Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	**CG Docket Nos. 17-59 and 02-278**
	)	**FCC 26-27**
Enhancing Know-Your-Customer	)	
Requirements	)	
	)	

Comments of Gregory Maxwell
June 25, 2026

Table of Contents

I. The Security and Privacy Harms of Mandatory Identification 1

II. Harm to Vulnerable Populations 3

III. The First Amendment Right to Anonymous Speech 4

IV. Routing Around the Fourth Amendment 5

V. The Commission Lacks Authority to Impose Such a Requirement 5

VI. The Commission Is Not a Law Enforcement Body 7

VII. The Cryptocurrency Payment Red Flag 7

VIII. The Forfeiture Penalty Will Drive Over-Compliance 8

IX. Safe Harbor Would Worsen the Problem 9

X. The Proposal Would Be Ineffective 10

XI. Conclusion 12

References 13

I urge the FCC to abandon the Further Notice of Proposed Rulemaking in CG Docket Nos. 17-59 and 02-278 and any other action which would require ordinary users of telecommunications services to provide identification as a condition of service. The fact that the mandate is imposed on providers rather than directly on subscribers does not change its practical effect: no identification, no service.

I am one of the earliest and best known developers of the Bitcoin protocol. As a result I am frequently asked about security and privacy advice by people who own Bitcoin, both regarding cryptocurrency-specific risks they may face as well as the background privacy and security concerns that brought them to Bitcoin in the first place.

I. The Security and Privacy Harms of Mandatory Identification

Many of the people I advise are concerned about the frequent kidnapping and torture of people known to own significant amounts of wealth. Due to previous data breaches — in some cases by employees of national tax agencies — criminals already have significant target lists to work from, and need only know where their prospective victims will be physically located and exposed in order to commit their heinous crimes.

It is the perception of relative wealth, not necessarily actual wealth, that amplifies the risk. Someone may hold only modest assets yet be believed to be far wealthier, and criminals act on what they believe. To the extent this is a danger even for those with the most means to protect themselves, it is worse for everyone else, who lacks the resources to hire security, relocate, or absorb a loss.

A key piece of advice I typically provide is the use of a non-identifying prepaid telephone. The reason for this is that a mobile phone is an always-on tracking device and the tracking nature is inherent in its operation, so the only mitigation available is to avoid connecting the phone's identity with other information that might allow targeting.

Although providers often provide privacy assurances, these assurances are meaningless. They routinely violate their policies with impunity, at most suffering infrequent regulatory fines that are commercially insignificant, and have legal resources that make civil action by private individuals largely futile, even where civil recourse for privacy harms exists, which it usually does not. Even if the provider itself doesn't intentionally share this information, they are routinely breached by hackers and leak information, again with general impunity.

The scale of these breaches is not hypothetical. T-Mobile has repeatedly disclosed significant data security incidents since 2015, including a 2021 breach affecting approximately 76.6 million people and a January 2023 breach affecting approximately 37 million customers, exploited through a vulnerable API [1]. The FCC itself reached a $31.5 million settlement with T-Mobile for these failures — a modest sanction for a carrier with well over 100 million subscribers and one that did nothing to recover the exposed data [2]. In 2024, AT&T disclosed that hackers had stolen the phone records of nearly all of its current and former customers — approximately 110 million people — through a third-party cloud platform [3]. These are not isolated incidents but a recurring pattern across the industry. The occasional fine is just a cost of doing business, and it arrives only after the information has already escaped.

The proposed rule would make this problem far worse. It would require providers to collect and retain, for four years following termination of the customer relationship, the name, physical address, government-issued identification number, and other sensitive personally identifiable information of every customer. This mandate would create a vast, centralized repository of high-value personal data across hundreds of providers — many of them small entities with limited security resources — each of which becomes a target. The FCC's own data shows that the largest, best-resourced carriers in the country cannot keep this kind of data secure. Requiring providers to hold it for years after customers leave is a data breach waiting to happen. Long retention also increases the risk that the data is acquired in an insolvency where even the limited contractual protections may be stripped. The irony is bitter: a rule proposed to protect consumers would expose them to precisely the kind of identity theft and targeting it claims to prevent.

