Cape

JUNE 2026

Securing the Line: America's Mobile Privacy Crisis

Uncovering today's mobile privacy paradox and the forces reshaping consumer expectations

Executive Summary

The Harris Poll, commissioned by Cape, built and conducted an independent survey of how Americans view mobile privacy and security. It surveyed over 2,000 adults in the United States aged 18 and over in October 2025—and aimed to uncover Americans' views of mobile privacy and security.

Survey results found that many Americans both significantly rely on and trust existing mobile communication channels. Among others:

- 81% of Americans trust phone calls for sensitive communication, while 76% say the same for SMS and 74% for voicemail.
- Baby Boomers trust phone calls for sensitive conversations more often than younger generations (86% vs. 79% of Gen Z vs. 78% of Millennials).
- Baby Boomers also rely on phone calls more overall; 38% say phone calls are their primary communication method compared to 23% of Gen Z and 28% of Millennials.
- 78% of Americans rely on either phone calls or SMS as the primary way they communicate with friends and family.
- Phone calls are used most often for communications with healthcare providers (48%), financial institutions (38%), and for parents of children under 18, schools, and daycares (38%).
- About another one in ten prefer SMS for these sensitive interactions (11% healthcare providers, 11% financial institutions, 9% schools and daycares).

At the same time, few Americans expressed awareness of the privacy and security risks of mobile devices and mainstream communications pathways.

- Fewer than one-third of Americans believe they have given carriers permission to share their location, browsing behavior, or demographic information, even though such collection is typically on by default unless consumers proactively opt out.
- 63% of Americans say it is easy to opt out of carrier data sharing, even though carrier transparency reports show opt-out rates below 1%.[4]
- 59% of Americans don't know that disabling location settings does not prevent all forms of location tracking, while 37% believe this stops tracking entirely, even though it does not.
- 71% agree that consumers need to accept risks to their privacy when using mobile devices, and 59% believe that what mobile service providers do with personal and usage data is beyond consumers' control. At the same time, 80% of Americans believe they can protect their privacy by actively managing their device settings.
- 41% don't know that mobile service providers can share personal information, such as contact information and usage data, with other companies for marketing and other purposes.

These findings underscore a critical paradox at the heart of Americans' use of mobile devices. Americans depend on them, including their phone call and SMS functions, for sensitive communications yet don't feel they can control what mobile carriers do with their data; they believe that device settings and opt-outs help them to protect their privacy yet don't always exercise those features and have serious knowledge gaps about cybersecurity flaws, data-collection and -sharing practices, and other privacy and security risks pervasive in mobile carriers and devices. But, perhaps most promising of all, some Americans do still care about their data—and many are interested in more secure, privacy-protective options for the communication systems that we use every day.

