# The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling

Allison McDonald
amcdon@umich.edu
University of Michigan
Ann Arbor, MI, USA

Carlo Sugatan
sugatanc@umich.edu
University of Michigan
Ann Arbor, MI, USA

Tamy Guberek
tamyg@umich.edu
University of Michigan
Ann Arbor, MI, USA

Florian Schaub
fschaub@umich.edu
University of Michigan
Ann Arbor, MI, USA

## ABSTRACT

Phone numbers are intimately connected to our digital lives. People are increasingly required to disclose their phone number in digital spaces, both commercial and personal. While convenient for companies, the pervasive use of phone numbers as user identifiers also poses privacy, security, and access risks for individuals. In order to understand these risks, we present findings from a qualitative online elicitation study with 195 participants about their negative experiences with phone numbers, the consequences they faced, and how those consequences impacted their behavior. Our participants frequently reported experiencing phone number recycling, unwanted exposure, and temporary loss of access to a phone number. Resulting consequences they faced included harassment, account access problems, and privacy invasions. Based on our findings, we discuss service providers' faulty assumptions in the use of phone numbers as user identifiers, problems arising from phone number recycling, and provide design and public policy recommendations for mitigating these issues with phone numbers.

## CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → *User studies*; • **Social and professional topics** → *Computing / technology policy*.

## KEYWORDS

Privacy, security, phone numbers, user identification, phone number recycling.

**ACM Reference Format:**
Allison McDonald, Carlo Sugatan, Tamy Guberek, and Florian Schaub. 2021. The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3411764.3445085


*CHI '21, May 8–13, 2021, Yokohama, Japan*

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445085

## 1 INTRODUCTION

"It took only an hour for my cellphone number to expose my life," wrote Brian X. Chen in *The New York Times* in August 2019 [14]. As a consumer technology writer, Chen had asked a security researcher to expose as much information about him as possible using only his phone number. Right away, the researcher obtained his home address, the full names of his immediate family members, phone numbers he had previously owned, his property tax records, and his (lack of) criminal history. Although the researcher did not use this information for any nefarious purposes, he noted that if he had wanted to, he had a good chance of getting into Chen's personal accounts, scamming his family out of money, or even taking over his phone number.

Although in this case no real harm was done, Chen's article highlights just how much information is available about us online and often connected to us by one key piece of information — our phone number. While a phone number used to serve as an intentionally public piece of information listed in community phone books for the convenience of one's friends and neighbors, these numbers now serve a far broader purpose. A phone number can reveal a significant amount about a person. In the hands of a company that relies on advertising, a user can have their online identity tracked, sold, and potentially exposed through data breaches or bad privacy practices [72]. In the hands of an individual, a phone number could reveal a person's physical location, their private online accounts, and provide direct, intimate access to them [17].

At the same time, it is becoming increasingly difficult to participate online without giving out one's phone number. Phone numbers are commonly required to create accounts for online services and mobile apps, and have become a default way for services and companies to identify their users [55]. Searching or uploading phone numbers from an address book is a common way to find acquaintances on social media platforms and in messaging applications, requiring users to share phone numbers to connect on platforms that do not otherwise need them.

Furthermore, phone numbers may be far less persistent than they ought to be for the many purposes they now serve. Unlike other numeric identifiers, such as a social security number, it is very

likely that someone else will be assigned a person's phone number when they 'stop' using it. In 2018, the Federal Communications Commission (FCC) reported that approximately 35 million phone numbers are recycled in that way each year in the United States [27]. This reuse carries a huge potential risk: the accumulation of multi-factor authentication (MFA) codes, bank alerts, personal messages from friends, doctor's appointment reminders, and job offers [20, 29] can sum up to a potentially vast amount of information about a person, potentially giving the new owner access to accounts associated with the phone number and sensitive information about the previous owner.

In this paper, we broadly characterize the issues faced by individuals related to using phone numbers, and in particular highlight the consequences of phone number recycling and phone numbers being used as identifiers by online services and mobile applications. Companies rely on phone numbers as convenient identifiers for their users, assuming that a phone number uniquely identifies a single person, persistently over time, and that users are comfortable and able to share their phone number with the company and with other users through an app or service. As we show, these assumptions lead to a host of potential privacy, security, and access problems for individuals. Exacerbating these issue and creating further problems are the ways that phone numbers change hands through number recycling, creating inconvenience for new owners of a number and exposing personal information about the previous owner.

We conducted a qualitative study with 195 participants, using an online survey with open-response prompts to elicit participants' negative experiences with phone numbers and the consequences they faced due to how their phone numbers were used. Our participants frequently reported issues caused by phone number recycling, unwanted exposure, and temporary or permanent loss of access to their phone number. The personal consequences of reported phone number issues included harassment, account access problems, and privacy concerns. Based on these findings, we discuss how the assumptions companies make about the utility of phone numbers as identifiers can be faulty and can lead to these issues, and explore design and public policy directions to mitigate risks with phone numbers.

## 2 BACKGROUND & RELATED WORK

We discuss work related to the identification and authentication of users and general issues related to phone use and phone numbers.

### 2.1 User Identification and Authentication

Digital identity and user authentication have been long-standing security and privacy challenges, as well as issues in economic, social and political contexts [9, 37, 63]. Traditionally, identity systems have been physical, e.g., a passport or identity card. The emergence of digital technology has introduced novel forms of identity and authentication including biometrics, passwords, and phone numbers [37, 74]. With the increased shift to digital interactions, companies and services have needed to establish ways that customers can identify and authenticate themselves online.

Most commonly, online accounts are connected to a person's username (sometimes an email or phone number, sometimes an alias) in conjunction with a password. The username serves to identify the user and the password proves ownership of the person accessing it. Passwords, however, are notoriously challenging for users to use effectively [28] and are susceptible to account hijacking and data breaches [30, 47, 64, 75]. While password creation policies and password meters have improved the strengths of passwords, users still practice unsafe password behaviors [44, 71], such as password composition being influenced by the online service's context [53]. Moreover, passwords tend to be shorter and weaker when created on mobile devices [52].

As an inexpensive alternative to passwords, many companies and services have begun using control over a phone number as a way to prove ownership of an account, especially in the mobile ecosystem [33, 56]. This allows users to log in without needing to remember a password; an application, for example, might send a one-time code to the phone via SMS, which is then entered into the application to prove control of the phone number. However, as has been shown with email [60], an authentication message that is sent to the wrong person due to mistyped or recycled phone numbers can create account security risks.

Access to a particular phone number may also be used for account security. Multi-factor authentication (MFA) is a means to mitigate some risks associated with passwords without completely replacing them. MFA often takes the form of a password and a mobile phone, where the possession of a mobile phone is proven through SMS time-based one-time passwords [45, 62] or an app-based authentication code.

Recent work has shown that SMS-based MFA can be relatively effective in protecting online accounts, but performs worse than other second factors against account compromise. Doerfler et al. found that SMS-based login challenges prevented 96% of phishing attacks and 76% of targeted attacks [19]. Due to hijacking risks with SMS-based MFA [65] and the availability of more effective second factors, the use of SMS as a second factor has been discouraged by the National Institute of Standards and Technology (NIST) in favor of hardware and software token generators [35].

In addition to a rise in the use of phone numbers for MFA and account authentication, the prevalence of mobile technology has shifted how users interact with and store their data online [13]. This means that phones and phone numbers provide a high value target. For example, SIM-swapping attacks, in which a person convinces a mobile phone provider to switch someone else's number to a SIM card they control [6], have increased in recent years and can have significant financial consequences when used to access banking and digital currency accounts [57].

### 2.2 Common Uses of Phone Numbers

Online services and mobile applications increasingly request or require users to provide their phone number for a variety of reasons. Privacy implications of targeted advertising with phone numbers have been studied, for example, showing that phone numbers shared for MFA are also sometimes used for targeted advertising [70, 72]. However, other uses of phone numbers are also common and respective privacy and security implications have not yet received sufficient scrutiny. In order to investigate the privacy, security, and access risks associated with phone numbers, we

identify five common uses of phone numbers by companies, each with varying levels of usefulness to users and benefit to companies.

**Phone Number for Notifications.** Online services and applications may use a phone number to send SMS alerts and notifications to users. Such alerts might be sent by online services or by businesses a person interacts with in the physical world (e.g., a doctor's office, apartment complexes, stores). For example, a pharmacy might offer to send customers an SMS when their prescription is ready [18], or airlines might alert a customer when their flight is delayed [4]. While such communication is often opt-in, SMS notifications can create a potentially sensitive leak of information. As with email [60], if these alerts were to go to the wrong person, for example after a number has been recycled, they could reveal a significant amount of personal information about the intended recipient and the intended recipient may miss important information.