Furthermore, mechanisms for law enforcement or the courts to access customer records are easily and frequently abused by criminals impersonating law enforcement, bribing insiders to obtain access, or abusing the process of overworked courts to obtain orders through sham cases — or in the all too frequent occurrence of the law enforcement officer being a criminal themselves. Criminals, including domestic abusers, will also often impersonate the victim themselves or pretend to be a concerned family member to get access to private information on their accounts and services.

Worse, because it's generally invisible when your privacy has been violated, you cannot take corrective action such as changing locations or adopting better security in response to a compromise. The risk-mitigating posture is to assume that anything which could be disclosed has been. Because of this the only way to be secure is to not share information you don't want leaked in the first place.

II. Harm to Vulnerable Populations

The harm from eliminating anonymous access to telecommunications falls hardest on those who are already vulnerable. Domestic violence organizations routinely advise survivors to use prepaid or "burner" phones to communicate with support services, shelters, and legal resources, because abusers monitor shared phone plans and can access call logs through family billing arrangements [4]. The FCC itself recognized this problem when it adopted rules in 2023 to protect domestic violence survivors' cell phone access on family plans [5]. Eliminating anonymous prepaid service would strip survivors of a critical safety tool.

Journalists communicating with confidential sources, whistleblowers reporting fraud or abuse, and political activists organizing under repressive regimes all depend on the ability to communicate without their identity being linked to their telecommunications usage. The Supreme Court recognized the vital relationship between free association and privacy in NAACP v. Alabama, 357 U.S. 449 (1958), holding that the NAACP could not be compelled to disclose its membership lists because of the danger to which losing anonymity would expose its members [6]. The proposed rule would achieve through regulation what Alabama could not achieve through litigation: the forced identification of everyone who seeks to use the telephone network.

Many essential services require a phone nowadays, including government services and medical devices whose use is hardly optional, and they can only be used privately if you have not provided your personal information to your phone carrier. Many websites now require people to link a mobile device to their online accounts, so in a very real sense your ability to speak online is tied to your mobile device.

The Commission also asks whether to exclude virtual addresses, P.O. boxes, and mail forwarding services as inadequate for identity verification. This would harm remote workers, small businesses, nomadic populations, and people without fixed housing — all of whom may legitimately use these services. I use a virtual address myself. Excluding these options would not stop criminals, who can provide a real address they have no connection to, but would exclude legitimate customers with valid reasons for not maintaining a traditional physical address.

The Commission might respond to these concerns by carving out exemptions for recognized vulnerable groups. This approach is dangerous and wrongheaded. Government recognition of vulnerable parties is at best eventual; from a current perspective we can see that past standards have not been good — full recognition of domestic abuse as a crime is itself a modern development. The only credible authority on a person's vulnerability is the person themselves, and the only person who can assure a person's

safety is themselves: no one else has the obligation, no one else has as great an interest in doing so. People will protect themselves, but only if they are not prohibited the tools to do so. Moreover, any process for identifying a person as vulnerable would inevitably require the collection of more personal information — proof of abuse, shelter address, protective order — which could itself be used to target or harm them.

III. The First Amendment Right to Anonymous Speech

The United States owes its very existence to the ability of the founders of the nation to publish their political views anonymously, such as in The Federalist Papers. The Supreme Court has repeatedly and explicitly recognized that the right to anonymous and pseudonymous speech is inherent in the First Amendment. In Talley v. California, 362 U.S. 60 (1960), the Court struck down an ordinance requiring identification on handbills, noting that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance" [7]. In McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995), the Court held that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment" [8].

Because mandatory identification burdens the right to speak anonymously — a right the Supreme Court has recognized as inherent in the First Amendment — any rule that conditions telephone access on identification must satisfy strict scrutiny: it must serve a compelling government interest and be the least restrictive means of achieving that interest.

