



CENTER FOR  
INFORMATION  
TECHNOLOGY  
POLICY

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

December 3, 2021

**Kevin Lee**

[kvnl@cs.princeton.edu](mailto:kvnl@cs.princeton.edu)

*Ph.D. Student*

Princeton University

Joint work with Arvind Narayanan

# Takeaways



1. Phone number recycling leads to many types of security and privacy risks
2. Most available phone numbers we sampled were recycled and also vulnerable
3. Attackers do not need special skills to exploit vulnerabilities
4. There are steps we can take to mitigate the harms

Study website and paper draft: [recyclednumbers.cs.princeton.edu](https://recyclednumbers.cs.princeton.edu)



CENTER FOR  
INFORMATION  
TECHNOLOGY  
POLICY  
PRINCETON UNIVERSITY

# Why recycle?

# The U.S. is running out of phone numbers

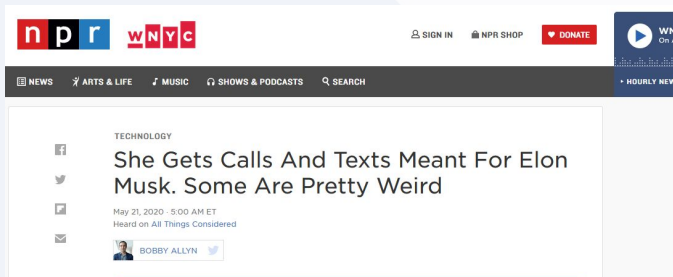


- U.S. numbers are 10 digits long: **NPA-NXX-XXXX**
  - Assigned to carriers in blocks of 1000 (NPA-NXX-X) or 10,000 (NPA-NXX)
  - 6.4 billion telephone numbers
  - 860 million numbers in use in 2018
  - 35 million phone numbers are disconnected every year
- Eventually, all numbers will be assigned to carriers, capping expansion
  - Currently estimated to be 2050
  - Replacing 10-digit dialing will be expensive

# Number recycling is a standard practice



- FCC has rules to forestall exhaustion for as long as possible
  - Only activates new NPA-NXX blocks when absolutely necessary
  - Strict usage reporting by carriers
  - **Encourages carriers to recycle numbers**
- FCC-mandated aging period: 45-90 days
- Consequence: calls/texts meant for the previous owner





# Security and privacy risks

# Your old number can leave you vulnerable



- Once your old number is made available again, someone can:
  - Amass PII on you on the web and perform impersonation attacks
  - Hijack your online accounts through SMS authentication
- Can be opportunistic, but can also be targeted
  - IPV survivors
- **Threat model:** a *UI-bound adversary*
  - Term borrowed from Freed et al. “A Stalker’s Paradise” (CHI 2018)
  - No special skills needed, a normal authenticated user
  - Expansive population

# Analysis I: we looked for vulnerable recycled numbers




- Logged available numbers at Verizon and T-Mobile through their prepaid interface
  - Verizon: randomly selected 875 of the 180,741 active NPA-NXXs and logged all available numbers at each NPA-NXX
  - T-Mobile: iterated all 330 active NPAs and logged all available numbers (up to 25 numbers per NPA---5 NXXs per NPA, and up to 5 available numbers per NXX)

Your current number  
(217) 550-■■■■

Numbers available near:

609 GOI

✓ I'm not a robot 

(609) 635-■■■■

☒ (609) 635-■■■■

☐ (609) 635-■■■■

☐ (609) 635-■■■■

☐ (609) 635-■■■■

☐ (609) 635-■■■■

Be sure to back up your stored messages and contacts by saving them to your phone memory. Your voicemail is tied to your number so you will lose all your stored information.

[Cancel](#) [Get this number](#)

## Confirm New Number

### You're about to change your mobile number.

This change will take effect immediately\*, and you won't be able to get your old number back.