**Phone Number as an Identifier.** Phone numbers are increasingly used as a way to identify and authenticate users in place of a username or email address. For example, loyalty programs frequently use phone number or email address to track purchases and rewards [46]. For some services, such as Twitter, users can opt to use a phone number rather than an email address to create an account [69]. In these cases, the user will typically need to verify that they own the phone number by receiving a phone call or SMS with a one-time code that they enter into the application or website. As noted above, the phone number may also be used in place of a password as the sole mechanism for proving ownership of an account.

Phone numbers are also valuable identifiers for companies wishing to perform targeted advertising or to connect profiling data across devices and sources. On platforms like Facebook, companies can upload lists of phone numbers in order to directly target those individuals with ads [22]. The common use of phone numbers across platforms means that companies may have a better chance of connecting and aggregating data from the same individual across multiple platforms and online spaces, compared to usernames which may or may not be consistently used. Much of this phone number use is done outside of the view of the user and therefore, such violations to privacy will be difficult for people to recognize. This use of phone numbers arguably offers little or no benefit to the affected users, but is profitable for companies.

**Phone Numbers to Build Peer Networks.** Phone numbers may also be used as a way to construct peer networks. For example, many mobile messengers like WhatsApp, Telegram, and Signal use phone numbers in place of usernames [66, 68, 73], which allows users to find each other on the platform if they know each others' phone numbers. This takes advantage of many people already having phone numbers of their friends, family, and colleagues saved in their phone's contacts, allowing a new app to construct a possible network of acquaintances by requesting access to the phone's contacts. For example, Facebook's People You May Know feature uses a user's phone number and uploaded contacts to suggest which other Facebook users to connect with [26]. This can be beneficial both for users, who can easily find other people on platforms, and for companies, who can profit from learning social networks. However, when companies *require* a phone number from all users and use it in this way, private personal connections can be unintentionally shared with a company — not only by the user, but by anyone who has their phone number stored in their contact list.

**Phone Numbers for Account Security.** Services may also ask users for their phone number to enhance account security. MFA can provide an extra layer of security to an account by preventing an attacker from logging into an account with a stolen or guessed password alone. While these one-time codes can be generated by a hardware token or sent via an app or email address, SMS remains a common medium for sending MFA codes to users, and is sometimes the only way for users to enable MFA.

Similarly, phone numbers are often used for account recovery [24, 32]. If a user has forgotten their password or lost access to an email address, access to the phone number that is associated with the account might be used as an indication that they are the rightful user of that account.

**Phone Numbers as a Test of Uniqueness.** A phone number is also sometimes used to prevent the same user from creating multiple accounts, or to limit the number of accounts per person. This mechanism relies on the assumption that having numerous phone numbers will be challenging for most users, as they may be expensive. Furthermore, in contrast to email addresses, which could be anonymous and which a user could have an unlimited number of, phone numbers are often connected to a person's legal identity. This restriction may also function as an accountability mechanism. If someone is banned from a platform, the need to obtain a different phone number might hamper their ability to rejoin the community under a different alias. For example, Facebook does not allow users to have multiple or fake identities on the platform, because they "believe that people are more accountable for their statements and actions when they use their authentic identities" [23]. Although Facebook enforces this policy using more information than phone numbers alone, they also prevent multiple accounts from using the same phone number [25].

Requiring a phone number to be associated with an account may also be used to reduce spam. For example, when creating a new account, Google asks the new user to "prove you're not a robot" by verifying their phone number via a text message or a call to their phone [34]. Google, like Facebook, also seems to limit the number of accounts per phone number [16, 42]. This restriction can benefit both users and the company, but when people are limited to only one account it may create barriers for people who have a legitimate need for multiple separate accounts, for example for professional and personal use or to represent different aspects of their identity.

## 3 STUDY DESIGN

While phone numbers are collected and used in various ways, the potential negative consequences of these uses on people have not yet been studied systematically. In order to uncover the range of problems that people experience with phone numbers, including those that may be uncommon, we sought to elicit negative experiences with phone numbers from a large number of people. In this study, we do not seek to answer which problems are the most or least common, nor to measure how prevalent various problems are. Our objective is to qualitatively identify the different ways in which phone numbers and their uses create risk for people, what those

risks are, and the consequences of those risks on people who have experienced them.

To meet these goals, we designed a concise, open-ended elicitation survey that we distributed widely. Using a survey as our elicitation instrument allowed us to ask a large number of people about their experiences, increasing our chance of hearing about issues that occur rarely and giving us a broader overview of problems than a smaller-scale interview study would have.

## 3.1 Experience Prompts

The survey consisted of four parts. The survey questions are provided in Appendix A.

**Device and phone number ownership.** We asked participants to indicate the type of their primary phone number (mobile, landline, or virtual), whether the number is theirs or shared with others, how often they have changed their phone number in the last 5 years, and how long they have had their primary phone number. Note that we did not ask for the actual phone number for privacy reasons.

**Annoying, weird, or disturbing experiences.** We next asked participants to describe any "annoying, weird, or disturbing experiences with phone numbers" in order to elicit whatever experiences were most salient to participants. This question was meant to ask for participants' experiences surrounding their phone numbers without priming them about a specific type of issue. We did not further define or clarify these words in order to elicit any associations participants might have with phone numbers. We also asked about any consequences resulting from their experiences.

**Specific experiences.** Next, we asked whether they had experienced several specific issues, including inability to use an online service or app; losing access to a phone number; phone number recycling; discomfort with sharing their phone number; and any other negative experiences they would like to share. Again, we also asked for consequences from the experiences described. We asked about these specific experiences because we anticipated, based on the common phone number uses listed in Section 2.2, that they would frequently be events that led to negative consequences for individuals.

**Demographics.** Lastly, we collected participants' country of residence, age, gender, highest level of education, and employment status. Responses to these questions were optional.

We iteratively refined the survey order and content through pilot testing. We translated the survey into Spanish to expand the responses for international experiences. Our study went through the IRB approval process and was exempt.

*3.1.1 Recruitment.* To collect responses from a wide and diverse group of people, we shared the survey across multiple social media sites such as Facebook, Twitter, and Reddit between March and June 2019. In addition, the survey was shared to personal and professional networks and email lists at multiple universities. We further distributed the Spanish version within the local immigrant community and to personal networks in South America. The survey did not collect any identifying information such as phone numbers and all participants remained anonymous.

**Table 1: Participant demographics (n=195).**

| | | |
|---|---|---|
| Age | 18-24 | 34 |
| | 25-34 | 89 |
| | 35-44 | 43 |
| | 45-54 | 9 |
| | 55-64 | 7 |
| | 65 or older | 5 |
| | Prefer not to answer | 8 |
| Education | High school graduate | 3 |
| | Some college but no degree | 9 |
| | Associate degree | 1 |
| | Bachelor's degree | 51 |
| | Graduate degree | 116 |
| | Professional degree | 5 |
| | Prefer not to answer | 10 |
| Employment | Employed full-time | 102 |
| | Employed part-time | 11 |
| | Student | 59 |
| | Self-employed | 2 |
| | Homemaker | 1 |
| | Retired | 3 |
| | Not working | 6 |
| | Prefer not to answer | 11 |

Participants could optionally enter into a raffle to win one of five $20 Amazon Gift Cards. Contact information for the raffle was stored separately from survey responses.

*3.1.2 Demographics.* We received 191 English and four Spanish responses. All Spanish responses were translated by the authors into English prior to analysis. Most of our participants lived in the United States with eight from Germany, and one each living in the Netherlands, Ireland, Guatemala, France, Colombia, Canada, and Australia. Participant demographics are summarized in Table 1.

*3.1.3 Qualitative Analysis.* After discarding empty responses, we used iterative, open coding followed by thematic analysis of the 972 open-text responses we received (7 open-response questions from 195 participants, some left blank). In line with the process described by Braun and Clarke [11], two researchers initially read the data and derived codes using participant language (e.g., "I don't care", "annoyed") and descriptive terms based on the event described ("account lockout", "changed number"). Codebooks were initially generated for each question, but we quickly observed heavy overlap across topics and combined them into one codebook (e.g., the question about phone number recycling contained descriptions of many of the other experiences we asked about). After an initial codeset was generated from these readings, two researchers discussed and merged overlapping codes, grouped similar codes into higher-level themes (e.g., "made up phone number" and "used old number" merged to "gave fake phone number"). We then tested the utility of the codebook on a subset of the data, adding new codes and merging further overlapping codes, with discussion, until no further changes were necessary, which required two rounds. The final codebook of 45 codes was applied to a subset of 15 responses with good inter-coder agreement (Cohen's $\kappa$=.76) [51], after which

all responses were recoded. The codes represent themes we describe in the paper and closely align with the summary in Table 2.