But as a practical matter this freedom is sharply curtailed, if not practically eliminated, for those who cannot access modern telecommunications networks with relative anonymity. When phone numbers are required to register for online services, participate in social media, or access government databases and regulatory filings, the anonymity of one's phone service is the foundation upon which all other anonymity rests. The Commission itself lists "political campaign" as an example of a high-volume use that triggers enhanced information collection [9a]. Political speech receives the highest First Amendment protection, yet the rulemaking considers no protection for this category. Political advocacy would be deemed "risky" by design. A requirement to present government identification to access the communications network makes a right to anonymous speech a right in name only.

IV. Routing Around the Fourth Amendment

The government could not directly compel every American to register their identity and home address with a federal agency as a condition of using the telephone. The Fourth Amendment would not tolerate it. But the proposed rule achieves substantially the same result by mandating that providers collect and retain this information, where it becomes accessible to law enforcement and intelligence agencies through processes that carry far less constitutional protection than a direct demand would.

This works because of the third-party doctrine: under the Supreme Court's precedent, information shared with a company receives diminished Fourth Amendment protection, on the theory that you "voluntarily" disclosed it. But that voluntary premise collapses when the government is the reason the information is collected in the first place. A disclosure the government compels as a condition of accessing the communications network is not voluntary in any meaningful sense. The Supreme Court recognized this dynamic in Carpenter v. United States, 585 U.S. 296 (2018), holding that cell-site location information retains Fourth Amendment protection despite being held by a third party, because carrying a phone is not a genuinely voluntary choice in modern society [18]. The same logic applies to identification mandates: if the government makes identification a condition of telephone access, the resulting disclosure is no more "voluntary" than the location data at issue in Carpenter. The rule places sensitive personal data — government identification numbers, physical addresses, call patterns — in a zone where the Fourth Amendment offers the least protection, and where provider data breaches and abuse of process can reach it with little oversight. The Commission must not construct a universal identification regime that routes around the constitutional constraints that would apply if it collected this information directly.

V. The Commission Lacks Authority to Impose Such a Requirement

The Commission identifies sections 201(b), 227(e), and 251(e) of the Communications Act, the Truth in Caller ID Act, and national security authority as possible bases for this rulemaking. None of these authorities gives the Commission general power to condition ordinary access to the communications network on government identification. Authority to prevent illegal robocalls, caller-ID spoofing, or abuse of numbering resources is not authority to burden the First Amendment right to speak anonymously by requiring identification from everyone who seeks ordinary telecommunications service.

Nor does the Commission's national security authority support this rulemaking. The Commission points to its statutory duty to "make available . . . a rapid, efficient, Nation-wide and world-wide wire and radio communication service . . . for the purpose of the national defense." 47 U.S.C. § 151. Making communication service available to the public is the opposite of conditioning access on government identification. The Commission cites no precedent for reading this general-purpose grant as authority to require identification from domestic users of communications services, and for good reason: Congress has never authorized the Commission to operate a domestic identity verification regime. The national security argument cuts the other way. Requiring every provider to collect and retain government identification creates a concentrated target that foreign intelligence services would seek to compromise — a breach of a single provider's KYC database could expose the real identities and home addresses of government officials, military personnel, and law enforcement officers, the importance of which to national security should be clear even to someone who disregards the security and privacy of ordinary Americans.

The Commission's own uncertainty about its authority is evident in its treatment of Section 303(r) and the General Agreement on Trade in Services. Rather than asserting GATS as a basis for rulemaking, the Commission merely asks whether it "might serve as authority." Proposing rules with serious constitutional consequences on the basis of authority the agency itself cannot confirm is not reasoned decisionmaking.

Under the constitutional avoidance canon, an agency must identify clear congressional authorization before adopting rules that burden constitutional rights. Reading general grants of authority over carrier practices, numbering resources, or caller-ID spoofing as permitting the Commission to require government identification from everyone who seeks telephone service is precisely the kind of aggressive statutory construction the avoidance doctrine forbids. The major questions doctrine reinforces this conclusion. In West Virginia v. EPA, 597 U.S. 697 (2022), the Supreme Court held that agencies must point to "clear congressional authorization" for decisions of "vast economic and political significance" [16]. Conditioning access to the telephone network on government identification nationwide is a decision of that magnitude. The Commission's reliance on general grants of authority over carrier practices, numbering resources, and caller-ID spoofing — none of which authorizes a domestic identity verification regime — does not satisfy this standard.