Contents

Introduction

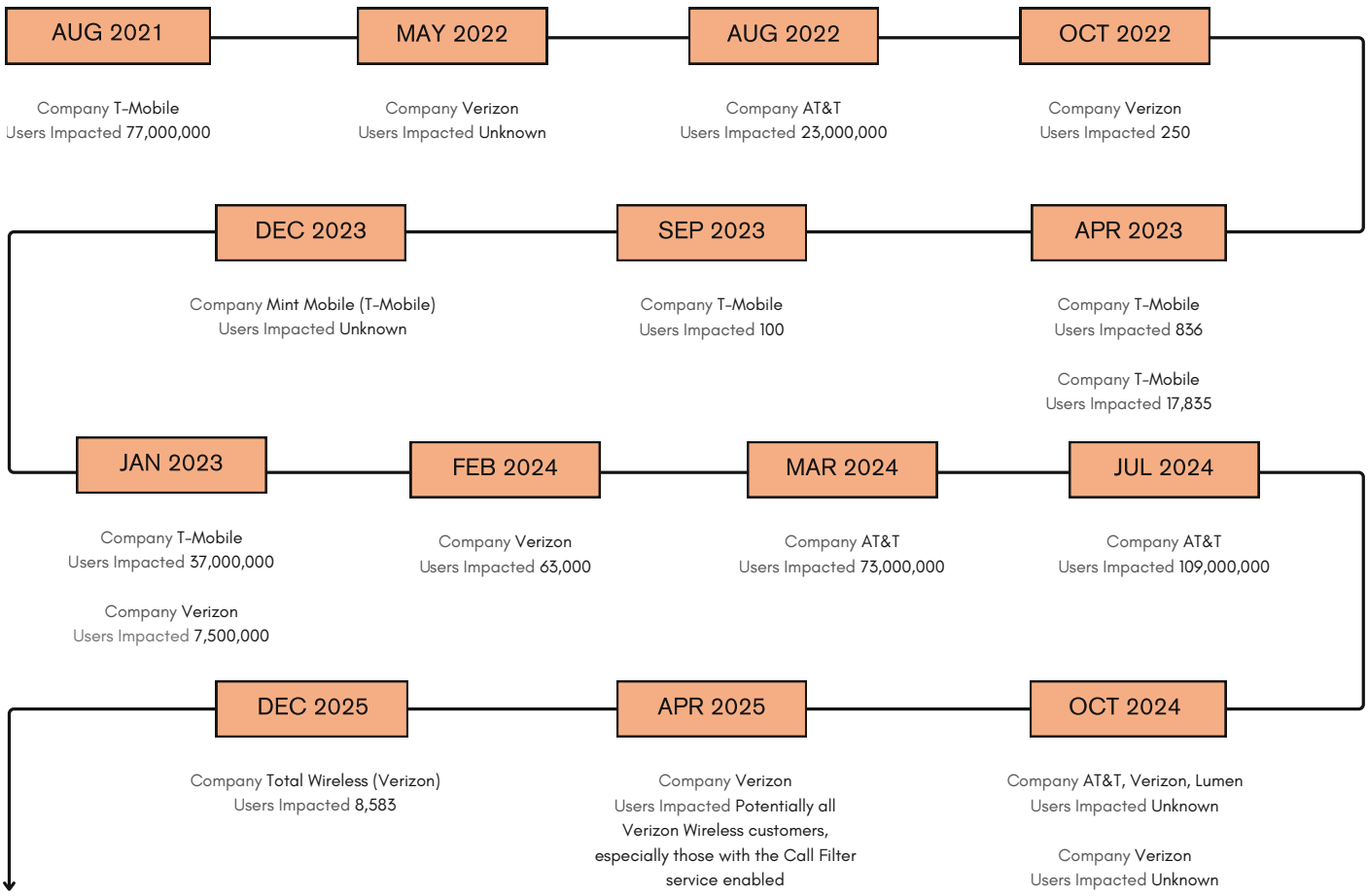
An Illusion of Privacy

Mobile phones sit at the center of American life. They carry family conversations, financial access, medical updates, school communications, and interactions with government agencies. Because so much flows through a single device, many Americans assume that managing privacy settings, limiting app permissions, or using tools such as VPNs and encrypted messaging provides meaningful protection.

These steps address real risks at the app and device level. They do not, however, protect against vulnerabilities built into the cellular networks that make mobile communication possible. Network-level systems operate largely in the background, outside the controls most people see or regularly use.

Every mobile phone must remain in constant contact with nearby cell towers to function. Even when location services are turned off and apps are restricted, a phone continues to report its approximate location so calls, texts, and data can be delivered. This location data is generated automatically as part of mobile service itself, independent of app settings. Major breaches at carriers such as Verizon, AT&T, and T-Mobile have exposed call records, location data, and account information affecting tens of millions of customers.[1] In recent years, these carriers have been fined for sharing this information with third parties. Data created simply by using a phone was collected and monetized without user awareness.[2]

U.S. Telecommunications Data Breach Timeline *2021 - 2025*



Phone numbers introduce another risk layer. What once served primarily as a way to place calls now functions as an identity anchor across banking, email, social platforms, and government services. Text messages are familiar, fast, and easy to use and as a result are regularly required for account registrations, package deliveries, and much more. Many websites also continue to require a phone number as part of their multi-factor authentication process. As a result, SMS remains deeply embedded in account creation, verification, management, and protection. But these phone numbers can be transferred or intercepted. Because many accounts rely on security codes sent by text, control of a phone number often determines access to a person's digital life. In a SIM-swap attack, attackers trick carriers into transferring a victim's phone number to a new device. Once the transfer occurs, text messages intended for the victim, including account security codes, are redirected, enabling account takeovers without ever touching the victim's phone.

At the network level, additional weaknesses compound these risks. Global signaling systems allow mobile networks to route calls and messages across carriers. A compromised or malicious network can request a user's location, intercept calls, or receive text messages by falsely claiming the user is roaming. U.S. cybersecurity officials have warned that these vulnerabilities are actively exploited, yet they remain invisible to most consumers and unaddressed by device-level privacy tools.[3]

Today's privacy landscape is shaped less by what users choose and more by what networks allow.

1 Exposure is the Default

Americans trust the channels that expose them the most

The survey found that phone calls and SMS remain central to how Americans communicate, especially when conversations feel private or high stakes. More than eight in ten (81%) survey respondents trust phone calls for sensitive communication while three-quarters say the same for SMS (76%) and voicemail (74%). Reliance and trust are strongest among older adults. Baby Boomers trust phone calls for sensitive conversations more often than younger generations (86% vs. 79% of Gen Z and 78% of Millennials), and they rely on phone calls more overall; 38% say phone calls are their primary communication method compared to 23% of Gen Z and Millennials.