Throughout the paper, we quote our participants' text responses. We removed or changed any identifying information (e.g., names), but we do not modify company names so as not to obscure the context of a described negative experience.

## 3.2 Limitations

Our goal with a qualitative elicitation study was to provide insight on the range of problems that people experience with phone numbers. Some of the experiences and consequences we discuss are difficult to capture. For example, interpersonal issues like harassment and stalking are among the most serious consequences of phone number exposure, but relatively few users might experience the worst forms of these harms or, even if they do, may not be willing to share such experiences.

Our sample is more highly educated than the general population, likely due to our recruitment method. This may mean that our participants, with more earning potential, are less likely to face issues that arise from prepaid phone numbers or inability to pay a phone bill. While six participants reported losing a phone number for financial reasons, research focusing on lower-income contexts might reveal additional nuanced consequences of this problem [49], in addition to the rich insights we report here.

While we do report the country of residence of participants, we did not ask our participants to specify where their experience took place. Some of the stories from U.S.-based participants happened internationally. Therefore, we do not make statements about phone issues in specific countries nor draw cross-cultural comparisons, but we also do not exclude any responses based on participant location. We did confirm that all themes reported by our non-U.S. participants were also reflected in similar U.S. experiences. In other words, none of our findings were based solely on non-U.S. responses.

# 4 RESULTS

In general, most of our participants reported having minor issues with phone numbers that frustrate and inconvenience them; however, some shared experiences that created significant risk and had severe repercussions in their lives, demonstrating that collection and use of phone numbers can have real consequences on people. Our findings are summarized in Table 2.

While our sample does not allow us to comment on the frequency of problems in the general population, we indicate the prevalence of each problem among our participants.

## 4.1 Participants' Phone Number Use

When asked what type of phone numbers participants have had in the last five years, 191 of 195 participants indicated that they have a mobile phone number; 85 have a virtual number such as Google Voice or Skype number and 51 have a landline. 108 reported having two or more types of phone numbers. Only one respondent indicated that they share their mobile device with someone else (their spouse).

Almost half of our participants (91) have gotten a new phone number in the last five years, suggesting that phone numbers are less persistent than one might expect. 48 participants obtained a new number once in that time; 41 obtained new numbers 2–5 times. Most other participants (88) reported having their primary phone number for 10 or more years.

## 4.2 Negative Experiences

Broadly, we identified six types of negative experiences with phone numbers as reported by participants. The frequency of these problems, as well as the consequences, varied widely. For example, some experiences, such as problems with spam, were reported by nearly all participants but resulted largely in minor inconvenience, while other issues like harassment and concern about personal safety were mentioned less but had a significant impact on the respondent's life. We first present the types of negative experiences and then discuss resulting consequences and behavioral responses.

*4.2.1 Losing access to a phone number.* 16 participants reported losing access to their phone number either temporarily or permanently. The most common reason was international travel or moving to another country. 14 participants reported having issues accessing a phone number or verifying an account while traveling or living internationally. This resulted in being locked out of financial applications, being unable to use their accounts, or needing to borrow family members' devices. P60 described, *"I lost my Chinese phone number [because] I forgot to pay my bill for several months. And it's very hard for me to get that back again... [T]o get the number back they require me to go to a service provider store in-person with my ID... so annoying... and this number is connected with many of my account[s] like my Alipay or WeChat. It's possible that this number would be registered by someone else if I don't get it back in a short time. I just don't know what to do in that case."*

For some users the lockout is not just temporary; accounts are permanently lost because users no longer have access to the phone number they used to register an account. P163 explained, *"My @126 email was linked to my old Chinese phone number which I cancelled. Now the first step to update that phone number is to receive a text validation code on that number on file. Which of course is impossible. Otherwise I need to go through a process to [prove] that I'm the owner with my ID or passport, which I feel is so unnecessary for an email. So I never updated that number."*

Several participants (6) reported losing access to a phone number because they were unable to pay the phone bill. Others had disputes with the service providers or changed numbers and were later unable to regain access to the old number when they needed to. Retrieving a phone number after it has been assigned to someone else is difficult, if not impossible. P20 described realizing that a deceased relative's phone number was the only method available to certain people for reaching their family after the number had already been recycled. When they could not retrieve it, they lost contact with those people.

Loss of access could also stem from an adversary. P194 described being the victim of a SIM-swapping attack: *"Someone went into a Verizon store in another city, showed a fake ID saying that they were my son, told the agent that they had lost their cell phone, and asked to have my son's cell phone number transferred to an old phone that they had brought into the store. We were lucky that my son noticed that his phone got a message that it was no longer 'authenticated' and that I knew what that might mean."* This participant was able

**Table 2: Summary of findings, with number of participants expressing each theme.**

| Negative experiences | # | |
|---|---|---|
| Loss of access to phone number | 14 | Loss due to international travel or move |
| | 6 | Loss due to unpaid mobile bill |
| | 1 | Loss due to SIM-swap attack |
| Phone number recycling | 67 | Must deal with the former owner's calls or text messages |
| | 5 | Harassed (e.g., by debt collectors) |
| | 4 | Gained personal information about the previous owner |
| | 4 | Contacted the wrong person when friend or family changed phone numbers |
| | 3 | Asked to relay messages to previous phone number owner |
| | 3 | Unable to use recycled number to register a new account |
| | 1 | Had personal information exposed to new owner of their old phone number |
| Companies sell or misuse data | 140 | Received spam (unwanted calls) |
| | 23 | Assumed companies collecting phone number would lead to spam |
| | 19 | Assumed companies would sell phone number |
| Interpersonal sharing | 3 | Feared dating websites would expose phone number |
| | 1 | Number exposed to someone through an app |
| | 1 | Phone number led to being found on another platform |
| Usability of phone numbers | 3 | Phone numbers are hard to remember |
| | 2 | International prefixes are confusing |
| | 2 | Changing phone numbers is burdensome |
| | 1 | Phone number looks like spam number to friends and family |
| Consequences | | |
| Degraded utility | 20 | Wasted time |
| | 18 | Inconvenience |
| Erosion of trust in companies | 21 | Mistrust in companies asking for phone numbers |
| Emotional toll | 80 | Annoyed (e.g., at dealing with spam or other inconveniences) |
| | 5 | Felt physically unsafe |
| | 1 | Experienced significant panic and anxiety |
| Financial Loss | 2 | Needed to pay to change number |
| | 1 | Fell for financial scam |
| | 1 | Lost financial opportunity due to wasted time |
| Behavior changes | | |
| Changing answering behavior | 46 | Stopped answering the phone or began ignoring unknown numbers |
| Correcting mistaken callers | 17 | Answered unknown numbers to tell caller the number was recycled |
| Sharing virtual or fake numbers | 14 | Gave companies or people fake numbers instead of real phone number |
| Blocking numbers | 18 | Routinely block numbers |
| | 12 | Use a call-blocking service |
| | 2 | Search unknown numbers online |
| | 1 | Report spam callers |
| Changing phone numbers | 7 | Changed phone number due to negative experience |
| Self-restricting behavior | 22 | Opted out of a service to avoid giving a phone number |
| | 3 | Used alternative service instead of sharing a phone number |
| Resignation | 21 | Shared a phone number when they did not want to |
| | 10 | Felt they had no choice but to share a phone number |

to quickly regain control of the phone number and was able to stop the attack before any financial harm had occurred.

*4.2.2 Phone number recycling.* Many participants (72) have had negative experiences related to phone number recycling. Most commonly, they reported receiving a number that had been recycled and having to deal with receiving calls and messages intended for the number's previous owner (67). Others reported contacting the wrong person after a friend or family member changed their number (4). One person had their number reassigned to someone else.