Before adopting a rule with these constitutional consequences, the Commission must at least identify a clear statutory basis and explain why targeted enforcement, traceback, gateway provider enforcement, call authentication, provider-specific penalties, and other narrower measures are inadequate.

VI. The Commission Is Not a Law Enforcement Body

The Commission asks whether enhanced KYC can prevent or deter criminal use of communication networks that goes beyond illegal calls, citing human trafficking and other crimes [9d]. Human trafficking is a serious problem, but it is not specific to telecommunications. If the mere existence of a crime were sufficient to justify FCC action, there would be no limit to the agency's scope or power. The FCC is not a law enforcement body. SIM box fraud is similarly a commercial matter for providers to address through technical detection and contractual enforcement. Nothing prevents providers from requiring identification based on their own risk and market analysis — if a provider loses too much to fraud, it can require more, and other providers can compete on the basis of better policy. That is a commercial decision for providers, not a basis for the government mandating identification of every subscriber.

The Commission repeatedly invokes anti-money-laundering rules as "a good model" for telecom KYC [9a]. The analogy fails. A bank intermediates every transaction: it sees the sender, the recipient, and the amount, and it can freeze funds or block transfers. A telephone provider is not a transaction intermediary — it provides infrastructure. The provider cannot see the content of calls, does not know who is being called in any meaningful sense beyond routing numbers, and cannot selectively block individual calls without becoming the kind of surveillance intermediary the Fourth Amendment was designed to prevent.

Even on its own terms the model does not work. By the UN Office on Drugs and Crime's own assessment, less than one percent of global illicit financial flows are seized and frozen [14]. Decades of increasingly stringent AML rules have created enormous compliance costs and privacy harms while failing to meaningfully reduce money laundering, much less meaningful crime. This is not a model to emulate.

VII. The Cryptocurrency Payment Red Flag

The proposed rule lists "paying for service in non-traceable ways such as the use of cryptocurrency" as a red flag that should trigger enhanced verification [9b]. This is discriminatory and unfounded. Cryptocurrency is a legitimate payment method used by millions of Americans and particularly by at-risk persons trying to avoid the privacy problems inherent in other popular forms of electronic payment. Treating its use as presumptively suspicious is equivalent to saying that use of cash implies criminal intent. The premise is also technically wrong as stated: many cryptocurrency

transactions are publicly traceable, while stolen cards and mule accounts are commonly available to criminals.

As someone who has worked in this field for over a decade, I can attest that the use of cryptocurrency says nothing about a person's intent to make illegal calls. Criminal actors use whatever means are most available, which sometimes involves cryptocurrency but more often does not. Criminals have numerous alternatives such as bribery or stolen identities that allow them to bypass privacy-violating requirements in ways that lawful actors cannot.

The proposed red flag would subject legitimate customers who value financial privacy to heightened scrutiny and burden, with no demonstrated connection to illegal robocalling. It would also encourage providers to refuse service to cryptocurrency users entirely, effectively excluding a class of customers from telecommunications access based on their choice of payment method. The Commission must not encode payment-method discrimination into its rules.

VIII. The Forfeiture Penalty Will Drive Over-Compliance

The Commission proposes a $2,500 base forfeiture per call for KYC violations [9c]. This creates potentially catastrophic liability: a single customer making 10,000 illegal calls could expose a provider to $25 million in penalties. Faced with such exposure, providers will not carefully calibrate — they will over-comply. A provider has no incentive to serve any customer who presents even marginal risk when the downside is unbounded forfeiture liability. The result will be a non-transparent and unaccountable discriminatory effect: providers will refuse service to anyone who seems unusual, difficult to verify, or simply not worth the risk — or in other words, not profitable enough to justify the potential liability. This falls hardest on the vulnerable populations described above — survivors of domestic abuse, the unbanked, the unhoused, and anyone whose circumstances do not fit a provider's risk model. The penalty structure makes over-collection and over-screening the only rational business decision, undermining whatever balancing the Commission hopes to achieve. The Commission's proposal to broaden downstream blocking requirements would compound this effect, creating a purity spiral in which each provider in the chain has incentive to block anyone flagged as risky or anyone they suspect an upstream provider would consider risky, excluding marginal customers from the network entirely. Requiring KYC compliance certification as part of Robocall Mitigation Database filings would add yet another lever, pressuring providers to certify compliance under threat of enforcement rather than exercise reasoned judgment about individual customers. The Commission tentatively concludes

