Congress of the United States

Washington, DC 20515

August 26, 2026

Orice W. Brown
Acting Comptroller General
U.S. Government Accountability Office
441 G Street NW
Washington, D.C. 20548

Dear Acting Comptroller General Brown:

We write to urge the Government Accountability Office to investigate the Department of Transportation's (DOT) systemic failure to protect passenger privacy using its authority to regulate the practices of commercial airlines and ticket agents. Although DOT has had sole authority to safeguard passenger data for over 40 years, DOT has never taken a single enforcement action related to privacy. That inaction is despite numerous widely-publicized privacy disasters impacting hundreds of millions of travelers.

DOT's abdication of its role as a privacy regulator has left the sensitive personal information of hundreds of millions of Americans exposed to corporate exploitation, warrantless government surveillance, and warrantless seizure of money and other property. In addition to harming the public, DOT's regulatory inaction also potentially threatens national security. Travel data held by airlines and travel agencies may be of interest to foreign adversaries, who could exploit such information to track U.S. military, diplomatic, and other U.S. government personnel.

Congress explicitly carved airlines out of the Federal Trade Commission's authority over unfair and deceptive practices and handed it exclusively to the DOT. But Congress also modeled DOT's authority to police unfair and deceptive practices on the FTC's authority. Over the past thirty years, the FTC has repeatedly brought successful enforcement actions against lax cybersecurity and privacy practices. Today, it is clear that such practices are unfair and deceptive. In contrast, during the four decades that DOT has had the sole authority to police airlines, a Congressional Research Service review found no instance of it taking a public enforcement action or issuing civil penalties regarding consumer privacy violations.

DOT told the European Commission in a public 2023 letter that the agency "received relatively few complaints involving alleged privacy violations by ticket agents or airlines. When they arise, they are investigated." But effective regulators do not sit back and wait for consumer complaints; they proactively audit companies subject to their jurisdiction. Government watchdogs proactively inspect countless industries, including banks, nuclear plants, slaughterhouses, and pharmaceutical labs. These other agencies have focused on preventing systemic failures before they harm the public, recognizing that the most severe risks are often invisible to the average consumer.

This regulatory passivity appeared to shift under the last Administration, following an investigation by Senator Wyden. On March 21, 2024, then-Secretary Buttigieg announced that DOT had begun the first industry-wide privacy review of the nation's ten largest airlines. According to that announcement, the Office of Aviation Consumer Protection sent letters to major airlines, seeking information about their privacy practices. Yet, more than two years after this announcement, it remains entirely unclear whether a

meaningful review ever took place. The response letters were never made public, and DOT failed to announce any public findings, release a report, or pursue any subsequent public enforcement actions against non-compliant carriers. Moreover, DOT appears to have abandoned this effort since Donald Trump took office, and has not announced any additional privacy reviews.

The consequences of DOT's regulatory neglect are vividly illustrated by the severe privacy abuses occurring within its jurisdiction. For years, a data broker collectively owned by major U.S. airlines, the Airline Reporting Corporation (ARC), sold access to a massive database containing roughly 722 million passenger travel records to federal agencies, including the Department of Homeland Security (DHS) and the Internal Revenue Service, without warrants or judicial oversight. Following bipartisan congressional scrutiny and public backlash, ARC finally shuttered this invasive travel surveillance program in November 2025. However, earlier this year, DHS issued a public request to government contractors for a replacement airline passenger surveillance system.

Furthermore, a 2016 Department of Justice (DOJ) OIG audit revealed that the Drug Enforcement Administration (DEA) has for years bribed airline employees millions of dollars to covertly siphon off Americans' private data. The OIG review found that the DEA was paying at least 19 airline employees, who "provided DEA Special Agents with passenger travel information including itinerary information, ticket purchase information, baggage information, origin and destination airports, connecting flights, dates of birth, flight numbers, and seat numbers." According to the OIG report, these airline employees were providing the DEA with passenger information "on a near daily basis." The OIG warned that these extra-judicial practices likely violated Americans' Fourth Amendment protections against unreasonable searches and seizures—an abuse left unchecked because the DOT failed to proactively police the privacy practices of the companies it regulates.

The DEA used this passenger data to identify travelers who would then be approached before boarding their flight and pressured to consent to a search of their bags. If passengers refused, they could be detained until they missed their flight. The DEA's goal was to identify passengers carrying large amounts of cash, which agency personnel could then seize without arresting the passenger or charging them with a crime.

