



**UNITED STATES OF AMERICA
DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY
WASHINGTON, D.C.**

Issued by the Department of Transportation
on the 7th day of March, 2005

Third-Party Enforcement Complaint of

**THE ELECTRONIC PRIVACY
INFORMATION CENTER**

against

NORTHWEST AIRLINES, INC.

Alleging Violation of 49 U.S.C. § 41712

Docket OST-2004-16939-14

Served March 7, 2005

ORDER AFFIRMING DISMISSAL OF COMPLAINT

SUMMARY

This order affirms Order 2004-9-13 ("Order"), dismissing the complaint filed by the Electronic Privacy Information Center ("EPIC"), and responds to EPIC's petition for review filed September 20, 2004.

BACKGROUND

On January 20, 2004, EPIC filed a third-party complaint, later joined by the Minnesota Civil Liberties Union ("MnCLU"), against Northwest Airlines, Inc. ("Northwest"). *See* Docket OST-2004-16939. The complaint alleged that Northwest's privacy policy, as published on its website, constituted an unfair or deceptive practice in violation of 49 U.S.C. § 41712, due to the carrier's transfer of a sample of passenger data to the National Aeronautics and Space Administration ("NASA") in December 2001.

The complaint alleged that Northwest violated its own published privacy policy when it shared Passenger Name Record ("PNR") data with government researchers at NASA's Ames Research Center ("ARC") in December 2001. According to the complaint, this violation constituted an unfair or deceptive practice in violation of 49 U.S.C. § 41712.

After reviewing the complaint, Northwest's answer, and supplemental briefing by EPIC, Northwest, and a letter from MnCLU that largely echoed the assertions made by EPIC

in the original complaint, the Assistant General Counsel for Aviation Enforcement and Proceedings (“Enforcement Office”) issued Order 2004-9-13 declining to initiate a formal enforcement proceeding and dismissing the complaint. The Enforcement Office concluded that the language of Northwest’s privacy policy did not expressly declare that the carrier would not share passenger data with government researchers. In addition, the Enforcement Office found that Northwest’s conduct, comprising its published privacy policy, public statements, and efforts to work with ARC in developing improved passenger pre-screening technologies in the immediate aftermath of the terrorist attacks of September 11, 2001, did not deceive its customers. The Enforcement Office noted that no evidence of actual or likely harm to consumers had been presented by EPIC or MnCLU, and consequently found that it would not be in the public interest to pursue an enforcement action in this case.

Although the Department’s rules do not specifically provide for review of such dismissal orders, EPIC filed a petition for review on September 20, 2004. As a matter of discretion, we are accepting the pleading as a petition for review of staff action under 14 CFR 385.30 *et seq.*

PLEADINGS AND ANSWERS

In its petition for review, EPIC offers various arguments why it believes that the Enforcement Office’s findings were erroneous. Specifically, EPIC asserts that:

1. The Order applied the wrong test for determining whether a violation of §41712 had occurred. Specifically, EPIC asserts that the Order “ignores the established analysis for deceptive trade practices,” and “engage[s] in a contrived ends-oriented interpretation of [Northwest’s] privacy policy that is inconsistent with relevant precedent and the reasonable consumer test.”
2. The Order misconstrues EPIC’s complaint, as EPIC “did not argue that [Northwest’s] privacy policy would preclude it from providing customer data to the government if required to do so by law.” EPIC reasserts that it is the “absence of a legal process supported by a judicial determination” that renders Northwest’s decision to share passenger data with NASA a violation of §41712.
3. The Order incorrectly cites the absence of “significant” consumer harm as determinative of the Enforcement Office’s decision not to initiate formal enforcement proceedings. EPIC asserts that “the dissemination of customer’s sensitive personal information without their knowledge or consent” is, *ipso facto*, actual harm.
4. The analysis provided in the Order undermines the Department’s position that “a carrier is bound by the representations it makes to its customers,” because the Order permits Northwest to avoid the consequences of its representations regarding privacy, which were likely to have misled a “reasonable consumer” into believing that the carrier would not share passenger data with the ARC.

FINDINGS

EPIC's petition for review of staff action does not introduce any information or argument not covered in its original complaint or subsequent submissions, and, as with EPIC's submissions *in toto*, fails to offer any evidence that consumers suffered or were likely to suffer harm as a result of Northwest's conduct. With respect to EPIC's specific allegations, we find the following:

1. The Order both stated and applied the correct test for determining whether a violation of §41712 has occurred. EPIC concedes that the Order correctly articulates the test for determining whether Northwest engaged in a deceptive trade practice. There is no question that Northwest's privacy policy constituted a "representation, omission or practice." However, there is no evidence to support EPIC's subsequent contention that "reasonable, law-abiding consumers" would have been materially deceived by Northwest's stated policy. To find a deceptive practice, the consumer must have had a *reasonable* basis for his or her mistaken belief, drawn from the carrier's own representations. The Order correctly applied the standard for determining whether Northwest had engaged in a deceptive practice when it concluded that no reasonable consumer would have adopted EPIC's preferred reading of the Northwest privacy policy.¹
2. The Order correctly framed the dilemma posed by EPIC, as between a reading of the Northwest privacy policy that permitted it to share PNR data with ARC, and a reading that would have prevented Northwest from sharing PNR data with the Department or with any other government agency absent a court order (or equivalent "process"). EPIC has consistently attempted to convert Northwest's assurance that its customers "are in complete control of [their] travel planning needs," into a promise of a comprehensive ban on any data transfers not specifically and separately identified as authorized. A paragraph in the policy, framed as a disclaimer, reserves the carrier's right to "comply with law enforcement requests or requirements," and generically provides that Northwest's performance under the policy is "subject to existing laws and legal process." EPIC has previously argued that because this paragraph does not specifically identify any third party other than "law enforcement" or any means other than "legal process," then all other instances of data sharing with governmental entities fall outside this exception, and are not captured by any other exception.² The

¹ EPIC offers no reason to question the Order's conclusion that such an overreaching reading of the implicit message of the text is both unsupported and unreasonable. To date, EPIC has provided no evidence that any actual customers of Northwest interpreted the policy in this fashion, and has relied solely on a "contrived ends-oriented interpretation of [Northwest's] privacy policy." Airlines inhabit an industry where passenger records are open to inspection by various governmental agencies, without the need for prior court intervention. In such a world, and in the absence of a carrier's unambiguous representations to the contrary, consumers simply cannot reasonably presume that an airline will refuse to share passenger data with government officials.

² Northwest's policy makes no explicit mention of non-profit data sharing, such as a transfer between the airline and an advanced research laboratory, although it does contain an explicit commitment barring Northwest from *selling* customer data. EPIC fails to show how it would be "reasonable" for a consumer to conclude that Northwest's policy contains a promise that it would not engage in non-commercial transfers, even where the

Order notes that such an interpretation would prevent Northwest from complying with its regulatory obligations, which do not require “legal process,” and do not necessarily involve typical “[criminal] law enforcement” issues. In its petition, EPIC attempts to save its analysis by broadening its interpretation of “existing laws” to encompass federal regulations, Department precedent, and corresponding industry practice. However, doing so places a corresponding strain on its original position that no disclosure is permitted unless it is separately and specifically authorized. If exceptions can be read expansively, then there is no reason to disturb the Enforcement Office’s conclusion that the policy as a whole is focused exclusively on the carrier’s assurance that it will not commercially exploit customer data beyond what is necessary to satisfy the customer’s travel needs.

3. The Order permissibly cites the absence of “significant” consumer harm as determinative of the Enforcement Office’s decision to not initiate formal enforcement proceedings. The focal points of EPIC’s complaint are two separate acts: first, Northwest made a representation to its customers; second, Northwest shared customer data with ARC. It is alleged that these two acts lie in contradiction. Nevertheless, the Enforcement Office has noted that *even if* (contrary to the conclusion reached above) these two acts were to lie in contradiction, there is no evidence that Northwest’s customers were significantly harmed by ARC’s access to the data. Thus, even if EPIC is correct as to the *existence* of a deceptive practice, the Enforcement Office acted within its discretion to decline to initiate enforcement proceedings in this particular case because the *extent* of harm was so slight. EPIC has provided no evidence of harm beyond the mere fact that ARC had access to a sample of Northwest’s customer data. EPIC does not even allege that ARC’s access to the data increased the risk of disclosure or unauthorized commercial exploitation. In the absence of such evidence, the Enforcement Office found that the public interest did not demand an enforcement proceeding. I agree.
4. The Order does not undermine the Department’s ability to ensure that the airlines comply with their privacy commitments. The “Safe Harbor agreement” cited by EPIC does not require that the Department abandon the ordinary parameters of prosecutorial discretion or that it impose upon airlines unreasonable interpretations of their privacy commitments. Nevertheless, it is important to recognize those facts that the Enforcement Office was not faced with. First, Northwest is not alleged to have transferred customer data for profit. Second, Northwest is not alleged to have transferred customer data to a nongovernmental entity. Third, Northwest is not alleged to have transferred customer data to a third party whose data protection protocols were not at least as secure as those that the airline itself maintains. Finally, Northwest’s privacy policy does not expressly or implicitly promise consumers that it will refrain from sharing passenger data with all third parties, public or private. As the Order makes clear, the presence of one or more of these scenarios might have compelled a different result.

recipient maintains a level of security at least equal to that of the carrier itself and the data remain the property of the airline.

CONCLUSION

Based upon a thorough examination of the information in this Docket and, for the reasons stated above, I believe that enforcement action is not in the public interest and I affirm Order 2004-9-13. This decision constitutes the final administrative action in this proceeding.

ACCORDINGLY, I affirm the dismissal of the third-party complaint in this docket.

This action is taken under authority assigned in 14 CFR §§385.33 and 385.34(b), and shall be effective as the final action of the Department on the second business day following the date of service of this decision.

By:

(SEAL)

ROSALIND A. KNAPP
Deputy General Counsel

*An electronic version of this document is available on the World Wide Web at:
<http://dms.dot.gov/>*