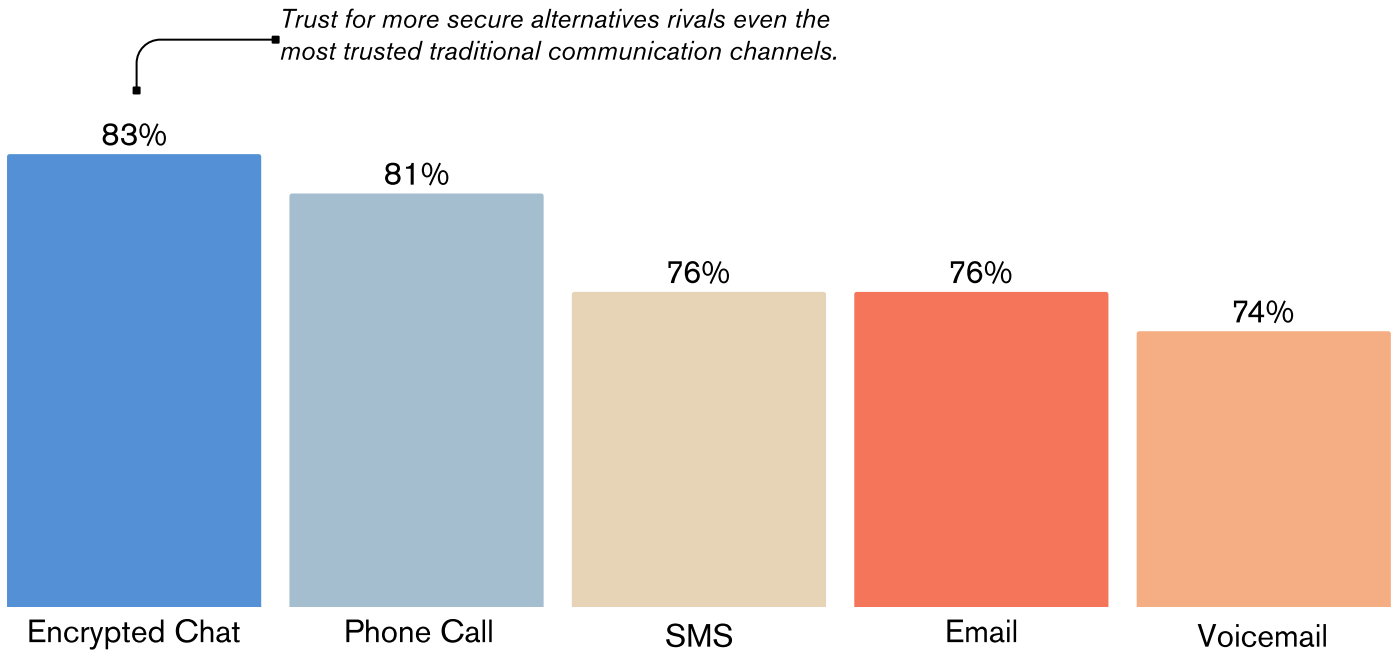
Phone calls and SMS depend on networking systems designed for reliability and interoperability, not security. Calls and texts generate rich streams of metadata, including who communicated with whom, when, how often, and from where. A routing protocol known as SS7 helps carriers exchange the information needed to connect calls, deliver messages, and support roaming between networks. SS7 assumes that once a request enters the signaling system, it is legitimate. That assumption has created several well-documented vulnerabilities.

Access to signaling can enable multiple forms of exploitation without touching the device itself. In documented cases, attackers have used signaling queries to identify which cell tower a phone is connected to and infer a person's location across cities or even national borders, regardless of whether location services were disabled or spyware was present.[5] The same signaling access has been used to reroute SMS traffic, intercepting one-time passcodes sent by banks and other services and enabling account takeovers without compromising phones.[6] Signaling controls have also been abused to silently redirect or copy phone calls and messages, making it possible to monitor communications with no visible indication to the user and no trace in app-level logs.[7]

These weaknesses persist because they operate at the network layer, beyond the reach of consumer tools. They have been exploited by surveillance vendors, criminal groups, and state actors precisely because they don't require malicious apps or user interaction. Regulatory reviews have repeatedly acknowledged that signaling-layer vulnerabilities remain unresolved despite years of awareness and partial mitigation efforts.[8] As long as that layer remains vulnerable, exposure will be dictated by the network, not the user.

Trust in Methods for Sensitive Communications

Among All U.S. Adults



Privacy settings feel empowering until the network takes over

The survey found that many Americans believe that device- and app-level privacy controls – such as disabling location services, limiting app-level data sharing, and using encrypted messaging – keep them safe from tracking because they are visible, accessible, and framed as protective. However, that confidence is often misplaced.

Fifty-nine percent of Americans don't know that disabling location settings does not prevent all forms of location tracking while more than a third incorrectly believe this stops tracking entirely. This misunderstanding extends to app controls: 64% don't know that disabling app-level data sharing does not prevent telecom-level tracking, and 35% incorrectly believe that it does. These gaps are largest among younger adults. Fifty percent of Gen Z and 46% of Millennials believe their location cannot be tracked once location services are disabled, compared with 32% of Gen X and 26% of Boomers.

