Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States

Kevin Lee and Arvind Narayanan
Department of Computer Science and Center for Information Technology Policy
Princeton University
{kvnl, arvindn}@cs.princeton.edu

This paper will be published in the *Proceedings of the 2021 APWG Symposium on Electronic Crime Research (eCrime)*

***Abstract*—We examined the security and privacy risks of phone number recycling in the United States. We sampled 259 phone numbers available to new subscribers at two major carriers, and found that 171 of them were tied to existing accounts at popular websites, potentially allowing those accounts to be hijacked. Additionally, a majority of available numbers led to hits on people search services, which provide personally identifiable information on previous owners. Furthermore, a significant fraction (100 of 259) of the numbers were linked to leaked login credentials on the web, which could enable account hijackings that defeat SMS-based multi-factor authentication. We also found design weaknesses in carriers' online interfaces and number recycling policies that could facilitate attacks involving number recycling. We close by recommending steps carriers, websites, and subscribers can take to reduce risk.**

I. Introduction

Recycled phone numbers can cause trouble for all those involved. Subscribers who are assigned a previously owned phone number often end up receiving communication meant for the previous owners, from threatening robocalls to personal text messages. One journalist, right after changing her number, was bombarded with texts containing blood test results and spa appointment reservations, while another accidentally wound up in a previous owner's email inbox after requesting a login passcode via SMS [1], [2]. A recent survey of 195 participants found these incidents are common; 72 reported negative experiences related to number recycling, including dealing with communication meant for previous owners [3]. While neither the journalists nor any of the study participants had any malicious intent, this naturally raises concerns about adversaries exploiting these incidents for gain.

In this study, we present eight different attacks enabled by phone number recycling. Of those, we empirically evaluated three low-cost attacks that allow new owners of recycled numbers to compromise the security and privacy of previous owners. We analyzed the set of phone numbers available through the online interfaces of two U.S. mobile carriers: T-Mobile and Verizon Wireless. By analyzing the structure of phone number blocks that contain primarily recycled versus primarily fresh numbers, we developed a strategy for the adversary to focus their attention on the former. Our key finding is that most of the available phone numbers we sampled (215 of 259) were recycled and also vulnerable to one or more of the three number recycling attacks.

Throughout our study, the adversary only needs to interact with standard online number change interfaces to carry out these attacks, and does not need to exploit software vulnerabilities. We found that the online interfaces in question imposed few restrictions on the adversary's ability to browse and obtain previously owned numbers for exploitation. We estimate the number of available recycled phone numbers at Verizon to be about one million, with a largely fresh set of numbers becoming available every month.

We found that carriers did not proactively notify subscribers about their policies regarding number recycling. Worse, they provided inconsistent responses when asked. We called in to customer service to ask about number aging periods—the time before a disconnected number is made available again. We received widely divergent answers at each carrier (seven unique responses out of 13 calls to T-Mobile, eight unique responses out of 13 calls to Verizon). Subscriber confusion or unawareness of recycling policies could be one reason why the vulnerabilities we document are so prevalent.

Finally, we obtained and monitored 200 recycled numbers from both carriers. With just one week of data, we conservatively found nearly 10% of numbers in our honeypot were still receiving security/privacy-sensitive communications meant for previous owners. Upon receiving these unsolicited calls / texts, owners of recycled numbers can suddenly realize the incentives to exploit and become opportunistic adversaries. Due to our limited monitoring period, the actual proportion of vulnerable numbers is likely much higher.

As the number of users coming online continues to grow, number recycling threats are unlikely to abate. Phone numbers have become tied to peoples' identities more than ever, through social media accounts, ridesharing apps, mobile banking, etc. They are used to link online accounts to real-world entities and for authentication. Unfortunately, numbers are a finite resource. In the United States, when a subscriber gives up their 10-digit phone number, it eventually gets reassigned to someone else. While carriers, websites, and subscribers can take steps to reduce risk, number recycling threats highlight fundamental problems with the use of phone numbers for security-sensitive purposes.

Responsible disclosure and responses. In October 2020 we provided an initial notification of our findings to the

978-1-6654-8029-1/21/$31.00 ©2021 IEEE

carriers we studied and to CTIA, the U.S. trade association representing the wireless communications industry.

In December 2020, T-Mobile informed us that after reviewing our research, it had updated its number change support page to 1) remind subscribers to update their contact number on bank accounts and social media profiles, and 2) specify the FCC-mandated number aging period. Along with raising subscriber awareness, it also informed us that customer service agent manuals had been updated to emphasize those two points during relevant interactions, effective early December.[1]

In December 2020, CTIA informed us that after reviewing our research, Verizon had updated its public-facing support document for number cancellations, suspensions, and transfers to 1) remind subscribers to update their contacts and unlink their business and online accounts, and 2) specify the FCC-mandated minimum aging period (45 days).[2]

Social impact. In March 2021, we reached out to academic researchers studying technology-enabled intimate partner violence (IPV), and discussed the harms of number recycling attacks targeting survivors of IPV.[3] The team is currently drafting an update to their clinic resources to include our research and recommendations.[4]

II. Background and Related Work

A. Phone-based authentication is prevalent

According to 2FA Directory—a crowd-sourced project to build a comprehensive list of sites that do or do not support multi-/two-factor authentication (2FA), about 30% of websites (455 / 1,565) support SMS-based authentication as of January 2021 [4].[5] Its popularity is only surpassed by that of authenticator apps, which is present at 40% (626/1,565) of websites. 957 websites in the dataset support at least one form of 2FA.

By SMS-based authentication, we mean the method of sending a single-use passcode (OTP) to the subscriber's phone via an SMS text message or a phone call. This type of authentication is vulnerable to phone line changes because they are tied to a phone number and the associated cellular service. Other types of phone-based authentication (e.g., authenticator apps) are not vulnerable to phone line changes.

Phone numbers themselves are regularly used by systems to authenticate callers. Some automated customer service phone systems—such as for credit cards—automatically announce sensitive account information if the caller ID corresponds to an existing profile, without any subscriber input [2]. Even after a phone line change, these external systems can continue to reveal a previous owner's credit card or utility account information to the new owner of the phone number, unless the previous owner manually updates their contact.

B. Subscribers may give up or lose their phone number for many reasons

According to the Federal Communications Commission (FCC), around 35 million phone numbers in the U.S. are disconnected every year [5]. At the end of 2018 (the latest published data at time of writing), there were more than 860 million phone numbers in use by active subscribers [6].

People may give up their phone number for various purposes, such as to:

1) Prevent unwanted parties from contacting them (e.g., abusive acquaintances, collections agencies)[6]
2) Switch to a new carrier[7]
3) Cancel telephone service altogether (e.g., moving out of the country, switching to a job-provided phone account)
4) Switch to a more desirable number [7]

Subscribers may also lose their account and their phone number due to:

1) Nonpayment
2) Violation of service terms
3) Inactivity (e.g., Google Voice [8], Twilio [9])

C. Most relinquished phone numbers get reassigned

Most relinquished numbers are not permanently retired. There is only a finite number of 10-digit phone numbers; all will eventually be assigned to carriers, thereby capping expansion. Since the FCC assigns phone numbers to carriers in contiguous blocks of 1,000 rather than individually, it has sought to forestall exhaustion for as long as possible by activating fresh blocks of phone numbers only when absolutely necessary.[8] To that end, it has enacted policies to prevent carriers from hoarding numbers and encourage carriers to routinely recycle numbers by assigning them to new subscribers after a waiting period [10]. As a result, new owners of previously-assigned numbers often end up receiving personal communication meant for the previous owners.

D. Number recycling is regulated by the FCC

There are also FCC rules specific to number recycling that aim to encourage carriers to recycle numbers while mitigating the risks to subscribers. However, the only risk that the FCC appears to be concerned about is that of receiving robocalls meant for previous owners, and not any of the other threats we discuss here.

Under 47 C.F.R. § 52.15, carriers are prohibited from reassigning disconnected numbers until 45 days have elapsed since disconnection, and can age numbers for up to 90 days (365 days for numbers assigned to business customers). In

[1] https://www.t-mobile.com/support/account/change-your-phone-number. (visited on 03/22/2021).

[2] https://www.verizon.com/support/cancel-suspend-transfer-lines/#change. (visited on 03/22/2021).

[3] https://www.ipvtechresearch.org/

[4] https://www.ceta.tech.cornell.edu/resources

[5] Anyone can contribute 2FA information about websites, while a group of private developers acts as the moderator. As such, the 1,565 websites should be viewed as a convenience sample.

[6] https://www.reddit.com/r/legaladvice/comments/bs2nbv/help_me_take_legal_action_against_my_ex_who_has/. ("A month after a nasty breakup, I told my abusive ex to never contact me again... I have to change my phone number because of him.")

[7] Most carriers are required to allow active departing subscribers to bring their numbers to their new carriers. Of course, subscribers may elect to receive new numbers, thereby releasing their original ones.

[8] One of the reasons to prolong the usefulness of 10-digit dialing is the exorbitant cost of adding another digit; many existing automated devices are only programmed to handle 10-digit phone numbers.

December 2018—in efforts to combat unlawful robocalls—the FCC announced a plan to create a reassigned number database (RND), along with establishing the 45-day minimum aging period [11]. Carriers would be mandated to report recycled numbers on a monthly basis, which would be compiled into a centralized source for legitimate robocallers (e.g., refill prescription reminders) to reference. Carriers were required to comply with the 45-day minimum period and maintain records of disconnected numbers starting in July 2020 [12]. The RND became operational in November 2021 [13].

Currently, RND access is available to FCC-verified accounts for a fee; database users need to register as a caller, service provider, toll-free number administrator, or FCC personnel [14]. Other entities, however, may take steps to mitigate number recycling threats if given access to the database (e.g., a website may be able to use the RND to check reassigned numbers against SMS 2FA/recovery settings and warn users). In October 2021, we reached out to the FCC and suggested that it consider number recycling risks and to encourage RND access for websites and relying parties for this use case.