For some participants, getting someone else's recycled number was simply an inconvenience. P170 wrote, *"[T]he last person who had [my] phone number didn't tell the majority of her contacts that she had switched phone numbers. ...the first couple years with my 'new' number were littered with random people texting/calling asking for her. This was funny at first and I even managed to pull a few pranks. But it became increasingly annoying as time went on. It has been 5 years with this number and I *still* get texts for her every once in a while."* Three participants even reported being contacted by the previous owner and asked to relay messages to them.

For others, dealing with someone else's number could be scary when the people calling for the previous owner did not believe it had been reassigned. Several participants (5) reported being harassed by debt collectors. Others experienced more personal attacks. P80 reported, *"I started receiving weekly collect calls from [a] Prison. Apparently the inmate's wife, ex-wife, girlfriend, or ex-girlfriend used to have my phone number. Even though there was an operator between us... I'd decline, yet I could hear the guy on the other end start screaming at me about stealing his woman, and threatening to hunt me down once he was out."*

Some participants even reported gaining access to the former owner's personal information when they received their new number. Four participants reported getting SMS notifications from businesses like banks and laundry services, or receiving birthday wishes from friends of the former owner. For each participant, this added up to a significant amount of information about their number's previous owner. In addition to the personal information, P105 reported having a "creepy" interaction with someone trying to contact the former owner: *"[T]he previous owner seemed does not change his contact info for bank services... I got messages regarding his bank transactions, had access to his [WhatsApp] account, received a dozen of phone calls from his friends looking for him, yet the most weird thing happened at one night—I was sleeping and hearing my phone ringing. it was a FaceTime call from an unknown Chinese number. ... I answered—there was a female's arm holding a baby and asked the baby to call daddy in a soft voice... it was midnight and that's just so creepy to me and I hung up the phone. She called several times afterwards and the following days. ... wonder what happened to [the former owner] as he seemed being away without notifying others about the change of his number."*

Conversely, one participant reported what happened to them when someone else was assigned their former phone number. P154 described discovering that their WhatsApp contacts had been talking to the wrong person after they had changed phone numbers. While only one person reported having their own information revealed by phone number recycling, several others expressed worry about what would be exposed about them if they eventually lost their phone number.

Phone number recycling can hinder access as well. Three participants reported being unable to create a new account with a company or sign up for rewards programs because the previous owner of the number had already created an account and had not yet changed the number. P24 shared, *"[I have] Maggie's phone number. I got her email address from groupme, can't open an uber account because the number is taken, have her birthday date because I got a happy birthday, got added to a whatsapp group..."*

*4.2.3 Companies selling and misusing contact information.* A large number of participants (74) described an experience in which they were uncomfortable sharing their phone number with a company or a person. For those who worry about sharing with a company, many of their concerns related directly to how companies used their phone numbers or how the participants expected their numbers would be used. The most frequently cited reason for discomfort was that participants assumed that companies would sell their phone number if they shared it with the company (19).

Even more participants (23) believed that sharing their phone number with too many companies would increase the amount of spam they receive. Sometimes a specific experience led them to this belief. For example, P191 described that they *"signed up for health care portal (obama care) to choose new health insurance. was bombarded with phone calls within minutes, for weeks and months to follow. still getting calls today, 2 years since."*

The concern about spam was significant. A majority of participants (140) complained about spam calls, such as calls from telemarketers, robocalls, or persistent unwanted calls of unknown providence. Of these respondents, nearly all brought up spam calls in the first question, which asked broadly about their experiences with phone numbers. This suggests that spam calls are a prominent issue in people's minds.

*4.2.4 Distressing interpersonal disclosure.* Potential interpersonal risks were another source of discomfort for some of our participants. Three participants said they dislike sharing their phone number with dating websites because they worry that the platform will expose their number to the people they connect with. P40 shared, *"[W]hen I have to use my number to log into dating apps, I worry that the app might give my number out to the other people on the app."*

Another participant (P157) described needing to share their phone number with a Grubhub delivery driver for their food order, but felt uncomfortable when the delivery driver *"tried to get personal."* In this case, the phone number had already been shared and the driver now had a direct line of access to the person they made uncomfortable.

Phone numbers, once shared, can open new avenues of contact that simple blocking cannot prevent because of the way that numbers are used across services. P97 described, *"There was also a time when some people were harassing me via text and then used my number to continue harassing me on WhatsApp with further information indicating that they'd doxxed me as well."* When phone numbers are used as identifiers across many platforms, they can help an attacker find alternative channels to harass or contact someone who has blocked them elsewhere.

*4.2.5 Poor usability of phone numbers.* Beyond negative experiences stemming from phone number use, several participants also complained about needing to use phone numbers at all. Three participants mentioned that phone numbers are hard to remember, two complained that international prefixes are confusing and difficult to use, and one reported being regularly ignored by friends and family because their area code begins with an "8" — leading their contacts to assume a telemarketer is calling. Several participants (2) also complained that updating all the services that have their phone number is burdensome if they want to get a new number, but that porting an old number to a new provider is also difficult.

## 4.3 Reported Consequences

The consequences that followed from the reported negative experiences with phone numbers varied in type and severity, ranging from annoyance and disruption to participants' lives, emotional ramifications like stress and fear, and even financial consequences. In total, these consequences demonstrate the real and sometimes significant impact problems like phone number recycling and phone numbers as user identifiers can have on people's lives.

*4.3.1 Inconvenience and degraded utility of phones.* Throughout our participants' experiences, many expressed their frustration at wasted time (20) and feeling inconvenienced (18) from dealing with their issues related to phone numbers. These feelings were most frequently associated with dealing with many spam calls or needing to answer calls for the former owner of their phone number.

When participants are locked out of accounts they had previously created because they cannot access their number, or are prevented from making new accounts with a recycled phone number, the convenience of using a phone number as an identifier is lost.

*4.3.2 Erosion of trust in companies.* Multiple participants (21) expressed a lack of trust towards companies or services who ask them to provide a phone number. Most frequently, participants connected this discomfort with a lack of understanding of why a company would ask them for this information. P187 wrote, *"I'm always uncomfortable sharing my phone number for no obvious reason (like why does Bath and Body Works care what my phone number is?) ...Unfortunately, I don't know what else to do, so I just bite the bullet and type in my phone number."*

Many other participants felt certain that companies would sell their phone number to other entities (19) and that sharing their number would result in more spam (23), and therefore did not want to provide their number. Unfortunately, as P187 expressed above, many felt they had no choice but to share their phone number. Many (21) described a specific situation in which they did not want to share their number, but did it because they had to. P121 described this frustrating trade-off: *"Telegram requires your telephone number as a user identifier. I was resistant at first, but eventually gave in. I don't like that this service has my number, but without the service, I would be unable to use it to speak with friends."*

*4.3.3 Emotional toll.* Many of our participants (71) expressed some emotional reaction to the experience they shared. The emotional reactions of our participants to their experiences varied from mild (e.g., annoyance) to extreme (e.g., fear).

Most commonly, participants expressed feeling annoyed about unwanted phone calls and text messages. But participants also shared harmful impacts and issues in their lives such as harassment and interpersonal problems.

Five participants shared experiences that made them feel physically unsafe. P158 described, *"One time several years ago, a man called my number in the middle of the night asking to speak to someone who was not me. I told him he had the wrong number. He called back and told me I sounded 'sexy,' that I should send him a nude photo, and that he knew where to find me. I told him I would call the police if he called back and I hung up the phone. He called back immediately but I did not answer and blocked the number."* P97 described being harassed and doxxed via SMS and then WhatsApp (see Section 4.2.4), which led to *"a metric [ton] of stress/anxiety"* and the decision to change residences.

While no participants specifically described physical harm being caused by these incidents, it is clear that the potential for such harm was present. Furthermore, the consequences of harassment itself can be long-term. For example, P196 described experiencing significant harassment over the phone that resulted in panic attacks whenever the phone rings, which was made worse by the increase in spam they began to receive. While cases of this severity may not be frequent, their existence demonstrates that significant emotional toll can be the price individuals pay for not having control over their phone number.

*4.3.4 Financial loss.* A few participants also described the financial cost of their experiences. P186 paid several thousand dollars for fraudulent car insurance as a result of a scam caller. Two participants described needing to pay fees to change phone numbers. P49 explained that they lose job opportunities and time (and consequently, money) every time they need to answer a spam phone call.

## 4.4 Behavioral Changes

Some participants found ways to cope or change their behavior in order to avoid the problems identified above. We found that many of these coping strategies in turn led to frustration or inconvenience for participants.