Further, eventy percent of Americans don't know that using encrypted chat apps does not prevent access to communications activity, such as metadata that exposes communication patterns, timing, and location information. Forty-two percent incorrectly believe encrypted messaging prevents this type of exposure. Among encrypted chat users, 62% believe their communications activity is fully protected, compared with 32% of non-users. This is despite the fact that encrypted messaging adds real protection but, in reality, does not provide security for the breadth of device and data issues that Americans appear to believe it does.

Taken together, the data show that Americans are building their privacy strategy around what they can see and control. However, the survey results indicate that Americans' placement of trust is often based on inaccurate assumptions about the current state of mobile device and network security.

Tracking Misconceptions

What Americans Get Wrong About Location and Data Privacy

Beliefs about app-level data sharing

64%
do not know disabling data sharing does not stop telecom-level tracking

35%
incorrectly believe turning off location data sharing does stop all tracking

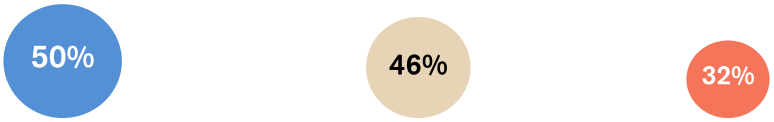
Beliefs about location tracking

59%
do not know turning off location settings does not prevent all location tracking

More than
1 in 3
incorrectly believe turning off location settings stops all forms of location tracking

Younger, digital natives more likely to get it wrong

Incorrectly believe disabling location settings prevents tracking



Americans think they've opted out, but almost no one has

Most Americans assume they have meaningful control over what their mobile carrier collects and shares. Consent is commonly understood as something explicit and intentional, given only when a user actively agrees.

Only 31% of Americans believe they have given permission to their mobile carriers for their location to be shared. Just 28% believe they allowed sharing of demographic information, and only 27% believe they permitted sharing of browsing behavior. These beliefs persist even though carrier data collection and sharing are typically enabled by default unless a consumer actively opts out. While 63% of Americans say it is easy to opt out of carrier data sharing, most consumers rarely do so in practice, based on available data. For example, Verizon's 2024 transparency report showed opt-out rates under 1%, leaving the overwhelming majority of customers in default data-sharing arrangements.[9]

Faith in self-management reinforces this gap. Eighty percent of Americans believe consumers can protect their privacy by actively managing the settings on their mobile devices, strengthening the perception that consent has already been exercised through interaction rather than passively accepted through default terms.

Generational differences add another layer. Boomers and Gen X are more likely than Gen Z to say they restrict sharing of texts (62% and 57% vs. 46%) and home addresses (54% and 58% vs. 45%) even though defaults remain largely unchanged.

The practical result is that many Americans believe they have drawn boundaries while carriers continue to operate unrestrained.

Phone numbers are easy to use – and easy to lose

Used for communication, account access, and authentication, phone numbers function as a core identity layer in the mobile ecosystem. Because calls and SMS are so embedded in daily life, the risk tied to controlling a phone number is easy to overlook.

Reliance on these channels is widespread. Seventy-eight percent of Americans rely on either phone calls or SMS as the primary way they communicate with friends and family. These channels also dominate sensitive interactions. Phone calls are used most often for communications with healthcare providers (48%), financial institutions (38%), and for parents of children under 18, schools and daycares (38%). Another one in ten prefer SMS for these sensitive interactions (11% healthcare providers, 11% financial institutions, 14% schools and daycares).

Awareness of SIM-swap risk remains low. A SIM-swap occurs when a phone number is reassigned to a new SIM card, allowing someone else to receive calls, texts, and security codes intended for the original user. Fifty-eight percent of Americans don't know that their phone number can be transferred to another device without their permission. More than half (54%) of Americans also use SMS for two-factor authentication (2FA) even though only 34% believe SMS is among the safest authentication options. For many Americans, the convenience of using a phone number for 2FA outweighs the security concerns, especially when many platforms and services still require it.

Generational patterns reveal uneven exposure. Millennials are more likely than Gen X and Boomers to use stronger authentication methods, such as an authenticator app (34% vs. 24% and 12%) or backup recovery code (30% vs. 22% and 15%). Older adults are therefore more dependent on SMS-based security—and therefore exploitations of SMS-related vulnerabilities. Still, even among those adopting stronger tools, SMS remains deeply entrenched, creating a single point of failure that attackers continue to exploit in major breaches.

Real-world incidents show how this vulnerability is exploited. SIM-swaps have been used to intercept one-time passcodes, reset financial and cryptocurrency accounts, and impersonate victims without access to their physical device. Documented cases include a retail store manager who sold unauthorized SIM-swaps, as well as a cryptocurrency investor losing $1.3 million after attackers transferred her phone number without permission and intercepted SMS codes to drain her accounts.[10] Further reporting has detailed similar incidents in which carrier employees are recruited to perform SIM swaps for pay, as well as incidents where consumer accounts are compromised through unauthorized number transfers.