E. Structure of U.S. phone numbers

United States phone numbers are of the 10-digit format:

NPA-NXX-XXXX

NPA stands for Number Plan Area, or area code. There are currently 330 area codes in use in the U.S. NXX refers to the central office (exchange) code. In § IV, we take this structure into account in designing our sampling strategy.

F. Previous work on the risks of number recycling

There have occasionally been mentions of number recycling incidents in the media; one blog post had even speculated on the feasibility of taking over linked social media profiles with recycled phone numbers [15]. Recently, McDonald et al. conducted a user survey to ask 195 participants about their experiences with using phone numbers as identifiers and phone number recycling [3]. They determined these incidents occur regularly; many participants (72/195) reported experiencing negative downstream effects, such as receiving calls / texts meant for previous owners and being unable to add their number to online services due to an existing account.

These negative effects can be greatly amplified if exploited by an adversary. Our research is the first to analyze how adversaries can exploit phone number recycling with ease. To the best of our knowledge, there has not been any prior academic work looking at the wide scale security impact of number recycling. Specifically, none of the eight attacks we present in § III appear to have been systematically studied.

G. Related work

Beyond the effects of number recycling, SMS-based 2FA is less secure because it is tractable to known security weaknesses at mobile carriers. IMSI-catchers can be used to eavesdrop calls and texts by intercepting a nearby mobile phone's cell tower connection [16]. The signaling protocol used by carriers to achieve interoperability—Signaling System 7 (SS7)—does not authenticate requests, and thus can be used by remote attackers to re-route SMS 2FA messages to their own phones [17], [18]. Some carriers have weak (or weakly enforced) policies for authenticating subscribers over the phone (e.g., recall two recently dialed numbers); attackers can easily obtain this information and trick customer service representatives (CSRs) into updating the SIM card on a victim's account to one they control, in a SIM swap attack [19].

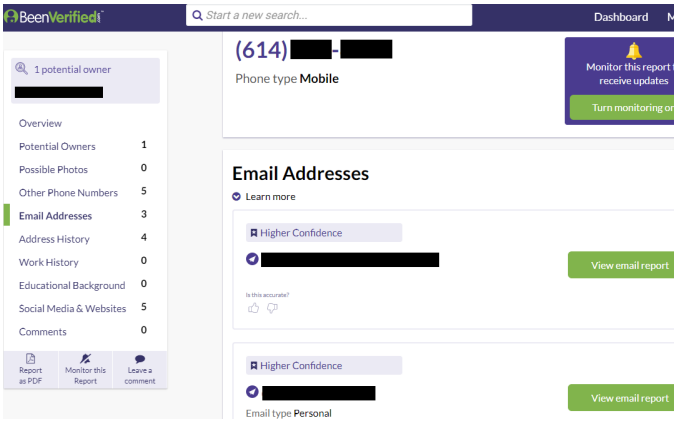

Fig. 1: Anyone can enter a phone number on BeenVerified to reveal personally identifiable information (PII) on the number's previous and current owners.

Some consumer email providers recycle usernames of dormant accounts. Like SMS-based authentication, email is commonly used to authenticate logins and recoveries. Of the top three providers, Yahoo and Microsoft both close accounts for inactivity and make the usernames available for new users [20], [21]. Google—the most popular provider—does not recycle email addresses [22]. While there has been significant backlash against Yahoo and Microsoft for prioritizing the ability to choose "short, sweet, and memorable" usernames over security and privacy, the practice remains unchanged. There has not been any analysis on the implications of recycling email addresses thus far [23], [24].

III. Threat Modeling Number Recycling Attacks

We present the first systematic analysis of number recycling attacks. In Table I, we present eight different threats enabled by number recycling, four in which attackers can target previous owners of recycled phone numbers, and four in which attackers can target future owners.

Number recycling can be leveraged in different attacks ranging from opportunistic to highly targeted. We selected the first three attacks in Table I to study in depth because they are both serious and can be studied without harming actual subscribers. We now describe them in more detail.

In an opportunistic scenario with the lowest barrier to entry, an attacker can use a recycled number—that they have obtained by signing up for service—to look up information on the number's previous owner on the web or through data aggregation services, which are available to anyone at low

TABLE I: Eight attacks enabled by number recycling. We empirically investigated the feasibility of the highlighted attacks.

Attack	Threat(s)	Population(s) affected
PII indexing. Attacker cycles through available numbers on the carrier's online number change form and checks for previous owners' personally identifiable information (PII) through people search services. They obtain the numbers that produce hits on these services.	Amass PII; create stepping stone to impersonate previous owner; read new messages intended for the victim	Previous owners; friends and family of previous owners
Account hijackings via recovery. Attacker cycles through available numbers and checks if any of them are linked to existing online accounts (e.g., social media, email, e-commerce). They obtain the numbers with hits and try to reset the password on the linked accounts via SMS-based password recovery.	Hijack online accounts; impersonate previous owner; read new messages intended for the victim	Previous owners; friends and family of previous owners
Account hijackings without password reset. Attacker cycles through available numbers and checks for linked accounts as well as previous owner PII on people search services. Attacker uses the PII to find and purchase passwords from data breach listings on cybercriminal marketplaces. They obtain the phone numbers that are linked both to online accounts and to breached passwords. They bypass SMS-based 2FA on the online accounts using the password and control of the phone number.	Hijack online accounts even with SMS 2FA enabled; impersonate previous owner; read new messages intended for the victim	Previous owners; friends and family of previous owners
Targeted takeover. Attacker learns that an acquaintance's contact has changed (e.g., stalker calls and gets a cancelled number intercept message, friend changes their number and tells everyone). They keep track of the aging period, and obtain the number once it becomes available.	Hijack online accounts; impersonate/stalk previous owner; read new messages intended for the previous owner	Previous owners, especially intimate partner violence (IPV) survivors changing their numbers to escape abusers
Phishing. Attacker logs available numbers but does not obtain them. Later, they keep checking whether the numbers are still available. Once a number is assigned to a new subscriber, they can phish the subscriber through SMS (e.g., "Welcome to your new service. Click here to enable high-speed data for your account"). Subscribers are more likely to fall for phishing attacks when the message sounds believable [25].	Hijack victims' online phone accounts; potentially take control of victims' phone numbers.	Subscribers who have been assigned a new number, whether fresh or recycled.
Persuasive takeover. Attacker logs available numbers but does not obtain them. After the number is assigned, they can spoof a carrier message (e.g., "Your number is part of an ongoing investigation on the previous owner and needs to be reclaimed. Please change your number online") and obtain the number for himself after the aging period.	Hijack online accounts with phone number linked; impersonate victim; read new messages intended for the victim	Subscribers who have been assigned a new number, whether fresh or recycled.
Spam. Attacker obtains a number, intentionally sign up for various alerts, newsletters, campaigns, and robocalls, and then release the number for recycling	Victim harassed with unwanted texts and calls; account calling balance depleted	Subscribers who have been assigned a recycled number.
Denial of service. Attacker obtains a number, sign-up for an online service that requires a phone number, and releases the number. When a victim obtains the number and tries to sign up for the same service, they will be denied due to an existing account. The attacker can contact the victim through SMS and demand payment to free up the number on the platform.	Denial of service; victim needs to pay ransom to use platform	Subscribers who have been assigned a recycled number and are new users of online services that require a unique phone number

cost (**PII indexing**). Fig. 1 shows lookup results at one such service, BeenVerified; a report can include information like previous owner names, photos, email addresses, work history, social media account handles. Armed with personally identifiable information (PII) and control of the number, the attacker can impersonate previous owners in calls and messages.

Consider another scenario: an attacker can use the recycled number to look for and break into linked profiles online via SMS-authenticated password resets (**Account hijackings via recovery**). Despite growing awareness of the risks of SMS-based authentication of online accounts, the practice remains prevalent [19].

Alternatively, the attacker can find and use the previous owner's email addresses to look for password breaches and purchase the stolen password on the dark web.[9,10] With the stolen password, the attacker can log in to most of the previous owner's accounts without going through recovery, and defeat SMS 2FA by receiving the passcode sent to the recycled number (**Account hijackings without password reset**). Note that the recovery pages usually don't reveal PII such as email addresses (only the existence of an account and available recovery methods), so the attacker needs to use **PII indexing** as a gateway to this attack.

An adversary might not even need to obtain the phone number in order to plan out an attack. At carriers that allow for

[9]PII—usually email addresses—are often used as usernames.

[10]Most users are known to notoriously practice poor security hygiene by reusing their passwords, so a purchased password may work at multiple websites.

full numbers to be previewed—either during signup or number change—an attacker can "scout out" a number by looking for linked accounts and owner history, all before obtaining the recycled number. As we will show later, this strategy is made possible by the lack of query limits on the carrier interfaces in our study (§ VI-A).

Attackers may have varying economic motivations for these attacks [26]. They may be interested in stealing money from victims, such as by taking over online accounts that hold cryptocurrency [27]. Alternatively, they may use amassed accounts on social media for spam campaigns or fake followers [28], [29]. The latter strategy requires a relatively large number of online accounts, and a correspondingly large number of phone number changes (assuming that the attacker controls a fixed number of SIM cards and service plans). Unfortunately, at the time of our study, some carriers not only had no query limits in place but also no rate limits for phone number changes (§ VI-A).

In our study, we simulated an opportunistic attacker with access to data aggregation (people search) services, data breach lookup tools, and one prepaid account per carrier, all of which can be obtained for under $100. We did not target any specific area codes, and we did not look for vulnerabilities before "obtaining" (logging) the numbers.