**Your current Number:**  
**330.949-■■■■**

**Your new Number:**  
**609.651-■■■■**

\*In some cases this may take up to two hours

[Cancel](#)

[Submit](#)



# Analysis I: we looked for vulnerable recycled numbers



- Grouped NPA-NXXs based on simple trait:
  - *Likely recycled*: no two numbers are within 10 of each other
  - *Possibly unused*: at least two numbers are within 10 of each other
  - **Simple heuristic can also be used by attacker**

Search bar: ( ) -\*\*\*\*

- ☒ ( ) -5415
- ☐ ( ) -5712
- ☐ ( ) -6405
- ☐ ( ) -6427
- ☐ ( ) -6632

Likely recycled numbers, since they are spaced out from each other

Search bar: ( ) -\*\*\*\*

- ☐ ( ) -0415
- ☐ ( ) -0416
- ☒ ( ) -0419
- ☐ ( ) -0421
- ☐ ( ) -0428

Possibly unused (fresh) numbers, since they are close to one another

(a) T-Mobile

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

(b) Verizon

	Available Numbers	NPA-NXXs
<i>Likely recycled</i>	159	32
<i>Possibly unused</i>	8,444	45

# Analysis I: we looked for vulnerable recycled numbers



- For each *Likely recycled* number (T-Mobile: 100 randomly sampled):
  - Looked for any returned previous owner info at 2 people-search sites
  - Looked for linked accounts at 6 sites via recovery: Google, Yahoo, Amazon, Facebook, AOL, Paypal

BeenVerified™ Start a new search... Dashboard Menu

1 potential owner

Overview

Potential Owners 1

Possible Photos 0

Other Phone Numbers 5

Email Addresses 3

Address History 4

Work History 0

Educational Background 0

Social Media & Websites 5

Comments 0

Report as PDF Monitor this Report Leave a comment

(614) [REDACTED]

Phone type Mobile

Monitor this report to receive updates

Turn monitoring on

Email Addresses

Learn more

Higher Confidence

[REDACTED]

View email report

Is this accurate?

Higher Confidence

[REDACTED]

View email report

Email type Personal

Is this accurate?

yahoo!

Do you have this phone?

We will send a verification code to

+1 217-819-[REDACTED]

Message and data rates may apply

Yes, send me a code

Try another way to sign in

# Finding: most recycled numbers are vulnerable



- 66% of numbers enable impersonation attacks
  - Attackers can gather PII and then take over these numbers
- 66% of numbers enable account hijacking attacks through recovery
  - Attackers can use SMS-recovery after taking over these numbers
- 39% of numbers were linked to usernames in password breaches AND linked to accounts on at least 1 of the 6 websites
  - Attackers can login and defeat SMS 2FA, no password reset needed
- More findings in paper

# Analysis I: we looked for vulnerable recycled numbers



- Ethical considerations:
  - IRB ruled protocol as non-HSR
  - Tested reverse lookups on our own accounts/numbers to confirm no risk of harm
  - Deleted all collected info after the analysis

# Takeaway: most recycled numbers are vulnerable



- Attackers can feasibly leverage number recycling to target previous owners and their accounts
- By focusing on blocks of *Likely recycled* numbers, an attacker can greatly increase their chances of success
- Attackers are UI-bound adversaries

# Analysis 2: inventory of recycled numbers



- We know that recycled numbers are vulnerable. How many are available to attackers?
- Won't go into this in the interest of time
  - Details in paper
- Investigated recycled numbers inventory at Verizon
  - Snapshot
    - We estimate number of recycled numbers to be ~996K [420K, 1.6M] at any given time
  - Churn
    - Available numbers are largely churned (assigned to customers) and replaced every month

# Analysis 3: are carriers facilitating attacks?



- Looked for limits at the prepaid and postpaid number change interfaces at T-Mobile and Verizon
  - *How easily can attackers discover recycled numbers and obtain them?*
  - FAQs, webpage inspection, and normal interaction
- Investigated carrier resources on number recycling
  - *Are customers losing their numbers as a result of unclear policy?*
  - Neither T-Mobile and Verizon had public-facing info online
  - Called CSRs 13 times at each carrier (some postpaid, some prepaid)
    - Asked about the minimum aging period for our previous numbers