2 Confusion Becomes Resignation

Privacy fatigue has become a security problem

Many Americans experience mobile privacy less as a problem to solve and more as a condition to manage. Nearly three in four (71%) agree that consumers need to accept risks to their privacy when using mobile devices, and 59% believe that what mobile service providers do with personal and usage data is beyond consumers' control. At the same time, four in five Americans (80%) believe they can protect their privacy by actively managing their device settings. These views coexist, reflecting a gap between perceived responsibility and perceived influence.

Rather than signaling disengagement, this pattern suggests that Americans feel they are doing what they can while also believing that the most consequential decisions about data collection and security sit with carriers. Privacy risk, in this context, feels persistent rather than solvable through individual action alone.

Generational differences help clarify this dynamic. Boomers are the most likely to trust their mobile service providers' ability to secure customer data, with nearly three-quarters expressing trust. Among younger and middle-aged adults, trust is lower. Just 65% of both Gen Z and Gen X say they trust their current provider to secure their data against potential breaches. At the same time, younger generations appear more likely to seek out tools they believe offer stronger protection. Twelve percent of Gen Z and 13% of Millennials say they use encrypted chat apps most often to communicate with friends and family, compared with 5% of Gen X and just 2% of Boomers. However, higher adoption of privacy solutions does not mean a better understanding of their limitations. Younger generations are also more likely to hold incorrect assumptions about the effectiveness of device-level controls, including beliefs about disabling location services.

As a result, effort and uncertainty often coexist. Americans continue adjusting settings, adopting tools, and managing perceived risk while accepting that individual actions alone may not meaningfully change their exposure. In fact, more than one in five admit they don't know whether they've allowed their mobile provider to share personal data including their texts (21%), voicemails (21%), location (21%), browsing behavior (24%), purchase history (24%), names (22%), and email address (22%) with third parties. In this context, privacy risk feels persistent rather than solvable through individual action alone.

When the stakes rise, the protections don't

In the absence of meaningful control, Americans default to the communication channels they know best. Approximately four in five Americans trust phone calls (81%), SMS (76%), voicemail (74%), and email (76%) for sensitive communications on their mobile device. These levels of trust persist despite broad recognition that privacy risks are difficult to avoid, indicating that confidence in specific channels is shaped by habit and long-standing use.

Encrypted chat apps play a more limited role. Only 37% of Americans use encrypted chat apps, and even among these users, reliance on traditional channels remains substantial. Nearly two-thirds of encrypted chat app users (64%) still use phone calls or SMS most often to communicate with friends and family. For those that do use encrypted chat apps, 83% trust them for sensitive communications—although this trust does not replace dependence on more exposed channels.

Boomers are the most likely to trust phone calls, with 86% expressing trust, compared with 79% of Gen Z and 78% of Millennials. Despite lower trust in traditional channels, behavior among younger generations does not fully shift, reinforcing the influence of habit. For example, even among Millennials — the generation most likely to adopt stronger 2FA methods — usage remains limited, with 34% using authenticator apps, 30% using backup recovery codes, and just 16% using hardware security keys. SMS's dominance as the most common form of 2FA, used by more than half of Americans, underscores how deeply legacy mobile infrastructure remains embedded in security best practices across generations.

In a landscape where privacy risks are widely viewed as unavoidable, familiar channels may retain trust not because they are perceived as secure, but because they are viewed as essential.

Different ages, different blind spots, same exposure

Generational risk profiles reflect varying levels of trust, tool adoption, and understanding. Boomers sit at one end as nearly three-quarters (74%) trust their provider to secure their data against potential breaches, and 90% report satisfaction with privacy and security features. Boomers and Gen X are more likely than Gen Z to say they do not allow providers to share texts (62% and 57% vs. 46%) and home addresses (54% and 58% vs. 45%), reinforcing a belief that exposure is already contained.