According to a 2024 follow-up review by the DOJ OIG, nearly a decade after the practice was first publicly identified by the OIG, the DEA is still paying airline employees for passenger records. The OIG cited an example of an airline employee who had for years been paid by the DEA to share information from the airline's reservation system identifying passengers who purchased last-minute tickets. The systemic theft of passenger data by rogue employees constitutes a severe, decade-long data breach facilitated by a total failure to manage insider threats. Airlines and travel companies inflict substantial, unavoidable injury on travelers when their failure to implement basic cybersecurity protections and access-log monitoring exposes passengers to warrantless surveillance, harassment by agents and illegal seizures of their assets by the government. By ignoring this systemic lack of internal data controls and failing to treat unauthorized corporate insider data exfiltration as an ongoing cybersecurity failure, the DOT has completely failed to protect the flying public.

DOT's regulatory failure also carries severe international and economic ramifications, specifically threatening the viability of the EU-U.S. Data Privacy Framework (DPF). In a July 2023 commitment letter to the European Commission, the DOT formally pledged to vigorously enforce DPF principles, prioritize

investigations into data violations, and publish enforcement orders to protect EU consumers. This framework is critical because it allows U.S. businesses to conduct essential commercial operations within the global economy while guaranteeing international data protections. If the DOT continues to neglect its domestic regulatory obligations, it risks undermining the integrity of this entire agreement, potentially collapsing transatlantic data flows and destroying vital economic benefits for U.S. companies.

Therefore, we request that GAO launch a formal, comprehensive investigation into the DOT's systemic abdication of its consumer privacy enforcement mandates. To ensure a thorough review, your investigation should specifically address and answer the following questions:

1. **Status of the 2024 Airline Privacy Review:** Provide a full accounting of the status, findings, and disposition of the industry-wide review launched on March 21, 2024. To what extent did major carriers submit responses to the Office of Aviation Consumer Protection (OACP)? If responses were collected, what are DOT's plans to publicly release the findings?

2. **Audit of Agency Personnel and Technical Expertise:** Identify the exact number of full-time personnel within the OACP currently dedicated exclusively to privacy enforcement, including the number of technologists. Does the DOT possess the internal expertise to effectively protect consumers from privacy harms?

3. **Audit of Interagency Coordination on DEA Informants:** Review the interagency coordination between DOT and the Department of Justice regarding airline employees acting as paid DEA informants to establish a precise timeline of this interagency outreach, identify any periods of administrative delay, and determine what concrete actions the DOT took—or failed to take—to secure information from the DOJ and hold non-compliant carriers accountable. The review should include communications, meeting logs, and formal inquiries between the agencies.

4. **Agency Response to Widespread Public Scandals:** Evaluate whether the DOT or OACP opened any independent, self-initiated investigations or compliance reviews following the widespread media coverage of ARC's sale of bulk passenger records to the government. Determine if the DOT took any proactive measures to investigate this practice, or if it remained entirely passive until Congressional pressure and bad press forced the program's closure in November 2025.

5. **Structural Nature of the Complaint-Driven Model:** Assess the structural nature of the DOT's passive, complaint-driven oversight model. Why has the DOT chosen such structure instead of a regime of proactive, routine technical privacy audits—similar to its approach to physical aviation safety—and what statutory or administrative barriers, if any, prevent the agency from utilizing its statutory civil penalty authority to address data practices deemed by DOT to be unfair and deceptive under 49 U.S.C. § 41712?

6. **Assessment of Insider Threat Mitigation and Data Governance:** Evaluate whether the DOT has established guidelines regarding airlines' protection of Passenger Name Record (PNR) databases against insider threats.

7. **International Data Commitments:** Identify and explain DOT's rationale of how DOT's domestic public privacy enforcement approach since July 2023 is consistent with formal compliance pledges

the agency made to the European Commission to sustain the EU-U.S. Data Privacy Framework (DPF).

Finally, we request that your office provide legislative recommendations to address the DOT's inaction and compel the agency to more vigorously protect the privacy rights of travelers, including any legislative changes required to remove obstacles to enforcement.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Shontel M. Brown
Member of Congress

CC: The Honorable Sean Duffy, Secretary of Transportation
The Honorable Howard Lutnick, Secretary of Commerce
The Honorable Sean Cairncross, National Cyber Director