Note that our attacker is a *UI-bound adversary*—an authenticated user who uses the system with the same privileges as any other user, albeit with malicious intent [30]. Since the adversary operates within the functionality of the user interface and does not need to use any tools or exploit a system vulnerability, the population of potential attackers is expansive.

IPV survivors are especially vulnerable to targeted takeovers. Survivors of intimate partner violence (IPV) face a higher risk of harm from number recycling attacks. Survivors may change phone numbers to escape their abusers [31]. Upon realizing that their victim's number has changed, the abuser (a *UI-bound adversary*) may keep track of the aging period and obtain the number once it becomes available (**Targeted takeover**). Armed with access to the survivor's old number and PII, as well as a desire to agonize, the abuser can cause devastating harm. For example, the abuser can hijack online accounts where the survivor has either forgotten or has not yet updated the SMS 2FA and recovery number. The abuser may also be able to impersonate the survivor via SMS to manipulate mutual acquaintances (e.g., trick friends into revealing the survivor's current number, or convince them that the survivor is no longer being stalked). Since they have already moved on to using a new number, survivors may be unaware that their abuser is using their previous number.

IV. Analysis of Attacks Against Previous Owners

We study the severity of the security risks associated with phone number recycling, and find that previous owners of most recycled numbers are at risk.

A. Method

We aim to answer three questions:

1) How easily can attackers find recycled phone numbers and corresponding PII on their previous owners?
2) How easily can attackers find recycled phone numbers with vulnerable linked online accounts?
3) Is it feasible for attackers to use PII from people search sites to look for likely passwords for these linked accounts?

1) Sampling available prefixes and numbers

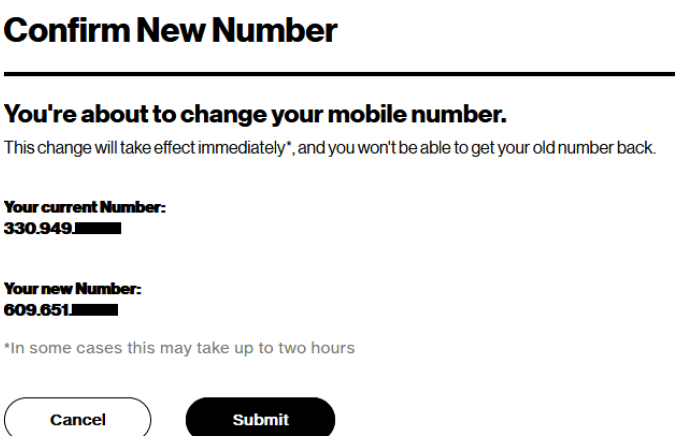

Fig. 2: Verizon's number change interface for prepaid subscribers.

We signed up for one prepaid account at each of the two largest U.S. carriers—Verizon Wireless and T-Mobile. Both carriers provide an online interface for subscribers to change their phone number. The third major carrier—AT&T—does not, so we omitted it from our study. We manually interacted with the interfaces just as a normal subscriber looking to change their number would. Throughout, we logged available numbers but did not complete any number changes.

All of the number change interfaces we saw in this study index available numbers by NPA-NXX prefixes; that is, subscribers need to choose an available NPA-NXX as an intermediate step. This constraint affects our number sampling strategy. At Verizon, we were able to randomly sample prefixes, but not numbers. We were unable to randomly sample prefixes at T-Mobile due to further selection constraints we highlight later in this section.

Verizon. Verizon allows prepaid subscribers to specify any NPA-NXX as criteria on the online number change request form. If the entered NPA-NXX is a valid Verizon prefix with at least one available number, the following screen will denote a single selected number with a predefined subscriber number (last 4 digits, see Fig. 2). The subscriber can either confirm the request (after which their line will be updated, often immediately) or go back to perform a new query. If the subscriber performs a new query with the same NPA-NXX, the following screen will show a different number from the previous query results. If the entered NPA-NXX is not serviced by Verizon or currently has no available numbers, the subscriber is presented with an error modal asking for a valid NPA-NXX entry. Since we also encounter the error modal at

different iterations of repeated queries for each NPA-NXX, we assume that the system temporarily keeps track of "seen" numbers and errors out when we have exhausted the available number pool for each prefix.

We started with a list of all currently active NPA-NXX prefixes by obtaining the central office code assignment records hosted on NANPA.[11] At the time of our experiment, there were 180,741 unique prefixes on record, and thus in use by telecoms in the U.S. We randomly selected prefixes, and for each prefix, we leveraged the number change request form to log all available numbers. That is, we repeatedly requested a new number with the same prefix until we encountered the invalid NPA-NXX message, and continued the process for all NPA-NXX prefixes in our list. We iterated 875 prefixes over the course of three days, for a total of 8,603 available numbers across 77 of those prefixes. The largest prefix contained over 900 numbers, while there were 28 prefixes with under 10 available numbers.

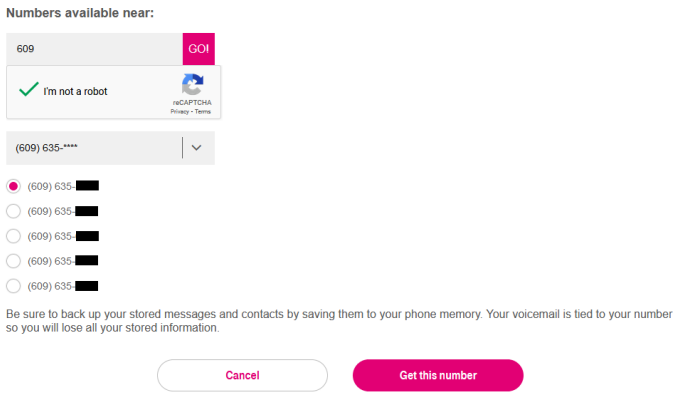

Fig. 3: T-Mobile's number change interface for prepaid subscribers.

T-Mobile. T-Mobile allows prepaid subscribers to specify any NPA as a query on the online number change request form. The system returns up to five NPA-NXX with the most available numbers (the raw JSON response contains an inventory count for each NXX). For each of the five NPA-NXX's, five available numbers are shown for the subscriber to choose from, for a maximum of 25 numbers per NPA (Fig. 3). Barring churn from other subscribers' activities, the 25 numbers do not change between subsequent queries. We iterated through the 330 active area codes and leveraged the number change request form to log accessible available numbers. We collected 6,928 available numbers across 1,393 NPA-NXX prefixes.

2) Identifying likely recycled numbers

In the next step, we focused on recycled numbers. We simulated an adversary trying to maximize chances of finding a recycled number. Accordingly, for both carriers, we restricted our attention to NPA-NXX blocks for which no two available numbers were within 10 of each other. Since new NPA-NXX blocks are more likely to have consecutive available numbers (like how newly printed money is consecutively numbered in stacks), an adversary who is interested in recycled numbers can ignore those blocks in their queries.

[11] https://nationalnanpa.com/reports/reports_cocodes_assign.html. (visited on 08/16/2020).

TABLE II: A detailed breakdown of applying our number classification strategy.

(a) T-Mobile

	Available Numbers	NPA-NXXs
Likely recycled	1,438	295
Possibly unused	5,490	1,098

(b) Verizon

	Available Numbers	NPA-NXXs
Likely recycled	159	32
Possibly unused	8,444	45

We therefore grouped the blocks into two categories:

- ***Likely recycled.*** No two available numbers are within 10 of each other. Numbers from this pool are likely to have been previously assigned.
- ***Possibly unused.*** At least two numbers are within 10 of each other. The pool consists of both unused numbers and some recycled numbers that are close together just by chance.

Table II details the result of splitting the NPA-NXX blocks along the constraint.

For Verizon, it may seem that *Likely recycled* numbers are rare in comparison to *Possibly unused* numbers. However, the number of NPA-NXX blocks in each group are actually comparable; if a Verizon subscriber selects a NPA-NXX at random they can happen upon a *Likely recycled* number nearly half of the time. Furthermore, numbers from the *Possibly unused* group can also be recycled. At T-Mobile, we logged nearly four times as many NPA-NXX blocks from the *Possibly unused* group as blocks from the *Likely recycled* group. This is possibly due to T-Mobile's interface design; NPA-NXX blocks with the most available numbers are most likely new blocks, and therefore appear in the five NPA-NXX choices more often.

3) Reverse lookups

For each of the 159 numbers in Verizon's *Likely recycled* group and 100 randomly sampled numbers in T-Mobile's *Likely recycled* group, we used the reverse phone lookup tools at two people search services—BeenVerified and Intelius—to look for owner history. We chose these two services based on positive user reviews [32], [33]. This step serves two purposes. It allows us to estimate the vulnerability to the **PII indexing attack** (§ IV-B). It also lets us validate our strategy for classifying numbers as *Likely recycled* and *Possibly unused*. We did so by randomly sampling 159 and 100 numbers from Verizon's and T-Mobile's *Possibly unused* groups respectively and looking for people search hits. We found that 53/159 and 44/100 of the sampled *Possibly unused* numbers returned hits, compared to 96/159 and 75/100 of the sampled *Likely recycled* numbers. For each carrier, we used a one-sided z-

TABLE III: Hit rates from our testing methods. Most of the numbers we analyzed were confirmed recycled (83%). Rows highlighted in yellow suggest immediate danger to accounts with a certain authentication configuration. Rows highlighted in red suggest immediate danger to accounts, regardless of authentication configuration.

