

July 27, 2026

Marlene H. Dortch, Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Via ECFS

Re: FNPRM on Know Your Customer Requirements

Dear Secretary Dortch:

The undersigned organizations urge the Commission not to impose a government mandate for phone providers to collect identity documents from all subscribers. This [proposal](#) seeks to expand the agency's Know Your Customer (KYC) requirements by imposing a requirement to "at a minimum, obtain and retain the name, physical address, government issued identification number, and an alternate telephone number of any new and renewing customer." While we support the Commission's efforts to reduce illegal robocalls, conditioning phone access on providing identity documentation would impose severe privacy harms on all phone subscribers, and cut off vulnerable populations that lack these documents from an essential service, which has become a [lifeline](#) for most Americans.

Mandatory identity collection from every subscriber would represent a significant and unreasonable expansion of existing know your customer rules for providers. This presents a serious privacy violation, as customers are subject to more data collection and retention, opening up opportunities for bad actors to access, misuse, or exploit that information through data breaches, unauthorized sales, or law enforcement overreach.

Beyond creating acute privacy risks for all subscribers, the proposal would endanger anonymous communications that have long protected whistleblowers, activists, journalists, and domestic violence survivors. A survivor of domestic violence fleeing an abuser should not have to create a record that leads back to their door in order to get a phone. Nor should a whistleblower or a survivor escaping a trafficking situation. Further, the FCC is responsible for protecting privacy of customer information through its telecom privacy provisions and laws like the [Safe Connections Act](#). This proposal undercuts those protections.

The proposal would impose significant barriers to obtaining phone service for vulnerable populations who cannot provide specific identifiers. Requiring [government ID](#), an [alternative telephone number](#), and a [physical address](#) as conditions of service would cut off unhoused individuals, low-income Americans, older adults, foster youth, and survivors of intimate partner violence from this critical form of communication. Further, the very populations that lack these identifiers are the ones who are also the most likely to switch services and disproportionately

rely on prepaid plans, meaning these burdens would primarily fall on the populations least able to comply for the service they most depend on.¹

The privacy risks of providing this information to carriers are not abstract, as phone companies have a [lackluster history](#) with protecting private data. All four major carriers shared customer location data with data brokers contrary to telecom [privacy law](#), ultimately reaching third parties like bounty hunters and bail bondsmen. Major carriers have also suffered repeated large-scale breaches exposing sensitive personal information. In 2021, a [T-Mobile](#) breach exposed the Social Security numbers and driver's license numbers of approximately 77 million people and, in 2024, an [AT&T](#) breach exposed the call and text records of nearly all its wireless customers (roughly 110 million subscribers). Mandating that thousands of originating providers, including small carriers with limited resources to protect the privacy and security of such an extensive amount of information, collect and retain government IDs for the life of the customer relationship plus four years creates significant new exposure.

These consumer costs would be difficult to justify even if the proposal were likely to make a meaningful impact in solving the robocall problem, but the Commission has not demonstrated that it would. The FTC recently [found](#) that “a significant proportion, if not the majority, of illegal robocalls originate from overseas.” Both the FTC and the Department of Justice have consistently said that the most harmful scam operations already use [stolen identities](#) and [foreign intermediaries](#) that may still not be caught by the new proposed requirements. Meanwhile, less than 45% of telecom companies have adopted the [STIR/SHAKEN](#) standards. The Commission should prioritize full deployment of existing, less privacy-invasive tools before mandating universal identity collection of unproven efficacy.

A government-mandated requirement for every American to surrender their privacy or go without a phone is not a proportional or advisable response. The Commission has not demonstrated that universal identity collection would meaningfully reduce illegal calls, yet the proposal would conscript every phone subscriber in the country into a forced data collection regime.

Several of the undersigned organizations have addressed these issues in greater detail in their individual comments filed in this proceeding. If you have any questions about this letter, please contact Sydney Saubestre at ssaubestre@cdt.org or Alan Butler at butler@epic.org.

Signed,

Access Now
American Civil Liberties Union

¹ The Commission's enforcement record has consistently targeted VoIP service providers, gateway carriers, and bulk access operators as the sources of illegal robocall traffic, not individual retail prepaid subscribers, and providers of retail prepaid service should be given more flexibility in what identifying information they collect and retain. See, e.g., FCC, FCC Cuts Off Provider for Violating Robocall Rules (Mar. 12, 2026); FTC, Project Point of No Entry (Apr. 2023).

Cape
Center for Democracy & Technology
Center for Digital Democracy
Consumer Federation of America
Defending Rights & Dissent
Demand Progress Education Fund
Electronic Frontier Foundation
Electronic Privacy Information Center
National Network to End Domestic Violence
New America's Open Technology Institute
Privacy Rights Clearinghouse
Radio Television Digital News Association
Restore The Fourth Action
Society of Environmental Journalists
The Leadership Conference on Civil and Human Rights
United Church of Christ Media Justice Ministry