*4.4.1 Changing call answering behavior.* The most common way that people responded to unwanted calls was changing whether and how they answer the phone (46). This ranged from only answering calls from people they know to not answering at all and only relying on voice messages or text messages. Many participants speculate that in doing so, they have missed job opportunities, business calls, and medical appointments. P49 wrote, *"I have missed important phone calls and messages from potential jobs, and it's gotten so extensive I've contemplated paying the 40 dollar fee to change my phone number."* Similarly, P91 wrote, *"I don't pick up the phone for any phone number that's not in my contacts list anymore. If they want to get in touch with me, they can leave a message or email me."* Others simply silence their phone for all calls.

These strategies suggest that to cope with spam and unwanted calling, users are forced to adopt behaviors that undermine the original purpose of having a mobile phone.

*4.4.2 Correcting mistaken callers.* One laborious way in which people approached phone number recycling is correcting callers who are looking for the previous owner. 17 participants reported answering calls in order to tell others that they had reached the wrong person. While some had no trouble communicating the mistake to the person on the line, others expressed that this caused problems with the caller. P115 recalled, *"Yeah, one time someone called me when I lived in Oregon and asked to talk to someone who wasn't me. I said wrong number. She called back and then got annoyed at me, thinking I was playing a trick on her when I again said wrong number."* This echoes Rader and Munasinghe's findings on how people respond to and correct senders of manage misdirected email [60].

Two participants changed their voicemail message to clarify who they were to wrong number callers so that they would not have to pick up their phones anymore. According to our participants, correcting callers constantly constituted a waste of time and decreased the value of using a mobile phone. While some decided to completely stop answering their phones, others have to deal with correcting callers just to not miss a specific opportunity through phone calls.

*4.4.3 Sharing virtual or fake numbers instead.* When participants felt uncomfortable sharing their phone number, some ended up giving a fake phone number (4) or a virtual number (10) instead. P144 mentioned that the reason they don't worry about phone number sharing is that they are not afraid of giving out their Google Voice number. However, several participants mentioned that Google Voice numbers only work in certain apps or services. P168 described their strategy for using a fake number: *"In general, if I have to use a phone number for something, I have a regular 'fake' phone number I use that was a PAGER number I had when I was in college. I recognize that it could be recycled to other people, but I don't care. Everybody wants your phone number for marketing purposes and people who claim they don't give your number to anyone could be telling the truth since they SELL your number to other people...."* Participants are aware of the implications of sharing their phone numbers and look for ways to mitigate these issues through obfuscation, or adding fake information into a system meant to track them, thus disrupting the efficacy of the system [12]. However, in cases where the number needs to be usable, this will not work. Strategies such as changing phone numbers or using virtual numbers can also be costly and are not always available to everyone.

*4.4.4 Blocking numbers or using call blocking services.* 18 participants described blocking numbers directly and 12 used some type of call blocking service, such as opting into the FTC's Do Not Call registry [15] or using call blocking apps like Mr. Number [39]. However, many of the participants who use these services claimed that this strategy is futile. P30 wrote, *"My efforts to block them don't work because they end up changing the number."* P119 wrote, *"My number is on the Do Not Call List, but it doesn't seem to matter. Recently I've been getting 2-3 per day".*

Two participants said they research any unfamiliar phone numbers (P18, P110), while P92 actively reports phone numbers (though they did not specify to whom).

*4.4.5 Changing phone numbers.* Only seven participants reported changing their numbers due to their negative experiences. P102 explained how their child had received a phone number that was formerly used by a drug dealer and sought to change the number. They complained that the service provider insisted on charging them to change the number, but eventually provided a new number for free. P49, despite receiving many spam calls, contemplated paying to change the number but had not done so. Specifically, four participants were concerned with the costs of changing numbers, with one participant claiming it would cost them $40 to change their phone number. Moreover, as phone numbers are increasingly used as identifiers for accounts, the time required to update all of one's accounts and services with a new phone number can be burdensome and thus be a further deterrent to changing numbers. P105 mentioned, *"I was thinking to change a phone number but then I need to update a lot info that associated with this phone number, it's kind of troublesome so I haven't changed it yet."*

*4.4.6 Self-restricting behavior.* 22 participants opted not to use a particular service or app because they either could not provide a valid phone number or felt too uncomfortable to share their phone number. Only three participants described being able to find an alternative service. P59 reflected, *"More than once I've been asked to provide a phone number before proceeding. In some cases this is jawboning, trying to make me provide my phone number, but caving when I refuse. In other cases, I can't move forward, so I don't."* P7 expressed that it is becoming more difficult to find alternative services that won't ask for a phone number. This shows that for certain services or apps, participants are being forced to choose between participating or restricting their usage just to preserve their privacy.

*4.4.7 Resignation.* While six participants expressed that they do not engage in any specific strategies to avoid these negative experiences, 21 participants reported that when prompted to share a number they didn't want to share, they surrendered and provided their phone number anyway. 10 participants felt as if they could not do anything but share their phone number if they want to receive a particular service, which reflects other work showing "digital resignation" as the inevitable result of consumer surveillance practices [21]. P95 stated, *"It is usually required for most things online, even when it seems unnecessary. I would prefer to not share this info but it seems mandatory to receive services online."*

## 5 DISCUSSION

The proliferation of phone numbers in commercial and social contexts, often with companies facilitating the exchange while collecting and processing the data, has led to significant costs to users. Our findings characterize the many problems individuals have with phone numbers, and highlight that the associated costs to them can be significant. In particular, we discuss how companies that use phone numbers as user identifiers make implicit assumptions about users that lead to some of these issues. We then discuss the implications for tech platforms and policy considerations.

### 5.1 Issues from Faulty Assumptions about Phone Numbers

As discussed in Section 2.2, the uses of phone numbers by companies can serve a wide range of purposes. However, our results

illuminate that many of the problems users face with their phone number also stem from these common uses. Here, we highlight how the use of phone numbers as identifiers by companies in particular creates challenges for individuals. Our findings show that the implicit assumptions by companies that phone numbers are *persistent* and *unique*, that a phone number is consistently *available* for authentication and account use, and that people are *comfortable* sharing their phone number with a company and possibly with other users, are flawed.

**Phone numbers might not be unique or persistent.** While many services operate assuming that a phone number will persistently belong to one user, people can and do change phone numbers; indeed, almost half of our participants had gotten a new number in the last 5 years. When people forget or are unable to update their phone number, this may result in missed notifications, login problems, account lockouts, or private information being sent to the wrong person.

Furthermore, not all users have a unique phone number or device to begin with. Although only one of our participants shares a phone number with a spouse, this is likely a larger issue internationally in places where sharing devices is more common [3]. Shared devices may cause additional problems when multiple accounts cannot be associated with the same number, or if a login can be processed through a verification code sent via SMS rather than a username and password, allowing a different user of the device to log in against the wishes of the account holder.

**Phone numbers are not always available.** Even when people are willing or required to provide their phone number, the mobile network may not be consistently available. As shown by our participants, people may be unable to pay their phone bill, may travel or move internationally, or otherwise lose access to a phone number temporarily or permanently. 14 of our participants reported issues with account access due to international travel or living, causing problems from inconvenience to complete and permanent inaccess. Potentially worse, phone number recycling means that recovery codes might be delivered to the wrong person, providing them with information that could be used to hijack an account. In either case, the use of a phone number as a way to authenticate or recover an account can create costly barriers, which may be especially frustrating in cases where the phone number itself is not necessary to provide the service.

**Sharing can give unwanted intimate access.** In the previous cases, problems arise when a number cannot reliably identify or authenticate someone over time. In other cases, a phone number *being* a persistent personal identifier — and shared inappropriately — is the issue. Phone numbers directly provide the ability to contact an individual, regardless of the context or reason the phone number was provided. As is well documented, Facebook's People You May Know (PYMK) feature has been shown to cause a number of similar issues to the ones we identify here. PYMK opportunistically suggests friends based on information Facebook collects about users, including phone numbers [26]. This can be a problem for someone who uses a phone number in multiple contexts. For example, sex workers who work under an alias to protect their identity may see clients being suggested as friends on Facebook, despite taking extra precautions otherwise to keep work and personal accounts separate [38].

Phone number use in the mobile messaging ecosystem can also be especially risky for certain users. Many mobile messengers, such as WhatsApp and Signal, display a user's phone number to everyone that person chats with. A protest group using WhatsApp to communicate not only exposes all members of the group to one another, but also to anyone who confiscates a member's device or infiltrates the group. This is exactly what happened in March 2020, when the Lebanese Government reportedly used WhatsApp groups to infiltrate the social networks of protesters and track them based on phone numbers [5, 43]. Once a phone number is in the hands of an adversarial government agency, it can be used to physically find and track the owner with a cell-site simulator, as has been done by the U.S. Immigration and Customs Enforcement to find and deport immigrants [67].