Test	**Attack**	**Hit count: T-Mobile (out of 100)**	**Hit count: Verizon (out of 159)**	**Hit count: total (out of 259)**
Found on people search services **OR** linked account at any of the six websites	Confirm that number is recycled	94 (94%)	121 (76%)	215 (83%)
Found on people search services	PII indexing	75 (75%)	96 (60%)	171 (66%)
Linked account at any of the six websites	Account hijackings via recovery (if SMS-based recovery is enabled)	79 (79%)	92 (58%)	171 (66%)
Linked account at any of the four *doubly insecure* websites	Account hijackings via recovery	44 (44%)	56 (35%)	100 (39%)
Amazon	Account hijackings via recovery	17 (17%)	17 (11%)	34 (13%)
AOL	Account hijackings via recovery	4 (4%)	5 (3%)	9 (3%)
PayPal	Account hijackings via recovery	16 (16%)	19 (12%)	35 (14%)
Yahoo	Account hijackings via recovery	22 (22%)	43 (27%)	65 (25%)
Linked account at any of the six websites **AND** involved in a password breach	Account hijackings without password reset	50 (50%)	50 (31%)	100 (39%)

test to evaluate if these difference was significant, and we found strong support for the hypothesis that the hit rate in the *Likely recycled* group was greater than that of the *Possibly unused* group ($p < 0.0001$ for both carriers).

In addition to finding hits, we also logged any associated email address that appeared in the owner history. For each address, we checked for involved password breaches on *Have I Been Pwned?* (HIBP)—an online service that allows users to check whether their credentials and other identifying information have been compromised in data breaches. This enabled us to quantify the effectiveness of the **account hijacking without password reset** attack (§ IV-B).

Finally, we measured the fraction of *Likely recycled* numbers linked to existing online profiles. For each number in the sample, we used the account recovery feature of Amazon, AOL, Facebook, Google, Paypal, and Yahoo to locate any linked accounts, as an adversary would. In contrast to an adversary, upon receiving a response (account found/not found), we aborted the recovery process. The procedure allowed us to determine whether an available number was still linked to an existing account. We selected Google (Alexa Rank 1; Google's YouTube is AR 2), Amazon (AR 3), Yahoo (AR 4), and Facebook (AR 5) based on their popularity in the U.S. We selected Amazon, AOL, Paypal, and Yahoo because they allow simultaneous use of SMS 2FA and SMS account recovery on new (previously unseen) devices, which was found in a previous study looking at SIM swaps [19]. Accounts with this *doubly insecure* configuration—a term coined by the study which we borrow for the remainder of our paper—are at immediate risk of takeover, an adversary can hijack a linked account just by obtaining a recycled phone number. These websites remain *doubly insecure* as of August 2020.[12] The other two websites in our study—Google and Facebook—use SMS-based recovery conditional on 2FA settings; SMS recovery is allowed only if SMS 2FA is not enabled. This enabled us to quantify the effectiveness of the **account hijacking via recovery** attack (§ IV-B). We were aided by the fact that all websites we selected give a negative response if no linked account is found.

[12]We verified the *doubly insecure* configuration on newly-created accounts with no associated assets on two different devices. It is possible that these websites employ additional authentication for real-world accounts based on activity or some other notion of value.

4) Ethical considerations and responsible disclosure

We registered our method with our university's Institutional Review Board in July 2020. Our research plan was ruled as non-human subjects research. Nevertheless, we took steps to mitigate the risk of harm to previous owners of the phone numbers in our study. We determined—through our own accounts—that initiating account recovery with a phone number and aborting once a linked account is found does not raise any alerts to the user at any of the six services studied. Secondly, we deleted all identifying information (e.g., phone numbers, emails) at the end of our study. Lastly, we kept the *Likely recycled* numbers in our study relatively small as to avoid any erroneous overshoots in account recovery processes, which we executed manually.

We performed these measurements in August and September 2020, and provided initial notification to the carriers we studied and CTIA on October 22, 2020. We presented our findings to major carriers and CTIA in November 2020.

B. Results: previous owners of most recycled numbers are at risk

We document the hit rates of our testing methods on all 259 numbers in Table III. As mentioned in § III, each method to test was motivated by a corresponding attack—presented in Table I—that an adversary can leverage on previous owners upon taking control of the number.

Our findings are as follows:

1) **Most numbers enable impersonation attacks through *PII indexing*.** Of the 259 numbers we analyzed, 171

(66%) produced a hit at either BeenVerified or Intelius. As previously described, an attacker can use these services to gather previous owners' PII. Once they obtain the previous owner's number, they can perform impersonation attacks.

2) **Most numbers enable *account hijackings via recovery*.** 171 / 259 numbers in our sample (66%) had a linked existing account on *at least* one of the six websites. An attacker can potentially break into all of these accounts—even at Facebook and Google if SMS-based recovery is enabled (highlighted yellow in Table III).
   One especially concerning result is the hit rate at *doubly insecure* websites: Amazon, Yahoo, Paypal, and AOL. 100 (39%) of the numbers we sampled had a linked account on ***at least*** one of the four websites (highlighted red in Table III)
   We do not know how many of the accounts in our sample had SMS-based recovery enabled since we aborted the account recovery process after determining whether a linked account exists. However, for a subset of numbers—68 of 171 (26%)—we can confirm that the accounts are definitely vulnerable. These numbers were linked to accounts at Yahoo or AOL, both of which have no alternative to *doubly insecure* configurations (Amazon and Paypal do have secure alternate configurations, though not by default).
3) **Some numbers enable *account hijackings without password reset*.** In total, we found 100 phone numbers (39% of our sample) with at least one associated email address that had been involved in a password breach and had linked profiles on at least one of the six websites. Apart from the *doubly insecure* sites, the rest of the websites in our analysis (Facebook and Google) allow for SMS 2FA, and thus are as vulnerable to this attack as much as the other four (highlighted yellow in Table III).
4) **Other authentication methods are also at risk of takeover.** Three of the six websites we analyzed—Google, Yahoo, and AOL—provide consumer webmail services in the U.S. 139 of the 259 numbers (54%) were linked to an account on at least one of the three websites. As a common recovery and 2FA option, email-based passcodes can also be intercepted once an attacker hijacks the inbox with a recycled phone number.

Our key finding is that attackers can feasibly leverage number recycling to target previous owners and their accounts. The moderate to high hit rates of our testing methods indicate that most recycled numbers are vulnerable to these attacks. Furthermore, by focusing on blocks of *Likely recycled* numbers, an attacker can easily discover available recycled numbers, each of which then becomes a potential target.

V. Analysis: Inventory of Recycled Numbers

According to the FCC, 35 million phone numbers in the U.S. are disconnected each year [5]. This suggests that a vast number of recycled numbers may be available to attackers. In this section, we quantify the inventory of recycled numbers in two steps: first we analyze a snapshot in time; then we analyze the churn rate. We confirm that a large number of recycled numbers (about one million) are available at Verizon, and tentatively find that this inventory of recycled numbers is largely replaced by a fresh set of numbers within a month.[13]

A. Recycled numbers estimates

We used the following strategy for estimating the number of available recycled numbers at Verizon.

- Let P be the number of all available phone numbers.
- Let R be the number of all available phone numbers that are recycled. This is our estimand.
- Let r be the probability that a number selected is recycled. By definition, $r = \frac{R}{P}$
- Let S be the number of numbers from NPA-NXX blocks with no two available numbers being within 10 of each other. **We assume that all such numbers are recycled.**
- Let H be the hit rate at people search services; that is, the proportion of numbers that return any information on past owners.
- By our assumption, $H_R = H_S$

$$
\begin{aligned}
H_P &= \frac{R}{P}H_R + (1 - \frac{R}{P})H_{\bar{R}} && \text{by definition} \\
&= \frac{R}{P}H_R && \text{We set } H_{\bar{R}} \text{ to 0 since a new number won't get any hits} \\
&= \frac{R}{P}H_S && \text{by substitution} \\
&= r\,H_S && \text{by substitution} \\
r &= \frac{H_P}{H_S}
\end{aligned}
$$

We now have two expressions for r; equating them, we get $R = P\frac{H_P}{H_s}$. Our measurements allowed us to estimate each of the three quantities on the right hand side of this equation as follows.

To estimate P (Verizon's inventory of available numbers), we extrapolated the results of our iteration through available NPA-NXXs in § IV. We had exhaustively iterated 875 of the valid NPA-NXX prefixes and logged 8,603 available numbers. Since there are 180,741 valid NPA-NXX prefixes, we estimate P to be 1.8M (95% CI [860K, 2.7M]).

In our lookups at people search services in § IV-A3, we had found H_S to be 96/159, and the hit rate from the *Possibly unused* pool to be 53/159. We then computed H_P by taking a weighted sum of those two sample proportions. We estimate R—the available number of recycled numbers—to be 996K (95% CI [420K, 1.6M]).

Recall that in the previous section we simulated an adversary trying to maximize chances of finding a recycled number. He restricts himself to the *Likely recycled* pool—NPA-NXX blocks for which no two available numbers were within 10 of each other. Even with this restricted strategy, the number

[13] We are unable to estimate the corresponding numbers for T-Mobile due to restrictions of the online interface that prevented us from viewing all available numbers.

of available recycled numbers at any given time is vast: we estimate S to be 33K (95% CI [18K, 48K]).

While the total number of available recycled numbers is important in terms of an adversary seeking to carry out large-scale attacks, the probability of receiving a recycled number from navigating the online interface is also relevant since it quantifies the risk to a subscriber seeking a fresh number. If a Verizon prepaid subscriber were to change their number online by entering an NPA-NXX at random, she would receive a recycled phone number 41.6% of the time (95% CI [30.5%, 52.6%]). This figure assumes all *Likely recycled* numbers are recycled, and that all *Possibly unused* numbers are brand new.

B. Churn analysis

New recycled numbers become available over time, in accordance with FCC number aging rules. To quantify number churn at Verizon, we randomly selected 20 of the 77 NPA-NXXs from our initial collection phase (§ IV-A1) and logged all available numbers. 15 of the 20 selected NPA-NXXs had availability in September. We collected numbers at the end of September and October 2020.