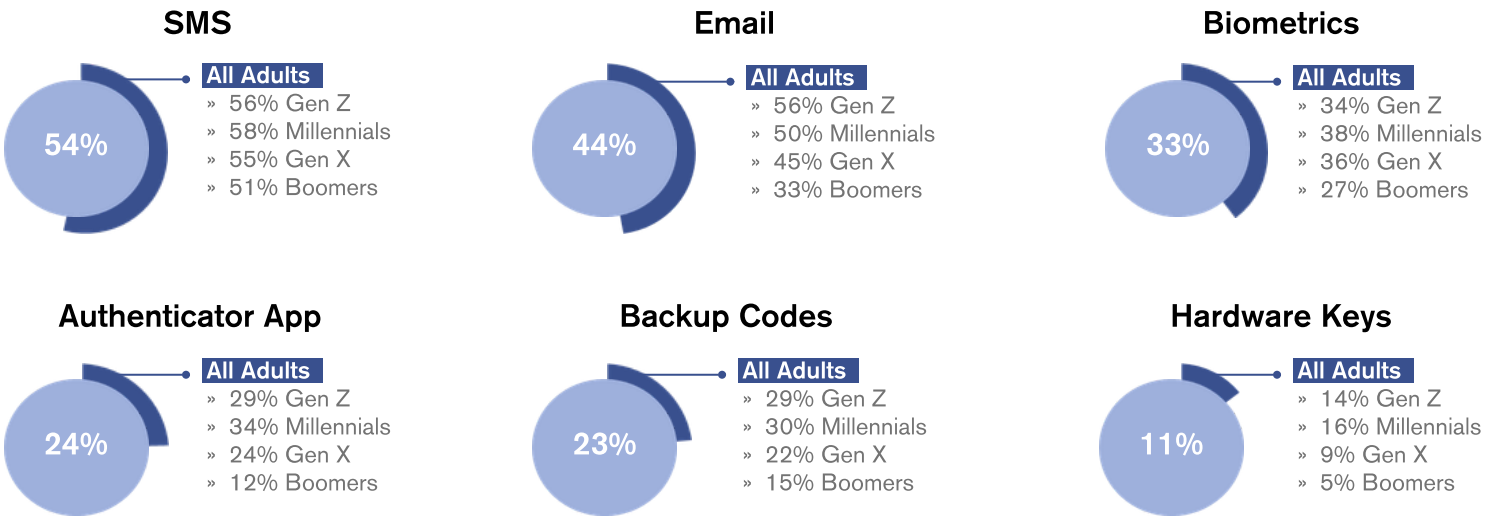
Younger generations show more proactivity but not necessarily more protection. Carrier trust drops to 65% among both Gen Z and Gen X. Gen Z and Millennials are more likely than Gen X and Boomers to use encrypted chat apps most often with friends and family (12% and 13% vs. 5% and 2%), yet they are also more likely to believe – incorrectly – that encrypted chat apps fully protect communications activity (54% and 51% vs. 38% and 32%). A similar misconception appears in beliefs about tracking: 50% of Gen Z and 46% of Millennials believe their location cannot be tracked once location services are disabled, compared with 32% of Gen X and 26% of Boomers.

Authentication choices further differentiate risk. Gen Z is the most likely to use email for 2FA (56%), compared with 33% of Boomers. While Millennials lead in adoption of most 2FA methods, Gen X puts greater trust in biometrics, with 51% believing they are among the safest 2FA options compared to 37% Gen Z and 43% Millennials. This far outpaces the third of Americans using biometrics for 2FA despite 44% believing it is among the safest solutions.

Overall, older adults tend to trust providers and assume restrictions are in place. Younger adults adopt privacy tools while overestimating their reach, and middle generations combine skepticism with uneven mitigation. These are distinct vulnerabilities that consumer-controlled privacy measures alone cannot resolve.

Adoption of Two-Factor Authentication Methods

By Generation



3 The Network Sets the Terms

Legacy infrastructure keeps mobile privacy one step behind modern threats

In the past year alone, AT&T, Verizon, and T-Mobile have each experienced severe breaches.[12] Attackers have intercepted communications, queried location data, and accessed call records. The gap in awareness helps explain why many consumers focus on device-level actions, even as key risks originate in carrier systems and network infrastructure that operate outside the user's view.

Recent telecom incidents illustrate why these risks cannot be managed through consumer controls alone. In October 2024, attackers claimed administrative-level access to Verizon's Push-to-Talk (PTT) systems and offered a massive dataset for sale, describing call logs alongside emails, phone numbers, addresses, and names. In a separate incident publicly reported in October 2024, a China-linked intrusion known as "Salt Typhoon" was reported to have compromised multiple major U.S. telecommunications providers, including Verizon, with attackers accessing lawful intercept systems and obtaining sensitive metadata such as call logs, and in some cases additional communications data.[13] Later reporting has warned that the attackers may still retain access to all the call logs, raising the prospect that metadata for nearly every American remains exposed.[14] Such incidents underscore a structural reality: the most consequential privacy threats originate in carrier-side systems, legacy infrastructure, and administrative access paths that consumers cannot see or configure away.

Metadata reveals more than messages ever could

Americans are only partially aware of what carriers can do with their data.

Even when content is encrypted, metadata often is not. Mobile carriers, by necessity, generate and retain much of this metadata to route traffic and manage networks, which makes it uniquely persistent and difficult for consumers to avoid. Carrier metadata can show who was in contact, when and where communication occurred, which online services were accessed based on associated IP addresses, and how heavily those services were used. Nonetheless, about two in five Americans (41%) don't know that mobile service providers can share personal information, such as contact information and usage data, with other companies for marketing and other purposes.

Many Americans recognize aspects of this reality, yet awareness of what encryption does and does not do remains limited. About two in three Americans (65%) know that their mobile service provider can track online activities on their device. However, 70% don't know that using encrypted chat apps does not ensure metadata cannot be accessed by anyone else.

