdictions mandate extended dormancy, secure deletion, or proactive notification before reuse, and there is no globally harmonized standard for handling identifiers after retirement.

Need for global alignment.

It is suggested that there is a globally recognized standard for telephone recycling, dormancy periods, deletion protocols and compulsory disclosure that a number is being reused. This is as a result of the cross border nature telecom signaling takes, and as a result, no uniform rules can cause privacy issues even for countries with the best privacy standards.

Recommendations.

For Carriers:

a. Ensuring extended dormancy periods, risk-tiered by number type (e.g enterprise vs. personal).

b. The deletion of all network and platform linked data in a secure and verifiable process before the number is recycled.

c. The use of SS7/Diameter firewalling and 5G anti-downgrade measures to reduce tracking risks.

d. The update of. such information in shared databases (e.g., FCC's RND) to alert service providers of changes.

For App Providers & Businesses:

a. The use of multifactor authentication as opposed to the use of phone numbers as a single source of authentication, especially the use of phishing-resistant MFA.

b. Use of privacy-preserving contact discovery automation

c. Automating workflows to update or revoke account bindings upon number changes

For End-Users:

a. Regularly updating all linked accounts before deactivating a number.

b. Use different numbers (or virtual/burner lines) for high-value services and public sharing.

c. Monitor for unauthorized access attempts after a number change.

Asides from being a logistic issue, number recycling can pose a challenge to privacy globally. As a result, there is the need for technical and policy safeguards, preventing identity theft/ recycled identity.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

References

1. European Parliament. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. (EUR-Lex)
2. Federal Communications Commission. (2021). Reassigned Numbers Database. (fcc.gov)
3. Lee, K., & Narayanan, A. (2021). Security and privacy risks of number recycling at mobile carriers. Proceedings on Privacy Enhancing Technologies, 2021(4), 108–128. (Author preprint). (recyclednumbers.cs.princeton.edu, Princeton University)
4. Manatt, Phelps & Phillips, LLP. (2021, December 16). Reassigned Number Database up and running. (Notes TCPA "safe harbor" linked to RND queries). (manatt.com)
5. NANPA. (2019). p-ANI Activity and Projected Exhaust Report (and related exhaustion projections). (nanpa.com)
6. Nigerian Communications Commission. (2019). Numbering Plan Regulations. (Dormancy / quarantine requirements before reassignment). (Vanguard News)
7. Ofcom. (2021). Mobile number recycling (FOI response) — indicates typical UK dormancy windows (often ~3 months to a year) and operator discretion. (www.ofcom.org.uk)
8. EUR-Lex. (2002). Directive 2002/58/EC (ePrivacy Directive). (EUR-Lex)
9. Hussain, S. R., Chowdhury, O., Mehnaz, S., & Bertino, E. (2019). Privacy attacks to the 4G and 5G cellular paging protocols using side-channel information (ToRPEDO). NDSS. (NDSS Symposium, syed-rafiul-hussain.github.io)
10. Singla, A., Hussain, S. R., Chowdhury, O., Bertino, E., & Li, N. (2020). Protecting the 4G and 5G cellular paging protocols against security and privacy attacks. Proceedings on Privacy Enhancing Technologies, 2020(1), 126–142. (Pet Symposium)
11. NIST. (2020). SP 800-63B: Digital Identity Guidelines — Authentication and Lifecycle Management. (and 2024 draft update). (csrc.nist.gov, NIST Publications)
12. ENISA. (2021). ENISA Threat Landscape 2021 (and SIM-swapping advisories). (enisa.europa.eu)
13. GSMA. (2021). Mobile Telecommunications Security Landscape 2021 (notes SMS/SS7 weaknesses relevant to 2FA). (GSMA)
14. AP News. (2024). FCC fines wireless carriers for sharing user locations without consent (nearly $200M total). (AP News)
15. Wired. (2019). Holes in 4G and 5G networks could let hackers track your location. (Coverage of ToRPEDO and related flaws). (WIRED)
16. RND (Administrator site). (n.d.). Reassigned.us — service portal for RND queries. (reassigned.us)
17. Manatt, Phelps & Phillips, LLP. (2017). Reassigned numbers: Commenters embrace database, split on safe harbor. (FCC NOI coverage). (manatt.com)
18. Meta. (2022). About Custom Audiences from customer lists. (Phone numbers accepted for audience matching). (Medium)
19. Clearcode. (2023). How phone numbers are used in digital advertising. (Explains hashed identifiers and matching). (gdpr-info.eu)
20. Gryphon.ai. (2024). Understanding the Reassigned Numbers Database and why it matters to compliance. (Explainer). (gryphon.ai)
21. The Hacker News. (2021). New study warns of security threats linked to recycled phone numbers. (Popular write-up of the Princeton results). (The Hacker News)
22. Commsrisk. (2021). Research shows recycling phone numbers threatens privacy. (Industry coverage of the study). (commsrisk.com)