We made two key findings:

1) **Available numbers are assigned quickly.** We measured churn by dividing the size of inventory lost at the end of the month (numbers that do not appear in the next month's dataset) by the inventory size at the beginning of the month. We estimate the monthly number churn rate to be 86.5% (95% CI [85.2%, 87.8%]); only 330 of the 2,449 total logged numbers in September were still available in October. Assuming a constant monthly churn rate, we estimate that an available number gets taken after 1.2 months. Individually, most NPA-NXXs had high monthly turnover. Of the 15 NPA-NXXs, 12 of them had at least 80% churn during the month of observation, eight NPA-NXXs had a 100% churn rate during observation. Only two NPA-NXXs had churn rates below 50%; we speculate these are prefixes in areas with numerous other highly available prefixes (since the number change interface allows geographic queries as well) or in areas with little subscriber activity.
2) **New recycled numbers were being made available over time.** Six of the eight NPA-NXXs had new available numbers that resembled *Likely recycled* traits (i.e., no two available numbers are within 10 of each other).

Taken together, these findings suggest that not only are about one million recycled numbers available at any one time (§ V-A), but also that a largely fresh set of recycled numbers becomes available within one month.

Unfortunately, we were unable to analyze churn after October. On November 17, 2020, we discovered Verizon had patched their prepaid backend system to return only a limited set of available numbers for each NPA-NXX, although we could still make unlimited queries. As such, we were unable to measure longitudinal trends of Verizon's numbering resources.

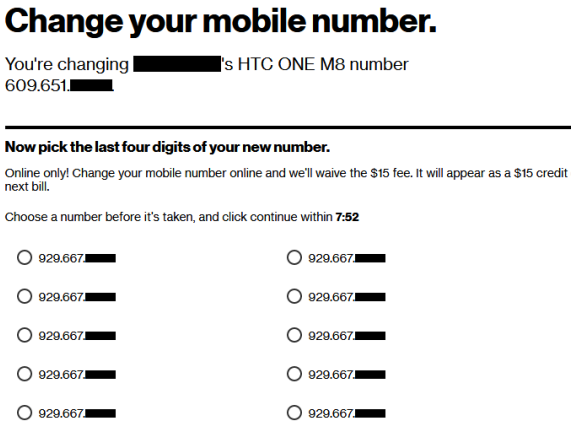

Fig. 4: Verizon's number change interface for postpaid subscribers. We have redacted the last four digits of each number.

VI. Analysis of carrier interfaces and recycling policies

A. Most number change interfaces have no limits

Adversaries can take advantage of the lack of limits on number change interfaces to quickly discover recycled numbers and carry out attacks. We further investigated the interfaces at T-Mobile and Verizon for postpaid and prepaid subscribers. Using carrier-published FAQs, webpage element inspection, and interactions with the interface (including interactions from § IV-A1), we documented the change and query limits carriers had in place. Our findings are shown in Table IV.

Both T-Mobile and Verizon prepaid interfaces allow for unlimited queries on available numbers. T-Mobile additionally does not place limits on changes. Both carriers impose limits on their postpaid subscribers: Verizon limits both the number queries and amount of changes, while T-Mobile does not support online number changes. All online interfaces display full numbers, which gives an attacker the ability to discover recycled numbers before confirming a number change.

Despite having more limits on their online interfaces (or lack of an interface altogether), postpaid customers are not immune to number recycling threats. We discovered both carriers using the same number pools when we were able to change the number on our postpaid lines (T-Mobile postpaid over the phone) to numbers we had seen on their prepaid interfaces. This means that **postpaid subscribers are also at risk for number recycling attacks**, despite throttling in their interfaces. In fact, attackers may choose to use prepaid accounts due to lower cost and absence of identity checks.

B. CSRs had inconsistent responses about aging periods

In addition to investigating interfaces, we attempted to learn the number recycling policies at T-Mobile and Verizon. Since neither carrier offers public-facing documentation on the matter, we called CSRs at each carrier and inquired about the status of our old numbers in a number change, using a different account each time. We asked for the aging period—the time

TABLE IV: Characteristics of the online number change interfaces at T-Mobile and Verizon for prepaid / postpaid subscribers.

	T-Mobile		Verizon	
	Prepaid	**Postpaid**	**Prepaid**	**Postpaid**
Change limit(s)	None	Online number changes are not supported; changes can only be done over the phone by calling customer service	3 changes per day; 5 changes per rolling 30 days	1 change every 7 days
Query limit(s)	No limit on amount of queries; up to 5 NXXs per NPA query, up to 5 available numbers per NXX (25 total numbers per NPA)		Queries not allowed if there are any change limits in effect, otherwise, no limits	6 NPA-NXX queries / day; up to 10 available numbers shown per NPA-NXX; subscriber is allowed 10 minutes to select an available number; queries not allowed if change limits reached
Fee(s)	Free	1 free change per year, per line; additional changes $15	Free	Free if done online

between subscribers losing access to their old number and the number being available for assignment. As mentioned, the FCC-mandated minimum aging period is 45 days (§ II). We placed 13 calls at each carrier—ten at prepaid and three at postpaid—from September to November 2020.

We found that CSR responses were wildly inconsistent.

1) At T-Mobile, we received seven different responses across 13 calls.
2) At Verizon, we received eight different responses across 13 calls.
3) Responses were highly varied. The purported aging period ranged from one hour to one year at T-Mobile, and one week to four months at Verizon.
4) At both carriers, there was no majority response, however, the plurality response at each was 30 days.
5) In two instances at each carrier, CSRs mentioned there was no specified aging period policy. In one of those instances at Verizon, the CSR purported that all previous numbers remained linked to the account—and could not be reassigned—as long as the account remained active.

Based on the widely different responses we received, we were unable to determine either carrier's current recycling policies. Furthermore, the inconsistent knowledge among company personnel also poses a concrete problem for subscribers.

C. Subscriber confusion about carrier recycling practices could result in security issues

If CSRs at T-Mobile and Verizon are uninformed of number recycling policies, they may end up passing incorrect information to subscribers. We systematically searched carrier-hosted community support forums at all major carriers—AT&T, T-Mobile, and Verizon—by using number recycling-related queries, and noting responses on top relevant posts as of January 2021. We further examined independent forums by searching with the same querystrings along with the carrier name. We noted nine different responses across seven posts.

On both types of forums, speculation on aging periods varies widely; responses ranged from no aging period to six months. Four responses claimed numbers were reassigned in 60 days, and three responses—one from company staff—claimed that numbers were reassigned in six months (see Appendix A for individual subscribers' statements).

These responses should be interpreted anecdotally, primarily due to limited number of posts and responses we were able to find. Regardless, the lack of any public-facing documentation and inconsistent CSR knowledge exacerbate the problem. Subscriber uncertainty about number recycling can have serious security consequences. Previous owners may incorrectly perceive the aging period for their disconnected numbers to be much longer than it actually is, and put off updating their online accounts. In the meantime, those numbers may have become available again for other subscribers—possibly attackers—to obtain. Temporarily-disconnected subscribers are also affected: they may return to find that their number has been reassigned, despite being told of a longer aging period.

VII. Analysis of calls and texts meant for previous owners of recycled numbers

So far, our analysis has centered on a motivated adversary who is aware of number recycling vulnerabilities and exploits them via online number change interfaces. Now we consider the perspective of a subscriber who is unknowingly assigned a recycled number and opportunistically exploits vulnerabilities.

We seek to estimate the fraction of recycled numbers which receive sensitive communications meant for previous owners without the need for any explicit action by the new subscriber. Such messages may by themselves compromise the privacy of the previous subscriber or alert the new subscriber to the fact that they are in a position to exploit a security vulnerability.

A. Method

1) We obtained 200 recycled numbers

At T-Mobile and Verizon, we signed up for 10 prepaid accounts, for a total of 20 accounts. For each Verizon account, we entered a random NPA-NXX and checked if the returned available number was linked to accounts at any of the six websites we studied in § IV-A3. If so, we confirmed the change and obtained the recycled number, otherwise, we randomly selected a new NPA-NXX and repeated the process. Similarly, at each T-Mobile account, we entered a random NPA and iteratively looked up the 25 selectable numbers (interface details in § IV-A1) until we found and obtained one with a linked online profile. We repeated the process at all 20

TABLE V: A breakdown of identified calls / texts. We inferred the nature of communication using metadata.

Nature of call / text	Unique senders	Total calls / texts	Recycled numbers affected (out of 200)
Security/privacy-sensitive	24	60	19 (9.5%)
Authentication OTPs	7	13	6 (3%)
PII	17	47	14 (7%)
Marketing	19	40	13 (6.5%)

accounts for 10 weeks, giving us a total of 200 recycled phone numbers that we monitored for one week each.

2) We collected info about incoming calls / texts

We kept all 20 phone accounts powered-on and actively connected for the entire 10-week period while monitoring incoming calls and messages. All accounts were provisioned on unlocked Android phones. We restarted the devices only after a number change each week. At the end of each week, we ran an Android application to 1) write the timestamp, sender phone number, and communication type (call / text) to a file on device storage, and 2) clear the call log and message inbox. We retrieved the file onto our computer and used it in our analysis.

We ran our honeypot from November 2020 to January 2021, and received 1491 total calls / texts (561 texts, 930 calls) from 1064 different senders. It is important to note that these unsolicited personal calls / texts made to our honeypot should mainly be the result of number recycling, but in rare cases, they can be the result of an incorrectly dialed number.

3) Identifying sensitive calls / texts with only metadata

To identify sensitive calls, we collaborated with Nomorobo—a robocall blocking service. We selected Nomorobo because of its popularity in the robocall detection space and its recent collaboration with academic researchers in a longitudinal study on robocalls [34]. We worked directly with the company's founder, who used Nomorobo's honeypot data to identify spam robocalls and likely spoofed numbers in our dataset. We were also provided with an allowlist of callers; that is, legitimate robocalls that appeared in our dataset. From the allowlist, we were able to infer the nature of the calls we received.