# Finding: most interfaces have few limits



- **Prepaid:** no query limits (both), no change limits (T-Mobile)
  - Verizon Prepaid allows 3 number changes a day
- Postpaid might have more limits, but number pool is shared
  - Previous owners on postpaid lines are still vulnerable to an attacker using a prepaid account

## Change your mobile number.

You're changing KEVIN LEE's HTC ONE M8 FOR WINDOWS number 609.651.████

### Now pick the last four digits of your new number.

Online only! Change your mobile number online and we'll waive the \$15 fee. It will appear as a \$15 credit on your next bill.

Choose a number before it's taken, and click continue within 7:52

- |                                    |                                    |
|------------------------------------|------------------------------------|
| <input type="radio"/> 929.667.████ | <input type="radio"/> 929.667.████ |
| <input type="radio"/> 929.667.████ | <input type="radio"/> 929.667.████ |
| <input type="radio"/> 929.667.████ | <input type="radio"/> 929.667.████ |
| <input type="radio"/> 929.667.████ | <input type="radio"/> 929.667.████ |
| <input type="radio"/> 929.667.████ | <input type="radio"/> 929.667.████ |

Continue

Back

Cancel



# Finding: CSRs are inconsistent on recycling



- **Remember:** FCC-mandated minimum aging period: 45 days
- T-Mobile: responses ranging from 1 hour to 1 year
- Verizon: responses ranging from 1 week to 4 months
- No majority response
- Some said there was no specific policy

# Finding: CSRs are inconsistent on recycling



- Inconsistent knowledge is passed on to customers



Device(s): Samsung Galaxy  
Note 4  
Carrier(s): Verizon  
Feedback Score: 0

I believe I recall reading that Verizon holds the number for 30 days and then it goes back into the pool to be reissued.

Master • 10.2K Messages



There is a 60 day "grace period" that exists even after your account expiration date. It preserves

Carrier(s): T-Mobile  
Feedback Score: 0

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.

OP, you should call VZW customer service and ask for a free mobile # change due to the inconvenience it has caused you. Just call them from a different phone or go to a retail location.

of phone numbers and they do get recycled. We hold off on recycling them for as long as possible, however depending on the area code and prefix, it can be reused as quickly as 6 months. Of course, typically calls stop shortly after the previous user updates their information. I can, of course, help changing your father's telephone number at no cost, if necessary. Please let me know if you are in need of assistance with that process.

Thanks,

## Analysis 4: recycled numbers receiving sensitive messages



- Built a honeypot of 200 randomly obtained recycled phone numbers
- Monitored incoming messages/calls for one week
  - 10 Android phones each at T-Mobile and Verizon, changed numbers every week for 10 weeks



“Honeypot”

## Analysis 4: recycled numbers receiving sensitive messages

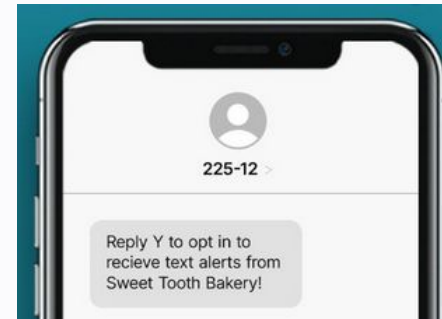


- **Considerations:**
  - IRB ruled this as non-HSR
  - No legal issue with us viewing/hearing messages meant for previous owners
  - Nonetheless, we made sure to never view the messages
    - Wrote an Android app to write all message/call log metadata (timestamp, sender info, type of message) to file
    - App also cleared out all messages and call logs
    - Ran this weekly on each device