that incremental compliance costs will be minimal, but no rule for which unintentional errors could result in millions of dollars in liability could practically be implemented with minimal costs. And even if providers managed a minimal-cost implementation despite the regulatory risks, the public's privacy would be left at the mercy of whatever cheapest implementation a provider could get away with.

The Commission argues that many originating providers already take KYC compliance measures, so any incremental costs will be minimal. Some providers do collect extensive customer information; others do not. That variation is not a gap to be closed — it is the market functioning as it should. Providers that don't require identification serve customers who value privacy, and the providers that do serve customers who prefer the trade-offs that come with identification. The Commission cites the existence of voluntary practices as evidence that a mandate would be cheap. It proves the opposite: the providers that have chosen not to collect this information are the ones whose customers depend on that choice. The freedom and privacy of Americans rest on their ability to choose a provider whose practices match their own judgment about their security — a choice the Commission seeks to take away.

The over-compliance machinery this rule creates is also a ready-made channel for political censorship. Providers need not wait for direct government instruction to cut off a disfavored speaker — the forfeiture structure already makes it irrational to serve anyone deemed "risky," and "risky" can be defined to include those whose speech attracts regulatory attention. Providers will anticipate what pleases their regulators, and no direct order is needed. Congress has recognized this danger: the JAWBONE Act, introduced with bipartisan support in June 2026, would create a cause of action against government agencies that pressure private companies to suppress protected speech [17]. But remediation after the fact is no substitute for avoiding excessive regulatory influence in the first place. The problem is especially acute because many domestic mass phone callers today are political activists, whose speech receives the highest First Amendment protection. A rule that treats high-volume political calling as a compliance risk gives providers every reason to avoid serving such speakers.

IX. Safe Harbor Would Worsen the Problem

The Commission asks whether KYC compliance should constitute a safe harbor from enforcement, and whether using accredited third parties or AI systems should trigger such protection [9c]. This would make matters worse. Third-party verification routes sensitive PII through yet another entity, expanding the attack surface for breaches without any demonstrated improvement in security. Safe harbor for AI-based

KYC would encourage providers to adopt opaque algorithmic systems that decide who gets telephone service — with no transparency, no accountability, and predictable disparate impact on the populations least able to challenge a machine's decision. A safe harbor incentivizes over-collection and over-compliance to gain legal protection, turning the rule into a liability shield that serves the provider's interests rather than any safety purpose.

X. The Proposal Would Be Ineffective

The Commission uses "illegal calls" to encompass criminal fraud, civil regulatory violations, and calls that are merely unwanted. Conflating these categories borrows the urgency of criminal enforcement to justify measures that reach far beyond it. This comment does not parse every category, but the Commission should not assume that rules calibrated for wire fraud are proportionate when applied to political speech or legitimate business calling.

I share the Commission's concerns about spam and scam phone calls and messages. However, this rulemaking would be unlikely to make a meaningful impact. The FTC has acknowledged that "a significant proportion, if not the majority, of illegal robocalls originate from overseas" [10]. The FTC's own enforcement strategy targets domestic gateway providers that route this traffic — a focused approach that addresses the problem at its choke point without requiring identification of every subscriber.

Faced with the uncomfortable fact that most of the illegal activity originates outside of its jurisdiction, the Commission also asks whether foreign customers use domestic U.S. providers to originate calls, and proposes to extend KYC requirements to them. This is practically incoherent. The proposed requirements — government-issued identification, physical address verification, supporting records — assume a domestic identity infrastructure. A U.S. provider cannot verify the authenticity of identification documents issued by foreign governments, which use hundreds of different formats and verification systems with no global interoperability standard. At the same time, many foreign jurisdictions impose privacy restrictions on the collection and retention of national identification data that directly conflict with the Commission's proposed four-year retention mandate. The result is that KYC for foreign customers is either unworkable or a formality — either way, it does nothing to stop determined scammers.