To identify sensitive messages, we focused on short codes—5-6 digit phone numbers—seen in our dataset. Short codes—which are used to send high-throughput content, such as marketing, alerts, and 2FA messages—are regulated differently from 10-digit numbers, making them harder to spoof and easier to find owner (organization) information.[14] We manually classified the 48 seen short codes in our dataset by looking up their owner in the publicly-available owner database, by texting "HELP"—a standardized keyword to request service information—from our personal phone numbers, and by searching the web for websites that mention this short code.

4) Ethical considerations

We registered our method with our university's IRB in July 2020. Our research plan was ruled as non-human subjects research. We also checked to make sure there were no legal issues with receiving communications meant for previous owners. Nevertheless, we took steps to mitigate the risk of harm to previous owners of the phone numbers in our honeypot. As we did in our analysis of attacks against previous owners (§ IV), we determined that reverse lookups on all six websites did not raise alerts to the previous owner. Secondly, we deleted all collected data at the end of the study. Most importantly, we took steps to protect previous owners' privacy: we only collected call / text metadata. We developed an app to collect metadata and clear out inboxes and call logs, ensuring no member of the research team would need to view message content. We made this decision despite knowing that it could result in underreporting the number of sensitive messages.

[14]CTIA oversees short code assignments and maintains an owner database that is publicly available.

B. Results: nearly 10% of numbers received sensitive calls / texts meant for previous owners

We documented the number of sensitive calls / texts sent to our honeypot in Table V. Our findings are as follows:

1) **19 numbers in our honeypot—nearly 10%—received sensitive calls / texts meant for previous owners.** These numbers received calls / texts containing PII or authentication passcodes. Upon receiving sensitive communication meant for the previous owner, a subscriber can realize his exploitative position and target the previous owner and her accounts. We highlight that this was the result of just one week of monitoring; it is possible that we could have identified more messages (and vulnerable numbers) if we monitored for longer.
   a) **6 numbers were still getting authentication calls / texts.** We identified seven senders that were associated with 2FA passcodes: Apple, Cash App, Facebook, Google, Microsoft, and WhatsApp (2 different numbers). As a result of losing their number, previous owners are now locked out of their accounts since they are unable to receive the sent OTP. Additionally, the adversary—after seeing the call / text—can zero in on hijacking the previous owner's account because he has now learned that she 1) has a linked account, and 2) uses SMS authentication, which he can defeat.
   b) **14 numbers received PII-revealing calls / texts.** We identified 17 senders that were associated with PII-revealing messages. These included pharmacy calls, school alerts, hospital calls, appointment reminders, and mobile banking texts. These potentially contain PII, which the adversary can amass to threaten previous owners. Worse, the adversary

can possibly manipulate appointments and prescriptions by responding.

2) **Separately, 13 numbers received unsolicited marketing texts.** Apart from our main finding, we identified 19 short codes owned by marketing campaigns, totalling 40 texts. Yet we did not consent to receiving these messages. This demonstrates a known issue faced by marketing campaigns: under 47 U.S.C. § 227, subscribers must opt-in to receiving messages, however, the senders currently have no practical way of determining changes in number ownership. It is important to note that marketing campaigns may apply to use the RND once available, so the number of unsolicited marketing messages may decrease in the future.

Our key finding is that a significant proportion of our obtained recycled numbers still received sensitive communication during their one-week monitoring period. Through industry collaboration and short code lookups, we were able to use only metadata to infer the nature of received calls / texts in our honeypot, and conservatively quantify a direct consequence of subscriber confusion about number recycling.

VIII. Recommendations

Phone number recycling attacks can harm subscribers, yet they involve different stakeholders. As mentioned, the FCC has recently implemented an RND to help legitimate robocallers avoid placing calls to recycled numbers (§ II-D). Since the database is a closed resource, it remains unclear whether this mechanism—along with access to it—can be extended to prevent any of the attacks we presented. In the meantime, carriers, websites, and subscribers can take protective measures.

A. Recommendations for carriers

1) **Warn subscribers of the risks of phone number reassignment.** Neither carrier offers any information about number recycling risks on their online interfaces. When we called T-Mobile to change the number on our postpaid account, we were briefly told to update our linked online accounts before consenting to the change. Carriers should inform subscribers that phone numbers are recycled, and provide adequate warning to them about possible threats before beginning the number change process. Specifically, carriers should ask subscribers to update any linked accounts number and to inform their peers. Carriers can also recommend subscribers keep track of any accounts tied to their new phone number upon a change (or upon account signup). That said, it is unclear whether the advice to update linked accounts is practical: according to a 2017 study, the average user has 150 online accounts [35].
2) **Publicly document number recycling policies and timelines.** Carriers should document their number recycling policies, including the ways subscribers can lose access to their numbers as well as a timeline for regaining access to them. Carriers stand to benefit from informing subscribers, as speculation on forums varies widely. Subscribers should not be left to guess the amount of time they have to update their peers, online accounts, and bank accounts. T-Mobile and Verizon should also clearly document their policy in CSR playbooks to ensure correct and consistent responses.
3) **Place limits on phone number inquiries online.** On postpaid interfaces, Verizon already has safeguards and T-Mobile does not even support changing numbers online (Table IV). However, the number pool is shared between postpaid and prepaid, rendering all subscribers vulnerable to attacks. Carriers should not allow for unlimited queries at their prepaid interfaces. They can also consider restricting subscribers from viewing full numbers online, and instead direct subscribers to contacting customer service if they wish to do so.
4) **Place limits on phone number changes online.** In addition to limiting queries, carriers should limit the amount of times subscribers can request a number change. Verizon already places limits on number changes for both prepaid and postpaid, yet T-Mobile allows for unlimited number changes at its prepaid service. Without restrictions, an attacker can carry out large-scale account hijackings with a single account by constantly switching numbers (§ III). Limiting number changes would essentially reduce the number of hijacked accounts an attacker can amass and sell on the dark web, hence reducing the profitability of the attack.
5) **Offer number parking for inactive subscribers.** If a subscriber knows that they will not require phone service for an extended period of time (e.g., a college student studying abroad), they should be given an opportunity to keep their number. There already are third-party services in which subscribers can store their phone number on a low-cost monthly subscription; transferring to the service cancels and removes the need to pay for their more expensive carrier plan [36]. This is different from a voluntary / vacation suspension, which does not cancel the mobile plan and is capped at 90 days by the FCC. T-Mobile and Verizon already offer voluntary temporary service suspensions for their postpaid subscribers only.

B. Recommendations for websites

While carriers can raise awareness and provide clarification about phone number recycling, subscribers with accounts on websites relying on SMS 2FA continue to be at risk. In a study looking at SIM swaps, Lee et al. examined 2FA and recovery settings at over 140 websites, and discovered 83 sites had defaulted to SMS 2FA, which could be defeated with a phone number hijacking like a SIM swap [19]. Worse, 17 websites were *doubly insecure* (4 of which we analyzed in § IV); an attacker could hijack SMS 2FA-enabled accounts without knowing the passwords.

Websites need to recognize the security ramifications of their default and allowed configurations, which put accounts at risk of takeover. Our recommendations for websites are identical to that from the SIM swaps study:

1) *Doubly insecure* websites need to prevent simultaneous use of SMS for account recovery and 2FA
2) Implement at least one secure 2FA option
3) Eliminate / discourage SMS 2FA

Websites can explore more effective 2FA and recovery reminders through usable security research. One such reminder design can explicitly ask users to remove inaccessible factors—such as previous phone numbers—when reviewing 2FA options. To that end, websites should also provide support to users who no longer have phone service at all, and offer alternate forms of identity proof.

Ultimately, number recycling attacks should give further reason for websites to move away from using phone-based authentication, since they have no reasonable way of determining changes in number ownership.

C. Recommendations for subscribers

Earlier, we highlighted that subscribers may choose to keep their phone number when switching providers (§ II). Number portability is regulated by the FCC and mandates that carriers allow active subscribers to switch to a competitor while retaining their original number for little to no cost (47 C.F.R. § 52.35). The transfer procedure is called *porting*. Portability facilitates seamless transition between carriers.

Porting has an added—and largely unrealized—use case: preventing reassignment of a number that a subscriber no longer wants to use. We refer to porting for this purpose as *parking*.

We recommend subscribers park their current phone numbers when disconnecting their lines. Subscribers can park their number at a dedicated parking service (e.g., NumberBarn offers low-cost monthly number parking), a mobile virtual network operator (which usually offers plans cheaper than those of major carriers), or to a VoIP provider like Google Voice (which charges a one-time fee to port in a phone number, which then never expires). This includes subscribers looking to change their number, and those who need to temporarily disconnect their lines beyond the 90-day suspension offered by some carriers (e.g., a worker contracted overseas).

Number parking mitigates several number recycling threats:

1) Subscribers now have more time to update their SMS 2FA settings.
2) Temporarily-disconnected subscribers can prevent accidental number losses from aging period confusion.
3) IPV survivors can prevent their old number from being available for reassignment for some period of time, in order to prevent abusers from taking over the old number (**Targeted takeover**).

When the subscriber is ready to release her old number, she can cancel her parking subscription. The parked number will be returned to the original carrier for recycling. Returning subscribers can resume usage by "unparking"—porting out their parked number—to their original or new carrier.

While effective, parking may not always be feasible. Number portability only allows active subscribers to move their current phone numbers; those who have already given up their number—for reasons we listed in § II-B—will generally be unable to get their number back to park.

TABLE VI: Measures that subscribers can take against the eight number recycling attacks.