## 5.2 A Public Number Becomes Private

Phone numbers by design were meant to be shared; they were commonly available in phone books to facilitate easy contact for friends and neighbors [58]. Now, phone numbers are becoming increasingly guarded. In this way the phone number has followed a similar trajectory to the American Social Security Number (SSN). As described by historian Sarah Igo, when introduced in the 1930s, SSNs were controversial; meant to facilitate the collection, and later disbursement, of financial benefits for workers, some skeptics feared they were the beginning of a national identity system. As the system gained traction and some critical number of Americans opted in, those who were left without this number began to be locked out of job opportunities. Those who had been assigned a number might even show it off publicly, for example by having it engraved on jewelry or even tattooed onto their bodies [40].

As with phone numbers, private companies began using SSNs for their own bookkeeping, making them more valuable for more purposes. Soon this number was no longer so comfortably shared, and today SSNs are carefully guarded because they can be used for identity theft, allowing an attacker to open credit cards, access government benefits, and wreak other havoc on one's financial life [1, 41]. Similarly, we found our participants carefully guard their phone numbers, worrying about the information being sold or exposed to scammers by companies, exposing private information about them, or giving an attacker access to their online accounts.

## 5.3 Disclosing Phone Numbers Should be Optional

As we explored in Section 4.3, the cost to users of the prolific ways phone numbers are currently used is hardly negligible. To various degrees, users are facing degradation of utility, financial harms, loss of trust in companies, and emotional and safety consequences in dealing with problems stemming from the overexposure of their phone numbers. Some of these issues can be considered a problem of context collapse [50] — phone numbers shared in one context with one intention create pathways to expose information in unexpected ways and contexts.

We argue that companies should stop requiring users to connect a phone number to their account when at all possible. In many cases,

a service can be run with an email or username rather than a phone number. Users should have the option to choose their preferred identifier based on their own privacy needs. Furthermore, in any application that does collect a phone number, that number should *never* be exposed to other users unless explicitly done by the user. More generally, the way a company plans to use a phone number should be clearly communicated to users and any additional uses after the number has been provided should be strictly opt-in.

## 5.4 Phone Numbers are a Risky Authentication Method

While SMS-based authentication may be easy and cheap to deploy, the likelihood that a phone number will not persistently belong to the same person, for example because of the high rates of phone number recycling, impairs the utility of phone numbers for security purposes. After a number is reassigned, the wrong person could receive MFA or login codes, allowing them to gain access to another's accounts. As one of our participants experienced, a determined attacker might even be able to hijack a *particular* user's phone number through SIM-swapping. Only one of our participants experienced this, but a recent study by Lee et al. found that of the five U.S. mobile service providers they tested, they were able to successfully perform a SIM-swap at all five, showing that the attack is easily achievable for a minimally informed attacker [48].

These attacks, especially when targeted to specific high-value users, can have significant consequences. For example, Twitter CEO Jack Dorsey had his Twitter account taken over by an attacker who proceeded to fill his account with offensive messages, harming the CEO's and the company's reputation [10]. These attacks can have financial consequences too, and have been used to steal hundreds of thousands of dollars worth of cryptocurrency from online wallets [57]. That SIM-swapping is such a lucrative attack demonstrates that having access to someone's calls and texts can provide access to a slew of sensitive accounts. As an additional risk, the mobile networks that transmit calls and SMS messages are themselves insecure [59], enabling untrusted entities and even enterprising individuals to eavesdrop on legitimate calls and texts without compromising any individual's accounts or mobile device.

In this way, our findings bolster other recent calls to deprecate SMS-based MFA [36, 54, 65]. While phone numbers for MFA and account recovery may still be useful in supplementing other account security mechanisms, the high cost of a phone-based attack should drive companies to consider making more robust security mechanisms, such as software- or hardware-based MFA tokens [19], a priority. Companies should further encourage users to opt for non-phone number based mechanisms as the default.

## 5.5 Mitigate Effects of Phone Number Recycling

Many of the most common issues reported by participants with phone numbers being used as user identifiers arise when they change phone numbers. These issues range from being locked out of accounts, getting unwanted calls for the previous owner, and being at risk for privacy exposures.

Because unwanted calls are a significant consumer complaint, the FCC has recently taken steps to address phone number recycling. In December 2018, the FCC imposed that phone carriers must wait a minimum of 45 days before returning a previously used number into circulation — a wait that was previously mere days — and introduced plans for a centralized recycled phone number database [27]. This database would be a list of all recently released phone numbers that companies will be able to query to learn whether the phone number they're trying to contact has been released and reassigned since it was provided to them. We suggest that similar information should be made available to consumers when they receive a new phone number.

Nevertheless, with this approach phone numbers will continue to be recirculated shortly after being released and the onus is on services to use the database to protect consumers. At this point it is unclear how effective this will be at reducing unwanted calls and preventing account creation problems for people who receive a recycled phone number. Additionally, such a database certainly raises several privacy and security concerns in itself, for example by creating a list of recently relinquished phone numbers for an attacker to use to authenticate to different services.

We argue that a more decisive solution is warranted. Scarcity of phone numbers is artificial. Phone service providers and regulators should expand the space of possible phone numbers to a size that significantly reduces the chance of phone numbers being recycled, or that allows for a significantly longer decommissioning of phone numbers between users. For instance, other countries (e.g., Germany) use 4- or 5-digit area codes, whereas the U.S. uses 3-digit area codes. This may be inevitable anyway; the North American Numbering Plan Administrator (NANPA), which controls the allocation of phone numbers in most of North America, projects that the current space of 10-digit numbers will be exhausted by 2049 [2]. Given the significant problems that are already arising with phone number recycling, we recommend this change be seriously and quickly considered.

## 5.6 Enable Contextualized Use of Phone Numbers

The measures that participants can and are taking to deal with the consequences of phone number (mis)use are insufficient to solve the problems created by having their phone numbers prolifically used in online accounts and applications. Steps such as permanently silencing phones, giving out fake numbers, opting out of using wanted services, or simply resigning themselves to being exposed are all annoying and disruptive to people, and ultimately ineffective.

Although in many cases phone numbers should *not* be required for identification, in the cases where this remains necessary or convenient to users, people should be able to easily and comfortably share a number they don't worry about being connected to the wrong part of their online identity. An excellent example of this is Apple's "Hide My Email" feature, in which Apple generates a unique email address that's associated with the user's account when they use Sign-In with Apple [7], effectively hiding the user's real email from third-party services. We recommend that phone service providers and regulators work to make it possible for consumers to have multiple phone numbers associated with the same SIM card or device in a similar way. This process has started somewhat: phone manufacturers have begun releasing phones with two SIM card

slots or the capability to manage two phone numbers virtually [8, 31]. However, these specifications are designed for managing two numbers. In the ideal world, a user should be able to share a different phone number with their Uber driver than they use on a dating website, or list on LinkedIn, or use for personal communication with friends and family.

While this does not eliminate all problems, this could relieve some of the anxiety that our participants expressed over having to give out their phone number, while retaining many qualities that make phone numbers useful as account identifiers for companies. Similar to how security experts recommend people to have a different password for each online account to prevent many accounts from being compromised if one site experiences a breach [61], a different phone number for different areas of one's life may give a person more control over how and where their identities are connected online.

However, this recommendation may be ideal only in the short term; as we heard from participants, the format of a phone number is also not user-friendly. A significant increase in the number of phone numbers each person has to remember and use risks complicating online identity management rather than relieving it. Similar to efforts aimed at eliminating the need for passwords [9], future work should consider a future without phone numbers as identifiers at all in favor of more flexible, usable methods of identification.

## 6 CONCLUSION

Phone numbers are intimately connected to our online and offline lives. Our online elicitation study with 195 phone users yielded qualitative insights into the range of negative experiences connected to the way phone numbers are used. We find that people struggle with phone number recycling, loss of access to their number, and deal with privacy concerns. We also find that people experience significant harms following these issues, including harassment, account access issues, and eroded trust in companies, which lead people to adopt inconvenient and largely ineffective coping strategies. Based on our findings we discuss how faulty assumptions made by companies in their use of phone numbers as user identifiers lead to inflexible and sometimes harmful design decisions, and how companies and regulators should step in to provide better protections against privacy harms from phone number use online.