Over 160 countries already require mandatory SIM card registration, [13] yet illegal robocalling persists as a global problem. But even if every jurisdiction adopted equally stringent KYC, criminals would not be meaningfully stopped: they would steal identities, compromise telecom providers, establish corrupt ones, or bribe insiders.

Identity requirements deter only those who have something to lose by being identified, and criminals already engaged in fraud have crossed that threshold.

India provides an instructive example. India requires KYC verification for all SIM card activations — though its Supreme Court struck down the mandatory biometric (Aadhaar) requirement in 2018 [15] — yet it continues to battle massive cyber fraud, with one report estimating broader cyber-fraud losses at over $113 billion [11]. The Department of Telecommunications has identified and disconnected more than 7 million fraudulent SIMs — demonstrating that even active enforcement has to chase criminals after they have already adapted. Worse, the KYC requirement itself spawned a new category of crime: "fake KYC verification scams" in which criminals impersonate telecom representatives to collect sensitive personal data under the guise of mandatory compliance updates [11]. The KYC mandate did not eliminate fraud; it created new opportunities for it.

This shouldn't be surprising. Against an identity requirement, an attacker will simply use the most expedient mechanism available. They might go to poor communities or homeless shelters and pay people a few dollars to use their identities — something that already happens today — or, given that they're already criminals, simply use any of the tens of millions of stolen identities already circulating from the very data breaches described above, where Social Security numbers have recently been reported for sale for $1 to $6 on dark web markets [12]. The proposed rule could not be more effective than requiring a few dollars in additional setup costs for anonymous accounts. Worse, it might potentially expand the market for identity theft and result in more people being victimized and in ways far worse than a nuisance phone call.

Even on the Commission's own theory, mandatory identification is not the least restrictive means available. A requirement that non-identifying accounts post a bond would raise the cost of anonymous access — the same deterrent effect the Commission seeks — without compelling every subscriber to surrender government identification. I do not advocate this approach, but it demonstrates that the proposed rule fails the least-restrictive-means test.

XI. Conclusion

Given the serious harm to the public's security, privacy, and legally protected right of free speech, such a measure could not be justified unless it were both highly effective and the least restrictive means available. It is obvious that it is neither. The rule would impose significant burdens on legitimate users — particularly the most vulnerable — while failing to meaningfully stop scam calls, especially the overseas-originated traffic that drives much of the problem, and creating new vectors for identity theft. The Commission should abandon this proceeding.

Respectfully submitted,

Gregory Maxwell
Rapid City, South Dakota
June 25, 2026

References

[1] T-Mobile Data Breach History, Security.org, https://www.security.org/identity-theft/breach/t-mobile/; see also Wikipedia, T-Mobile data breach, https://en.wikipedia.org/wiki/T-Mobile_data_breach

[2] FCC, "T-Mobile Required to Change Business Practices After Data Breaches," Consent Decree, DA-24-860, released September 30, 2024, https://www.fcc.gov/document/t-mobile-required-change-business-practices-after-data-breaches-0; Consent Decree, https://docs.fcc.gov/public/attachments/DA-24-860A1.pdf

[3] AT&T Inc., Form 8-K, filed with the SEC, July 12, 2024, https://www.sec.gov/Archives/edgar/data/732717/000073271724000046/t-20240506.htm; see also Mozilla Foundation, "What You Need to Know About AT&T's Huge Data Breach," https://www.mozillafoundation.org/en/privacynotincluded/articles/att-had-a-huge-data-breach-heres-what-you-need-to-know/; Security.org, "AT&T Data Breach: What Happened and What to Do," https://www.security.org/identity-theft/breach/att/

[4] Pathways to Safety, "Staying Safe," https://pathwaystosafety.org/staying-safe/; Safety Net Project, "Cell Phone Safety Plan," https://www.techsafety.org/resources-survivors/cell-phone-safety-plan