Attack	Mitigating step(s)
PII indexing	Avoid unnecessarily sharing PII; opt out of people search databases [37]
Account hijackings via recovery	Avoid SMS 2FA/recovery if secure options are available; avoid *doubly insecure* setups; remove previous numbers from account settings
Account hijackings w/o password reset	Avoid password reuse; avoid SMS recovery; remove previous numbers from account settings
Targeted takeover	Park old number indefinitely; file criminal complaint for cyberstalking
Phishing	Ignore and report phishing messages, avoid clicking on links; call carrier to verify
Persuasive takeover	Ignore and report phishing messages
Spam	Report spam texts to carrier and to FCC; enable spam blocker
Denial-of-service	Ignore ransom requests to "free-up" recycled number; contact websites to manually prove ownership of number

In Table VI, we list steps subscribers can take to combat the threats from the eight number recycling attacks we introduced in § III. For attacks affecting previous owners (**PII indexing**, **Account hijackings via recovery**, **Account hijackings without password reset**, and **Targeted takeover**), these steps should be taken with our primary recommendation to park the number (if feasible).

These mitigating steps require subscribers to be proactive. Moreover, not all steps guarantee complete protection, and some may be hindered by external factors. For instance, a website might not allow a subscriber to remove their previous recovery phone number without providing a new number—the subscriber might not have an active number. Furthermore, even if a subscriber opts out of people search databases, their PII remains publicly available on websites from which it originates. While subscribers can certainly reduce the risks of number recycling attacks with these measures, these threats remain feasible so long as phone numbers are recycled.

IX. Conclusion

As a regulated industry practice, phone number recycling is unlikely to cease. We highlighted eight different security and privacy threats that are perpetuated by number recycling, and empirically showed the seriousness of three of those attacks. Although we successfully advocated for the two carriers we studied to clarify their number recycling policies for subscribers, more work can be done by all stakeholders to illuminate and mitigate the issues. In particular, online services should no longer equate a correctly-entered SMS passcode with successful user authentication.

Acknowledgements

We are grateful to Aaron Foss of Nomorobo for providing much-needed assistance during our number monitoring analysis, and for being so accommodating during the collaboration.

We thank Malte Möser for his tremendous support throughout the study design and writeup, Tony Ye for his advice on the number inventory analysis, and Ben Kaiser, Paul Ellenbogen, Ryan Amos, and Conor Gilsenan for their helpful feedback on our writeup. We are thankful to Jonathan Mayer and Mihir Kshirsagar for assisting with our vulnerability notification to carriers.

This work is supported by a grant from the Ripple University Blockchain Research Initiative.

References

[1] B. Krebs. (Mar. 17, 2019). "Why Phone Numbers Stink As Identity Proof." Krebs on Security, [Online]. Available: https://krebsonsecurity.com/2019/03/why-phone-numbers-stink-as-identity-proof/ (visited on 01/04/2021).

[2] N. Lloyd. (Nov. 26, 2016). "Why giving up your phone number can mean giving up your privacy." Los Angeles Times, [Online]. Available: https://www.latimes.com/business/la-fi-tn-phone-number-security-20161125-story.html (visited on 01/08/2021).

[3] A. McDonald, C. Sugatan, T. Guberek, *et al.*, "The annoying, the disturbing, and the weird: Challenges with phone numbers as identifiers and phone number recycling," in *Proceedings of the 2021 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, May 2021. DOI: 10.1145/3411764.3445085.

[4] 2factorauth, *2FA Directory*. [Online]. Available: https://2fa.directory/ (visited on 01/15/2022).

[5] Federal Communications Commission. (). "In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Second Notice of Inquiry," [Online]. Available: https://docs.fcc.gov/public/attachments/FCC-17-90A1.pdf (visited on 01/18/2021).

[6] ——, (). "Numbering Resource Utilization in the United States," [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-367592A1.pdf (visited on 01/18/2021).

[7] P. Bump. (Apr. 23, 2015). "People are paying tens of thousands of dollars for custom phone numbers. These are the most expensive." The Washington Post, [Online]. Available: https://www.washingtonpost.com/news/wonk/wp/2015/04/23/how-to-make-100000-by-selling-a-phone-number-on-the-internet/ (visited on 01/09/2021).

[8] Google. (). "Google voice acceptable use policy," [Online]. Available: https://www.google.com/googlevoice/program-policies.html (visited on 04/15/2021).

[9] Twilio. (). "Best practices for phone number use," [Online]. Available: https://www.twilio.com/docs/phone-numbers/best-practices (visited on 04/15/2021).

[10] Federal Communications Commission. (). "Numbering Resources," [Online]. Available: https://www.fcc.gov/general/numbering-resources (visited on 01/14/2021).

[11] ——, (). "In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Second Report and Order," [Online]. Available: https://docs.fcc.gov/public/attachments/FCC-18-177A1.pdf (visited on 01/18/2021).

[12] ——, (). "Consumer and Governmental Affairs Bureau Announces Compliance Date for Reassigned Numbers Database Rules," [Online]. Available: https://docs.fcc.gov/public/attachments/DA-20-706A1.pdf (visited on 01/18/2021).

[13] ——, (). "Reassigned Numbers Database," [Online]. Available: https://www.fcc.gov/reassigned-numbers-database (visited on 01/23/2022).

[14] ——, (). "Reassigned Numbers Database (RND) Technical Requirements Document," [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-361954A1.pdf (visited on 01/18/2021).

[15] L. Särud. (May 24, 2018). "The danger of recycled phone numbers." Detectify Labs, [Online]. Available: https://labs.detectify.com/2018/05/24/recycled-phone-numbers/ (visited on 01/04/2021).

[16] D. Strobel, "IMSI catcher," M.S. thesis, Ruhr-Universität Bochum, Jul. 13, 2007. [Online]. Available: https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf (visited on 06/08/2020).

[17] Positive Technologies. (). "SS7 Security Report," [Online]. Available: https://positive-tech.com/storage/articles/ss7-security-report-2014-eng.pdf (visited on 06/07/2020).

[18] K. Nohl, "Mobile self-defense," 31st Chaos Communication Congress (31C3), Dec. 27, 2014, [Online]. Available: https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf (visited on 06/08/2020).

[19] K. Lee, B. Kaiser, J. Mayer, *et al.*, "An Empirical Study of Wireless Carrier Authentication for SIM Swaps," in *Proceedings of the 16th Symposium On Usable Privacy and Security (SOUPS)*, Virtual Conference, Aug. 2020. [Online]. Available: https://www.usenix.org/system/files/soups2020-lee.pdf (visited on 11/29/2020).

[20] Verizon Media, *Verizon Media Terms of Service*, Feb. 2021. [Online]. Available: https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html (visited on 04/15/2021).

[21] Microsoft, *Microsoft Services Agreement*, Aug. 1, 2020. [Online]. Available: https://www.microsoft.com/en-us/servicesagreement/default.aspx (visited on 04/15/2021).

[22] Google, *Create a replacement Google Account*. [Online]. Available: https://support.google.com/accounts/answer/7564124 (visited on 04/15/2021).

[23] D. Gross. (Jun. 20, 2013). "Yahoo 'recycling' old e-mail, raising security concerns." CNN, [Online]. Available: https://www.cnn.com/2013/06/20/tech/web/yahoo-recycled-email/index.html (visited on 01/19/2021).

[24] J. Schofield. (Jul. 18, 2013). "Hotmail: are my lost accounts a security risk?" The Guardian, [Online]. Available: https://www.theguardian.com/technology/askjack/2013/jul/18/hotmail-lost-accounts-security-risk (visited on 01/19/2021).

[25] Federal Trade Commission. (Aug. 31, 2020). "How to Recognize and Report Spam Text Messages," [Online]. Available: https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages (visited on 01/20/2021).

[26] L. H. Newman. (May 21, 2020). "ShinyHunters Is a Hacking Group on a Data Breach Spree." WIRED, [Online]. Available: https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/ (visited on 02/08/2021).

[27] R. McMillan. (Nov. 8, 2019). "He Thought His Phone Was Secure; Then He Lost $24 Million to Hackers." The Wall Street Journal, [Online]. Available: https://www.wsj.com/articles/he-thought-his-phone-was-secure-then-he-lost-24-million-to-hackers-11573221600 (visited on 12/01/2019).

[28] B. Krebs. (Dec. 18, 2017). "The Market for Stolen Account Credentials." Krebs on Security, [Online]. Available: https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/ (visited on 01/11/2021).

[29] R. Richmond. (May 2, 2010). "Stolen Facebook Accounts for Sale." The New York Times, [Online]. Available: https://www.nytimes.com/2010/05/03/technology/internet/03facebook.html (visited on 01/11/2021).

[30] D. Freed, J. Palmer, D. Minchala, *et al.*, ""A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology," in *Proceedings of the 2018 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, Apr. 2018. DOI: 10.1145/3173574.3174241.

[31] N. Kelley. (). "DIY Cybersecurity for Domestic Violence, My partner is harassing me through my cell phone." HACK*BLOSSOM, [Online]. Available: https://hackblossom.org/domestic-violence/threats/cell-phones.html (visited on 03/21/2021).

[32] B. Willingham. (May 8, 2019). "Intelius vs. Spokeo vs. BeenVerified — A Private Investigator's Review," [Online]. Available: https://diligentiagroup.com/background-investigations/intelius-vs-spokeo-vs-been-verified-private-investigator-review/ (visited on 03/22/2021).

[33] R. Clemmons. (Nov. 7, 2019). "Intelius Review: Is the Background Check Service Worth It?" [Online]. Available: https://www.asecurelife.com/intelius-review/ (visited on 02/25/2021).

[34] S. Prasad, E. Bouma-Sims, A. K. Mylappan, *et al.*, "Who's Calling? Characterizing Robocalls through Audio and Metadata Analysis," in *Proceedings of the 29th USENIX Security Symposium (USENIX Security)*, Aug. 2020. [Online]. Available: https://www.usenix.org/system/files/sec20-prasad.pdf (visited on 04/15/2021).

[35] M. Caruthers. (May 18, 2018). "World password day: How to improve your passwords," [Online]. Available: https://blog.dashlane.com/world-password-day/ (visited on 01/18/2021).