Access to customer metadata can be consequential. In July 2024, AT&T disclosed that records tied to roughly 109 million customer accounts, roughly one-third of all Americans, were illegally downloaded, including call and text records.[15] Although the files did not include the content of calls or texts, some records included cell site identification numbers that could be used to determine the approximate location where a call was made or a text was sent. This is the core problem with metadata: it can be aggregated to map contact networks, infer location over time, and reconstruct patterns of life even when people believe they have protected the content of their communications.

Privacy tools stop at the screen, not the network

Consumers gravitate toward tools that promise privacy: VPNs, app permissions, encrypted messaging, and device settings. These solutions reduce some risk, but they cannot reach the network-level exposures that matter most.

The gap between perceived protection and structural protection is visible in how Americans approach authentication. SMS remains the most common method for 2FA, likely reflecting its convenience and accessibility. More secure alternatives remain niche. For some options, use aligns with safety perceptions: 25% believe authenticator apps are among the safest options while 24% use them, and 22% believe backup recovery codes are among the safest options while 23% use them. Other alternatives have struggled to gain adoption despite their safety perceptions. Hardware security keys are used by only 11% of Americans even though 15% believe they are among the safest options while 44% believe biometrics is among the safest 2FA options, yet only 33% use it. This pattern suggests that the tools Americans rely on the most are not necessarily the ones they think are the safest. It could also be explained, among other factors, by the interoperability still offered by phone calls and SMS, compared to how interoperable network carriers, mobile device operators, and other technology companies have made encrypted app messaging with one another's systems.

The same limitation applies to privacy tools used for communication. VPNs can help protect browsing traffic in certain contexts, but they do not protect calls or texts, and they do not prevent carrier-level tracking. Still, 90% of people who use a VPN to protect their privacy on their mobile device believe it is effective. Encrypted chat apps can protect message content, but they do not eliminate metadata exposure; carriers can still see traffic patterns, including timing and volume. Encrypted chat accounts can also be vulnerable to account takeovers when they are tied to traditional phone numbers since attacks that compromise control of a number can enable an attacker to hijack account access.[16] In short, more proactivity does not guarantee more privacy, leaving many vulnerable despite their efforts.

4 The Public Is Ready to Switch

Americans are ready to reward carriers that make privacy real

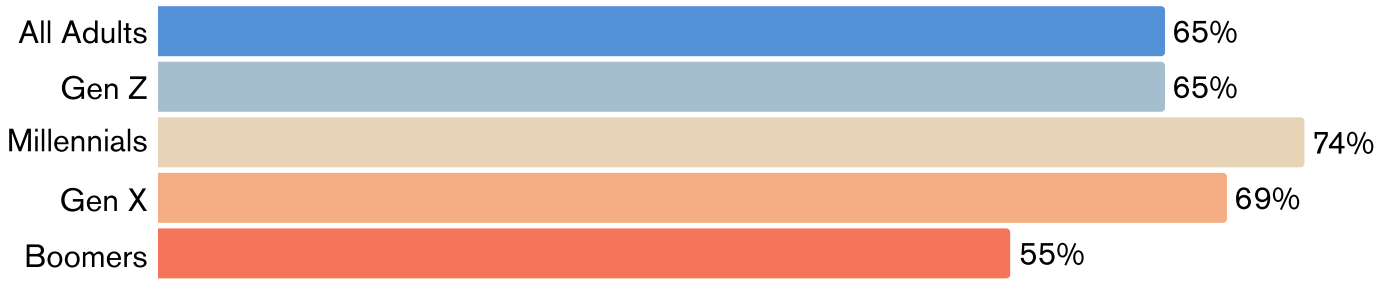
Interest in stronger mobile privacy protections is no longer limited to a small segment of security-conscious consumers. Nearly two-thirds of Americans (65%) say they are interested in switching to a mobile provider that offers enhanced privacy and security, including less personal data collection and greater protection against hacking. One in five (21%) say they are very interested, signaling meaningful demand for alternatives that reduce exposure rather than simply adding new settings or features.

This level of interest reflects a broader shift in consumer expectations. Americans are increasingly treating privacy and security as core service requirements, not optional add-ons.

The demand spans generations. Interest in switching reaches 74% among Millennials and 69% among Gen X, compared with 65% among Gen Z and 55% of Boomers. The desire for enhanced protections is already widespread, but the intensity of that demand, and the likelihood of acting on it, is being led by younger and middle-aged adults.

Interested in Switching to a More Secure Mobile Provider

By Generation



Education turns trust into safer behavior

Boomers highlight the sharpest vulnerability gap; few are very interested in switching to a more data-secure mobile provider (13%), yet they are the most likely to trust traditional channels like phone calls for sensitive communications (86% vs. 79% Gen Z and 78% Millennials) and to trust their carrier to prevent breaches (74% vs. 65% Gen Z and 65% Gen X). Those most dependent on legacy channels, and most confident in carrier protection, may also be the least likely to seek out stronger safeguards on their own.

Millennials, by contrast, display the highest urgency. Nearly a third (32%) are very interested in switching, indicating a readiness to reward providers that offer privacy and security that is structurally stronger, simpler to understand, and easier to adopt.