Ultimately, while individuals might be able to take small steps to protect themselves, the ability to make the best decisions for themselves is severely limited by the decisions companies are making about how to collect and use phone numbers. People use phones and their phone numbers in so many different ways — not every person will have a phone number that is uniquely theirs across space and time, that corresponds to all parts of their online identity. It is the joint responsibility of companies, regulators, and researchers to find the way forward for online account management that is safe and feasible for all people.

## ACKNOWLEDGMENTS

This research has been partially funded by the University of Michigan School of Information. Allison McDonald was supported by a Facebook Fellowship. The authors are grateful to all participants, the members of spilab for feedback on study design, and the anonymous reviewers for their helpful suggestions.

## REFERENCES

[1] The Social Security Administration. 2018. Identity Theft and Your Social Security Number. https://www.ssa.gov/pubs/EN-05-10064.pdf, accessed 2020-08-15.
[2] North American Numbering Plan Administrator. 2019. April 2019 North American Numbering Plan (NANP) Exhaust Analysis. https://nationalnanpa.com/reports/April_2020_NANP_Exhaust_Analysis%20Final.pdf, accessed 2020-09-02.
[3] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 17 (Dec. 2017), 20 pages. https://doi.org/10.1145/3134652
[4] American Airlines. no date. BeNotified. https://www.aa.com/i18n/travel-info/travel-tools/benotified.jsp, accessed 2020-08-26.
[5] Deborah Amos. 2020. Lebanon's Government Is Accused Of Swarming WhatsApp To Catch Protesters. https://www.npr.org/2020/03/09/809684634/lebanons-government-is-accused-of-swarming-whatsapp-to-catch-protesters, accessed 2020-09-01.
[6] Nathanael Andrews. 2018. "Can I get your digits?": Illegal Acquisition of wireless phone numbers for SIM-swap attacks and wireless provider liability. *Nw. J. Tech. & Intell. Prop.* 79 (2018). https://doi.org/10.13094/SMIF-2013-00004
[7] Apple. 2020. Hide My Email for Sign in with Apple. https://support.apple.com/en-us/HT210425, accessed 2020-01-08.
[8] Apple. 2020. Using Dual SIM with an eSIM. https://support.apple.com/en-us/HT209044, accessed 2020-08-03.
[9] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy*. IEEE, USA, 553–567.
[10] Russell Brandom. 2019. The frighteningly simple technique that hijacked Jack Dorsey's Twitter account. The Verge. https://www.theverge.com/2019/8/31/20841448/jack-dorsey-twitter-hacked-account-sim-swapping, accessed 2020-08-27.
[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa
[12] Finn Brunton and Helen Nissenbaum. 2015. *Obfuscation.* The MIT Press, USA.
[13] Pew Research Center. 2019. Mobile Fact Sheet. https://www.pewinternet.org/fact-sheet/mobile, accessed 2020-08-23.
[14] Brian X. Chen. 2019. I Shared My Phone Number. I Learned I Shouldn't Have. The New York Times. https://www.nytimes.com/2019/08/15/technology/personaltech/i-shared-my-phone-number-i-learned-i-shouldnt-have.html, accessed 2020-08-10.
[15] Federal Trade Commission. no date. National Do Not Call Registry. https://www.donotcall.gov, accessed 2020-08-27.
[16] Google Account Help Community. 2019. How Many Gmail accounts can a person have? - I assume they all have to be linked to one number? https://support.google.com/accounts/thread/11008132, accessed 2020-08-26.
[17] Joseph Cox. 2019. I Gave a Bounty Hunter $300. Then He Located Our Phone. Vice. https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile Accessed 2020-08-10.
[18] CVS. no date. Pharmacy Text Alerts. https://www.cvs.com/mobile-cvs/text, accessed 2020-08-27.
[19] Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy. 2019. Evaluating Login Challenges as A Defense Against Account Takeover. In *The World Wide Web Conference* (San Francisco, CA, USA) *(WWW '19)*. Association for Computing Machinery, New York, NY, USA, 372–382. https://doi.org/10.1145/3308558.3313481
[20] James Doubek. 2016. What Happens When You Get Sir Mix-A-Lot's Phone Number. NPR. https://www.npr.org/2016/01/16/463219936/what-happens-when-you-get-sir-mix-a-lots-phone-number, accessed 2020-08-27.
[21] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New Media & Society* 21, 8 (2019), 1824–1839. https://doi.org/10.1177/1461444819833331
[22] Facebook. no date. Custom Audiences from your Customer List. https://www.facebook.com/business/help/170456843145568?id=2469097953376494&helpref=search&sr=5&query=custom%20audience, accessed 2021-01-12.
[23] Facebook. no date. Facebook Community Standards (IV)(18) Misrepresentation. https://www.facebook.com/communitystandards/misrepresentation, accessed 2020-08-27.
[24] Facebook. no date. How does Facebook use my mobile phone number? https://www.facebook.com/help/251747795694485, accessed 2020-08-26.
[25] Facebook. no date. I'm receiving email or text notifications about a Facebook account that doesn't belong to me. https://www.facebook.com/help/225089214296643/?ref=u2u, accessed 2020-09-01.
[26] Facebook. no date. Where do People You May Know suggestions come from? https://www.facebook.com/help/163810437015615, accessed 2020-08-10.

[27] FCC. 2018. Second Report and Order. https://docs.fcc.gov/public/attachments/FCC-18-177A1.pdf, accessed 2020-08-10.

[28] Dinei Florencio and Cormac Herley. 2007. A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web* (Banff, Alberta, Canada) *(WWW '07)*. Association for Computing Machinery, New York, NY, USA, 657–666. https://doi.org/10.1145/1242572.1242661

[29] Adrian Harris Forman. 2012. My Phone Number's Other Woman. The New York Times. https://www.nytimes.com/2012/10/14/opinion/sunday/my-phone-numbers-other-woman.html, accessed 2020-08-27.

[30] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. 2018. "What Was That Site Doing with My Facebook Password?": Designing Password-Reuse Notifications. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1549–1566. https://doi.org/10.1145/3243734.3243767

[31] Google. no date. How to use dual SIMs on your Google Pixel phone. https://support.google.com/pixelphone/answer/9449293, accessed 2020-08-12.

[32] Google. no date. Set up a recovery phone number or email address. https://support.google.com/accounts/answer/183723, accessed 2020-08-26.

[33] Google. no date. Sign in with your phone instead of a password. https://support.google.com/accounts/answer/6361026, accessed 2020-08-27.

[34] Google. no date. Verify your account. https://support.google.com/accounts/answer/114129, accessed 2020-08-25.

[35] Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, and Mary F. Theofanos. 2019. Digital Identity Guidelines: Authentication and Lifecycle Management. https://doi.org/10.6028/NIST.SP.800-63c NIST Special Publication 800-63B.

[36] Roger Grimes. 2019. The many ways to hack 2FA. *Network Security* 2019, 9 (2019), 8–13.

[37] World Bank Group. 2016. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf, accessed 2020-08-27.

[38] Kashmir Hill. 2017. How Facebook Outs Sex Workers. Gizmodo. https://gizmodo.com/how-facebook-outs-sex-workers-1818861596, accessed 2020-09-01.

[39] Hiya. no date. Mr Number: Call Block & Reverse Lookup. https://hiya.com/downloads, accessed 2020-08-27.

[40] Sarah E. Igo. 2018. *The Known Citizen.* Harvard University Press, USA.

[41] Alison Grace Johansen. no date. 5 Kinds of ID Theft Using a Social Security Number. NortonLifeLock. https://www.lifelock.com/learn-identity-theft-resources-kinds-of-id-theft-using-social-security-number.html, accessed 2020-08-15.

[42] jp88. 2019. Phone number limit. Google Account Help Community. https://support.google.com/accounts/thread/13443342, accessed 2020-08-23.

[43] Richie Koch. 2020. The Proton guide to privacy at protests. https://protonmail.com/blog/how-to-protect-privacy-at-protests/, accessed 2020-09-11.

[44] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of Passwords and People: Measuring the Effect of Password-composition Policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. ACM, New York, NY, USA, 2595–2604. https://doi.org/10.1145/1978942.1979321

[45] Pawel Laka and Wojciech Mazurczyk. 2018. User perspective and security of a new mobile authentication method. *Telecommunication Systems* 69, 3 (01 Nov 2018), 365–379. https://doi.org/10.1007/s11235-018-0437-1

[46] Ravie Lakshmanan. 2019. Loyalty programs cost you your personal data - are the rewards worth it? The Next Web. https://thenextweb.com/insights/2019/06/12/loyalty-programs-cost-you-your-personal-data-are-the-rewards-worth-it/, accessed 2020-09-01.