## Analysis 4: recycled numbers receiving sensitive messages



- 1491 calls/texts in our dataset
- We identified sensitive calls and texts using metadata only
  - Sensitive calls: teamed up with *Nomorobo* to try and identify sensitive calls based on sender info (calling party number + time) only
  - Sensitive texts: looked at short code messages (5-6 digit numbers)
    - Owner information publicly available per regulation
    - Harder to spoof



## Finding: sensitive messages for previous owners still being received



- 19 lines in our honeypot (~10%) received sensitive calls/texts meant for previous owners
  - 6 lines still receiving authentication calls/texts (OTPs)
  - 14 lines received PII-revealing texts (pharmacy calls, appointments)

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



CENTER FOR  
INFORMATION  
TECHNOLOGY  
POLICY  
PRINCETON UNIVERSITY

# Recommendations

# Customer best practices



- Best thing we can do when changing numbers: port out instead
  - Allowed to bring our numbers with us to low-cost alternatives like MVNOs, parking services, or Google Voice
  - More time to update SMS 2FA settings
  - Google Voice: no need to worry about losing number if ported in
  - Prevent targeted takeovers using your old number
- More complementary mitigations in paper





# Carrier best practices



- Be more transparent about number recycling policies
  - After we informed T-Mobile about our research, they updated their website to include the 45-day minimum aging period, and informed us that they had updated their CSR playbook to specify this (December 2020).
  - Verizon also updated their website to include the 45-day minimum aging period in response to our research (December 2020)
- Consider limiting available number viewing/number changes at prepaid

# Regulator best practices



- FCC recently implemented a reassigned numbers database (RND) to combat unwanted robocalls
  - Users (legitimate robocallers) can query the database with a number and last-called date
    - Response: YES - number has been reassigned, NO - not been reassigned/not in DB
  - Must apply for access, cost-per-query is nontrivial
  - FCC can consider giving relying parties special access to the RND
    - Or RPs should deprecate SMS 2FA altogether

# Website best practices



- SMS 2FA is not secure!
  - Other attacks: SIM swaps, IMSI-catchers, SS7
  - Consider supporting other 2FA options
- Consider more effective 2FA and recovery reminders

The image displays three sequential screenshots of the Google account recovery process. Each screen features the Google logo at the top and a user profile icon with a redacted email address.

**Screen 1: Add recovery information**  
The header reads "You're signed in" followed by the redacted email. Below, it says "If you'd like, take a few moments to help Google work better for you". There are two buttons: "Add a home address" (with a house icon) and "Add or confirm your recovery email or phone number" (with a lock icon). At the bottom, it says "You can always manage this information in your Google Account." and a "Not now" link.

**Screen 2: Verify phone number**  
The header is the same. Below, it says "Verify your phone number so Google can help you if you forget the password to your account". There is a text input field with a country dropdown (showing the US flag) and a "Next" button. A "Cancel" link is also present.

**Screen 3: Recovery information updated**  
The header is the same. Below, it says "If you'd like, take a few moments to help Google work better for you". There are two buttons: "Add a home address" (with a house icon) and "Recovery information updated!" (with a green checkmark icon). At the bottom, it says "You can always manage this information in your Google Account." and a "Done" button.

# Recap



1. Phone number recycling leads to many types of security and privacy risks
2. Most available phone numbers we sampled were recycled and also vulnerable
3. Attackers do not need special skills to exploit vulnerabilities
4. There are steps we can take to mitigate the harms

# Questions, provocations, activity



- Who do you think are the specific adversaries in number recycling attacks? How can we protect against them?
- (To industry security experts) Does this convince you that SMS-based authentication is even more dangerous now? What are you planning to do about it?



# Thank you!

Full findings, recommendations, carrier/website  
responses: *[recyclednumbers.cs.princeton.edu](https://recyclednumbers.cs.princeton.edu)*

*Email: [kvnl@cs.princeton.edu](mailto:kvnl@cs.princeton.edu)*