[5] FCC, "FCC Adopts Rules Implementing the Safe Connections Act for Survivors of Domestic Abuse," Report and Order, released November 2023, https://www.fcc.gov/consumer-governmental-affairs/fcc-adopts-rules-implementing-safe-connections-act-survivors-domestic-abuse; Federal Register, "Supporting Survivors of Domestic and Sexual Violence; Lifeline and Link Up Reform Modernization," 88 Fed. Reg. 84296, Dec. 5, 2023, https://www.federalregister.gov/documents/2023/12/05/2023-25835/supporting-survivors-of-domestic-and-sexual-violence-lifeline-and-link-up-reform-modernization

[6] NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958), https://www.law.cornell.edu/supremecourt/text/357/449

[7] Talley v. California, 362 U.S. 60 (1960), https://www.law.cornell.edu/supremecourt/text/362/60

[8] McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995), https://www.law.cornell.edu/supct/html/93-986.ZO.html

[9a] FCC 26-27, FNPRM, CG Docket Nos. 17-59 and 02-278, section I.A: "marketing, education, political campaign) and the customer's IP address from which each call will be placed"; and "Gathering such information is the standard to prevent money laundering, and given the misuse of networks by bad actors such as organized criminal groups, we believe it provides a good model for our work."

[9b] FCC 26-27, FNPRM, CG Docket Nos. 17-59 and 02-278, section I.B: "paying for service in non-traceable ways such as the use of cryptocurrency."

[9c] FCC 26-27, FNPRM, CG Docket Nos. 17-59 and 02-278, section I.C: "we propose to codify a $2,500 per call base forfeiture amount"; and "should we deem compliance with any enhanced KYC obligations or baseline KYC expectations a safe harbor from any enforcement action against the originating provider?"

[9d] FCC 26-27, FNPRM, CG Docket Nos. 17-59 and 02-278, section I.D: "We seek comment on whether enhanced KYC requirements can prevent or deter criminal use of communication networks that do not involve illegal calls."

[10] "FTC Ramps Up Fight to Close the Door on Illegal Robocalls Originating from Overseas Scammers and Imposters," FTC Press Release, April 2023, https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters

[11] "India Battles Rising SIM Card Scams as Fraud Losses Hit $113.3 Billion," Mobile ID World, https://mobileidworld.com/india-battles-rising-sim-card-scams-as-fraud-losses-hit-113-3-billion/

[12] "Dark Web Data Pricing 2025: Real Costs of Stolen Data," DeepStrike, https://deepstrike.io/blog/dark-web-data-pricing-2025; see also PCMag, "Here's How Much Your Identity Goes for on the Dark Web," https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web; Frank on Fraud, "Social Security Numbers Only Cost $4 On The Dark Web," https://frankonfraud.com/social-security-numbers-only-cost-4-on-the-dark-web/

[13] Comparitech, "Which governments impose SIM-card registration laws to collect data on their citizens?" https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/

[14] UN Office on Drugs and Crime, "Money Laundering" factsheet, https://www.unodc.org/documents/hlr/FactSheets/Money_Laundering.pdf

[15] Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India, decided September 26, 2018 (striking down Section 57 of the Aadhaar Act, which had permitted mandatory biometric authentication by private entities including telecom providers), https://indiankanoon.org/doc/127517806/; see also Supreme Court Observer, "Constitutionality of Aadhaar Act: Judgment Summary," https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/

[16] West Virginia v. Environmental Protection Agency, 597 U.S. 697 (2022), https://www.law.cornell.edu/supremecourt/text/20-1530

[17] "Cruz, Wyden Introduce Legislation to Guard First Amendment Speech Rights Against Government Jawboning," U.S. Senate Commerce Committee, June 11, 2026, https://www.commerce.senate.gov/press/rep/release/cruz-wyden-introduce-legislation-to-guard-first-amendment-speech-rights-against-government-jawboning/

[18] Carpenter v. United States, 585 U.S. 296 (2018), https://www.law.cornell.edu/supremecourt/text/16-402