[47] Selena Larson. 2020. Every single Yahoo account was hacked - 3 billion in all. https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html, accessed 2020-09-11.

[48] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan. 2020. An Empirical Study of Wireless Carrier Authentication for SIM Swaps. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX, USA, 61–79. https://www.usenix.org/conference/soups2020/presentation/lee

[49] Mary Madden. 2017. PRIVACY, SECURITY, AND DIGITAL INEQUALITY. https://datasociety.net/library/privacy-security-and-digital-inequality, accessed 2020-08-01.

[50] Alice E. Marwick and danah boyd. 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13, 1 (2011), 114–133. https://doi.org/10.1177/1461444810365313

[51] Mary L. McHugh. 2012. Interrater reliability: The kappa statistic. *Biochemia Medica* 22 (2012), 276–282. https://doi.org/10.11613/bm.2012.031

[52] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2016. Usability and Security of Text Passwords on Mobile Devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. ACM, New York, NY, USA, 527–539. https://doi.org/10.1145/2858036.2858384

[53] Blase Ur Miranda Wei, Maximilian Golla. 2018. The Password Doesn't Fall Far:How Service Influences Password Choice. *Proceedings of the Who Are You?! Adventures in Authentication 2018 Workshop (WAY)* 4th WAY (2018).

[54] Ariana Mirian, Joe DeBlasio, Stefan Savage, Geoffrey M. Voelker, and Kurt Thomas. 2019. Hack for Hire: Exploring the Emerging Market for Account Hijacking. In *The World Wide Web Conference* (San Francisco, CA, USA) *(WWW '19)*. Association for Computing Machinery, New York, NY, USA, 1279–1289. https://doi.org/10.1145/3308558.3313489

[55] Lily Hay Newman. 2018. Phone Numbers Were Never Meant as ID. Now We're All At Risk. Wired. https://www.wired.com/story/phone-numbers-indentification-authentication, accessed 2020-08-26.

[56] Casey Newton. 2014. Inside Twitter's ambitious plan to kill the password. The Verge. https://www.theverge.com/2014/10/22/7034113/inside-twitters-ambitious-plan-to-kill-the-password-on-mobile-devices, accessed 2020-08-27.

[57] Nathaniel Popper. 2017. Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency. The New York Times. https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html, accessed 2020-08-26.

[58] Henry F. Pringle and Katherine Pringle. 1954. Sixty Million Headaches Every Year. The Saturday Evening Post. http://www.saturdayeveningpost.com/wp-content/uploads/satevepost/sixty_million_headaches.pdf, accessed 2020-08-15.

[59] Cooper Quintin. 2018. Our Cellphones Aren't Safe. The New York Times. https://www.nytimes.com/2018/12/26/opinion/cellphones-security-spying.html, accessed 2020-08-16.

[60] Emilee Rader and Anjali Munasinghe. 2019. "Wait, Do I Know This Person?": Understanding Misdirected Email. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland UK) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300520

[61] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, USA, 89–108. https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

[62] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/soups2019/presentation/reese

[63] J. H. Saltzer and M. Schroeder. 1975. The protection of information in computer systems. *Proc. IEEE* 63 (1975), 1278–1308.

[64] Richard Shay, Iulia Ion, Robert W. Reeder, and Sunny Consolvo. 2014. "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra": Experiences with Account Hijacking. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. ACM, New York, NY, USA, 2657–2666. https://doi.org/10.1145/2556288.2557330

[65] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, and Nasir Memon. 2017. Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers and Security* 65 (2017), 14–28.

[66] Signal. no date. Register a phone number. https://support.signal.org/hc/en-us/articles/360007318691-Register-a-phone-number, accessed 2020-09-01.

[67] Robert Snell. 2017. Feds use anti-terror tool to hunt the undocumented. The Detroit News. https://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/, accessed 2021-01-10.

[68] Telegram. no date. Telegram FAQ - Phone Number. https://telegram.org/faq#q-i-have-a-new-phone-number-what-do-i-do, accessed 2020-09-01.

[69] Twitter. no date. About your email and phone number discoverability privacy settings. https://help.twitter.com/en/safety-and-security/email-and-phone-discoverability-settings, accessed 2020-09-01.

[70] Twitter. no date. Personal information and ads on Twitter. https://help.twitter.com/en/information-and-ads, accessed 2020-08-22.

[71] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proceedings of the 21st USENIX Conference on Security Symposium* (Bellevue, WA) *(Security'12)*. USENIX Association, Berkeley, CA, USA, 5–5. http://dl.acm.org.proxy.lib.umich.edu/citation.cfm?id=2362793.2362798

[72] G. Venkatadri, A. Andreou, Y. Liu, A. Mislove, K. P. Gummadi, P. Loiseau, and O. Goga. 2018. Privacy Risks with Facebook's PII-Based Targeting: Auditing a Data Broker's Advertising Interface. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEE, USA, 89–107. https://doi.org/10.1109/SP.2018.00014

[73] WhatsApp. no date. How to verify your number. https://faq.whatsapp.com/iphone/verification/how-to-verify-your-number, accessed 2020-09-01.

[74] Yan Zhao, Shiming Li, and Liehui Jiang. 2018. Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment. *Security and Communication Networks* 2018 (05 2018), 1–13. https://doi.org/10.1155/2018/9178941

[75] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 197–216. https://www.usenix.org/conference/soups2018/presentation/zou

# A SURVEY QUESTIONS

**Q1**: Please select all types of phone numbers you have had in the last 5 years.

- Mobile phone number
- Landline (i.e. household number)
- Virtual phone number (e.g. Google Voice, Skype number)

**Q2**: Do you have your own mobile phone or do you share it with someone else?

- I have my own mobile phone
- I share a mobile phone

*[Conditional]* **Q3**: Who do you share a mobile phone with?

- My spouse / partner
- My parent(s)
- My sibling(s)
- My children
- Other: [free response]

**Q4**: How many times have you gotten a new phone number in the last 5 years?

- 0 times
- 1 time
- 2-5 times
- 5+ times

**Q5**: How long have you had your current primary phone number (in years)?

[Drop down of items from 1 year to 10 years]

**Q6**: Have you had any annoying, weird, or disturbing experiences involving your phone number? Please describe your experience in as much detail as possible. Feel free to write about as many experiences as you wish.

**Q7**: Were there any consequences for you because of the experiences you described above (e.g., with respect to your privacy, safety or ability to access services)? Please explain.

**Q8**: Have you ever been unable to use an online service, app or other resources because you could not provide a phone number? If yes, please 1) explain what happened and 2) describe any consequences for you.

**Q9**: Have you ever lost access to a phone number (e.g. because you couldn't pay your cellular bill)? If yes, please 1) explain what happened and 2) describe any consequences for you.

**Q10**: Have you ever had any weird experiences with phone number recycling (e.g. getting a number that was previously owned by someone else)? If yes, please 1) explain what happened and 2) describe any consequences for you.

**Q11**: Have you had any experiences in which you had to share your phone number with an online service, an app, a company, or a person but felt uncomfortable doing so? If yes, please 1) explain why you were uncomfortable and 2) what any consequences were for you.

**Q12**: If these questions jogged your memory about any other negative experiences with phone numbers that you have not yet shared, please tell us about the experiences and the consequences here.

**Q13**: In which country do you currently live?
[Drop down of list of countries]

**Q14**: What is your age?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65 or older
- Prefer not to answer

**Q15**: What is your gender?

- Male
- Female
- Nonbinary
- Other: [free response]
- Prefer not to answer

**Q16**: What is the highest level of school you have completed or the highest degree you have received?

- Less than high school degree
- High school graduate (high school diploma or equivalent including GED)
- Some college but no degree
- Associate degree in college (2-year)
- Bachelor's degree in college (4-year)
- Master's degree
- Doctoral degree
- Professional degree (JD, MD)
- Prefer not to answer

**Q17**: Which statement best describes your current employment status?

- Employed full-time (working 40 or more hours per week)
- Employed part-time (working up to 39 hours per week)
- Not working (looking for work)
- Not working (not currently looking for work)
- Self-employed
- Homemaker
- Retired
- Student
- Unable to work
- Prefer not to answer