[36] A. Fendelman. (Nov. 14, 2019). "How to Park Your Cell Phone Number." Lifewire, [Online]. Available: https://www.lifewire.com/parking-how-to-hold-cell-number-577582 (visited on 04/04/2021).

[37] Y. Grauer. (Aug. 20, 2020). "How to Delete Your Information From People-Search Sites," [Online]. Available: https://www.consumerreports.org/personal-information/how-to-delete-your-information-from-people-search-sites/ (visited on 03/23/2021).

[38] R. Campbell. (Oct. 15, 1998). "Your number is up!" The Orange County Register, [Online]. Available: https://web.archive.org/web/19990222023921/http://www.ocregister.com/business/codex105w.shtml (visited on 04/04/2021).

[39] North American Numbering Plan Administrator. (Oct. 2020). "October 2020 North American Numbering Plan (NANP) Exhaust Analysis," [Online]. Available: https://www.nationalnanpa.com/reports/October_2020_NANP_Exhaust_AnalysisFinal.pdf (visited on 04/04/2021).

[40] Federal Communications Commission. (). "Consumer and Governmental Affairs Bureau Releases Report to Congress on the Status of the Reassigned Numbers Database," [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-368620A1.pdf (visited on 01/18/2021).

APPENDIX

A. Subscriber responses on forums

- https://community.verizonwireless.com/t5/Basic-Phones/How-Do-I-Check-If-Phone-has-Been-used-Before/td-p/333440.
  - (Staff: "We hold off on recycling them [phone numbers] for as long as possible, however depending on the area code and prefix, it can be reused as quickly as 6 months.")
  - ("Cell numbers get recycled (depending on where the

number is) rather often.... as in about 6 months. So it is not surprising if he is getting calls from others. ")

- https://old.reddit.com/r/verizon/comments/8d9twz/changing_number_question_does_verizon_recycle/. ("It could be as long as 90 days or as little as a few weeks depending on the carrier, the availability of other numbers in that area, etc.")
- https://www.howardforums.com/showthread.php/1801610-How-Often-Does-VZW-Re-Cycle-Numbers.
  - ("I believe I recall reading that Verizon holds the number for 30 days and then it goes back into the pool to be reissued.")
  - ("I thought it was 60 days before mobile #'s are recycled. I do recall a story a few years ago about a new customer being assigned a phone # previously owned by a high profile person in a big court case in less than 3 weeks in error.")
- https://community.t-mobile.com/accounts-services-4/how-do-you-get-your-old-number-back-after-it-s-been-hijacked-8260. ("More importantly, no one informed me that I had 60 days to get my number back.")
- https://www.howardforums.com/showthread.php/1778962-How-many-days-until-cell-number-is-recycled. ("I've heard 90 additional days after the funds expire (180 total I suppose) however your post got me curious and I called [T-Mobile] customer service. She said I would lose the number the day after funds are depleted, which I think she's in error cause I let it go once way over the 90 days and still had the same number.")
- https://forums.att.com/conversations/more-att-prepaid-discussions/recycle-deadline/5defcecebad5f2f606bc34fc. ("There is a 60 day "grace period" that exists even after your account expiration date.")
- https://forums.att.com/conversations/data-messaging-features-internet-tethering/phone-number-recyclingreusing/5ee57d68c17a067c9e6d2dbf. ("There is no stated policy that is published. The general understanding is disconnected numbers cannot be used for six months. After six months they go into 'the pool' and can be reassigned or selected randomly.")

B. Background: the North American Numbering Plan

In the United States, telephone numbers are formatted and geographically assigned according to the North American Numbering Plan (NANP). Developed by the Bell System (later known as AT&T) in the 1940s to unify inconsistent and unorganized numbering across its various regional telephone networks, the NANP has expanded to comprise the Public Switched Telephone Network (PSTN) in 20 North American countries and their territories. This has served to reduce long-distance international dialing confusion within the NANP network: all numbers are fixed-length and all countries utilize the same international calling code ("1").

The North American Numbering Plan Administrator (NANPA) serves as the supervising body for all NANP resources. As a neutral entity, the NANPA oversees interactions between NANP member countries, including disputes, audits, requests, and most importantly, number allocation. Each participating country maintains a regulatory authority over its assigned numbering resources. In the U.S., the Federal Communications Commission (FCC) serves as the regulator for U.S.-assigned phone numbers. Additionally, the FCC serves a plenary role: it periodically appoints a new administrator from the private sector to serve the position. At the time of writing, Somos, Inc. is serving as the NANPA under a five-year contract.

All NANP phone numbers are of the 10-digit format:

NPA-NXX-XXXX

- The number plan area (NPA) code, or area code, comprises the first three digits. The first digit can be in range [2,9], while the second and third digits can be in range [0,9].
- The central office (exchange) code (NXX) comprises the the next three digits. The first digit can be in range [2,9], while the second and third digits can be in range [0,9].
- The line number (XXXX) comprises the last four digits of the telephone number. All digits can be in range [0,9].

The NANP divides all territory into distinct NPAs, and assigns a three-digit area code to each region. New area codes are primarily added through NPA splits or NPA overlays. In an NPA split, the original NPA is partitioned into two smaller NPAs; one keeps the original area code, while the other is assigned the new area code. All customers in the NPA with the new area code would have their numbers replaced with new ones, freeing up resources in the original area code. In an overlay, a new area code is additionally assigned to one or more adjacent NPAs. Existing customers keep their numbers, but new customers may be assigned numbers with the new overlay code. In New York City, area code 212 was split to only cover Manhattan in 1984, customers in the other boroughs were assigned the new 718 area code. In 1999, area code 347 was added as an overlay for 718. There are currently 330 area codes in use in the U.S.

C. Background: Numbering resources and exhaustion

Historically, all carriers looking to set up service in a region were assigned an exclusive NXX within the corresponding area code, that is, blocks of 10,000 contiguous numbers. Upon the advent of new technologies—cable modems and Voice over IP (VoIP), coupled with the Telecommunications Act of 1996, barriers-to-entry were lowered, and many new local carriers sprung up in a suddenly competitive environment. As a result, available NXX assignments were rapidly depleted and new area codes had to be deployed, leading the director of the then NANPA to speculate that 10-digit phone numbers would be completely exhausted by 2025, thereby capping expansion [38]. The proliferation of new and unfamiliar area codes

also contributed to the severity of the 809 scam—a social engineering attack that baits U.S. subscribers into returning missed calls to premium-rate numbers in the Caribbean.

In 2000—in an effort to combat number hoarding and resource exhaustion—the FCC reassigned the authority of reclaiming unused NXXs to the states, away from the NANPA. State commissions could now investigate whether NXXs were being activated (made available to subscribers) within six months of assignment to the carrier, and order the NANPA to reclaim the resources otherwise. In 2001, the FCC introduced thousands-block number pooling (or simply, number pooling)—the allocation of 1,000 number blocks (NXX-X) to carriers. This essentially allowed carriers in the same service region to use the same NPA-NXX, reducing the amount of unused numbers and the rate of exhaustion. With the rollout of number pooling, carriers with entire NXX blocks in certain jurisdictions were required to donate unused to lightly used NXX-Xs back to NANPA. Carriers would also have to prove that they have less than a six-month inventory remaining in the service area before requesting additional numbers. Number pooling is currently mandatory in the top 100 Metropolitan Statistical Areas (MSAs) and in states that require number pooling; it remains optional in most of the U.S.

Recent NANPA estimates from October 2020 predict that 10-digit phone numbers will be exhausted by 2050 [39].

D. Background: Number recycling

The NANPA only activates new area and central office codes when absolutely necessary. With the FCC-imposed restrictions on NANP resources in the U.S., carriers must also strategize and plan their number assignments efficiently. To satisfy inventory and utilization requirements, carriers may choose to return disconnected blocks or reassign them to other customers. Carriers routinely pursue the second option by placing numbers back into their pool upon disconnection of service and making them available for reassignment after a waiting period. According to the FCC, 35 million phone numbers are disconnected and placed back in the pool every year [5]. As a result, new subscribers who select "new" numbers will often end up receiving communication meant for the previous owners, from threatening robocalls to personal texts.

E. Background: Related legislation

Under FCC rules, all telecommunications carriers that receive U.S. numbering resources are required to semi-annually report resource and utilization statistics, unless mandated otherwise by state commissions.[15] Carriers are also limited to a six-month inventory of telephone numbers in each of their service areas.[16] With regards to number recycling, carriers are prohibited from reassigning disconnected numbers until 45 days have elapsed since disconnection, and can age numbers for up to 90 days (365 days for numbers assigned to business customers).[17]

The FCC has taken interest in phone number recycling by way of combating unlawful robocalls made to reassigned numbers. Specifically, previous owners of recycled numbers may have consented to robocalls, whereas current owners may find such calls undesirable, but may not be given a chance to consent. Under the Telephone Consumer Protection Act of 1991 (TCPA), certain telephone calls—such as robocalls—made without the called party's consent are prohibited. In December 2018, the FCC announced a plan to create a reassigned number database, along with establishing the 45-day minimum aging period [11]. Carriers would be mandated to report recycled numbers on a monthly basis, which would be compiled into a centralized source. Callers can then check for reassigned numbers against their calling lists before initiating communication, thereby reducing the possibility of TCPA violations from calling new subscribers.

In December 2020, the commission selected SomosGov—a wholly-owned subsidiary of Somos, Inc. (the current NANPA)—as the Reassigned Numbers Database Administrator (RNDA) [40]. In November 2021, the RND became operational to FCC-verified accounts for a fee.

[15] 47 C.F.R. § 52.15(f)

[16] 47 C.F.R. § 52.15(g)(4)(iii)

[17] 47 C.F.R. § 52.15(f)(1)(ii)