Together, these patterns define the market opportunity. The next generation of mobile privacy will be shaped by providers that make protection automatic and the default while communicating risk in clear, credible terms that help consumers recognize exposure before it becomes personal.

From Perceived Control to Real Protection

Mobile privacy has reached a breaking point. Americans are trying to manage exposure through device-level settings and tools even though the risks that matter most exist at the network level, at the device operating system level, or within companies' business practices, beyond what individuals can control or configure.

This is not simply a gap in consumer understanding. It is a mismatch between how mobile systems were built and what modern life now demands of them. When privacy depends on perfect consumer behavior, it will fail for most people most of the time. The future of mobile privacy requires shifting from opt-in protection to baseline safeguards that reduce exposure automatically.

The standard moving forward is clear: less collection, less retention, less exploitable metadata, and fewer pathways for identity and communications to be hijacked. Anything short of that will continue to deliver the illusion of control, substituting luck for true protection. Real mobile privacy is possible, and it starts beneath the screen.

Endnotes

1. "Telco Data Breach Timeline," Cape, 2025.
2. "FCC Fines Larges Wireless Carriers for Sharing Location Data," Federal Communications Commission, April 29, 2024.
3. Andy Greenberg, "Security News This Week: US Official Warns a Cell Network Flaw is Being Exploited for Spying," Wired, May 18, 2024.
4. "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers," Federal Trade Commission, October 21, 2021; "California Consumer Privacy Act - 2024 Reporting," Verizon, October 2025.
5. "How First Wap Tracks Phones Around the World," Lighthouse Reports, October 14, 2025; Gabriel Geiger, et al., "The Surveillance Empire That Tracked World Leaders, a Vatican Enemy, and Maybe You," Mother Jones, October 2025.
6. Luana Pascu, "2FA fail; hackers exploit SS7 flaw to drain bank accounts," Bitdefender, May 5, 2017; Andy Greenberg, "Security News This Week: US Official Warns a Cell Network Flaw is Being Exploited for Spying," Wired, May 18, 2024.
7. Andy Greenberg, "Security News This Week: US Official Warns a Cell Network Flaw is Being Exploited for Spying," Wired, May 18, 2024; Zack Whittaker, "A surveillance vendor was caught exploiting a new SS7 attack to track people's phone locations," TechCruch, July 18, 2025.
8. Copper Quintin, et al., "EFF to FCC: SS7 is Vulnerable, and Telecoms Must Acknowledge That," EFF, July 15, 2024.
9. "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers," Federal Trade Commission, October 21, 2021; "California Consumer Privacy Act - 2024 Reporting," Verizon, October 2025.
10. Mike Dano, "Telecom store manager pleads guilty to selling SIM swaps for $1,000," Light Reading, March 19, 2024; Terrence Zimwara, "Canadian Woman Sues After $1.3M in Bitcoin Vanishes in SIM-Swap Scam," Bitcoin.com, July 6, 2025.
11. "T-Mobile Employees Across The Country Receive Cash Offers to Illegally Swap SIMs," TMO Report, April 15, 2024; Jason Knowles, et al., "Hackers take over family's Cricket Wireless account, shut down phones and take over financial apps," ABC7 Chicago, March 14, 2014.
12. "Telco Data Breach Timeline," Cape, 2025.
13. Ibid.
14. Ibid.
15. Adam Goldman, "'Unrestrained' Chinese Cyberattackers May Have Stolen Data From Almost Every American," The New York Times, September 4, 2025.
16. "Telco Data Breach Timeline," Cape, 2025; Thomas Brewster, "Watch As Hackers Hijack WhatsApp Accounts Via Critical Telecoms Flaws," Forbes, June 1, 2016.

Methodology

This survey was conducted online within the United States by The Harris Poll on behalf of Cape from October 9-14, 2025, among 2,070 U.S. adults ages 18 and older. Data were weighted where necessary by age, gender, race/ethnicity, region, education, marital status, household size, household income, and political party affiliation, to bring them in line with their actual proportions in the population. The sampling precision of Harris online polls is measured by using a Bayesian credible interval. For this study, the sample data is accurate to within +/- 2.5 percentage points using a 95% confidence level. This credible interval will be wider among subsets of the surveyed population of interest. For complete survey methodology, including weighting variables and subgroup sample sizes, please contact press@cape.co.

About Cape

Cape is a mobile carrier built with privacy and security as core priorities. Using a minimum-trust model, Cape focuses protections at the network level, where many serious vulnerabilities originate, rather than relying on users to manage risk on their own. Its architecture limits data collection, hardens its network against insider threats, and addresses signaling-based attacks, metadata exposure, and SIM-related account takeovers that apps or device settings cannot fully mitigate. As part of this approach, Cape also reduces reliance on long-lived network identifiers through features such as identifier rotation, helping limit persistent tracking over time. These protections ensure Cape integrates privacy and security directly into how connectivity is delivered.

RESEARCH / RESEARCH