

**IN THE UNITED STATES BANKRUPTCY COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

In re:

**SPIRIT AVIATION HOLDINGS,
INC., et al.**

Debtor

Case No. 25-11897 (SHL)

Chapter 11

Jointly Administered

**[PROPOSED] BRIEF OF *AMICI CURIAE* THE ELECTRONIC PRIVACY
INFORMATION CENTER & PROFESSOR SEEMA N. PATEL IN
SUPPORT OF THE ASSOCIATION OF FLIGHT ATTENDANTS-CWA,
AFL-CIO'S LIMITED OBJECTION**

Thomas McBrien
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, D.C. 20036
Tel: 202-483-1140
Email: McBrien@epic.org

Mason A. Kortz #MA0057
Cyberlaw Clinic
Harvard Law School
1557 Massachusetts Avenue, 4th Floor
Cambridge, MA 02138
Tel: 858-922-1990
Email: mkortz@law.harvard.edu

Counsel for proposed amici curiae

October 1, 2026

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Bankruptcy Procedure 7007.1(a), the undersigned counsel certifies that *amicus curiae* the Electronic Privacy Information Center has no parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT	ii
TABLE OF CONTENTS	iii
TABLE OF AUTHORITIES	iv
INTERESTS OF AMICUS CURIAE.....	1
ARGUMENT.....	1
I. The Sale Agreement does not adequately protect the privacy of AFA members.	3
A. The Sale Agreement provides little to no recourse for AFA members whose personal data is misused.	4
B. The Agreement does not adequately mitigate the risk of reidentification by third parties.	7
C. Deidentification of employee data does not adequately protect against exposure of sensitive information by inference.....	10
II. Allowing the sale of employee information would create incentives for other businesses to over-collect employee data.	13
CONCLUSION.....	16

TABLE OF AUTHORITIES

Cases

<i>Wilson v. Dantas</i> , 746 F.3d 530, 537 (2d Cir. 2014).....	5
---	---

Statutes

C.R.S. § 6-1-1306	6
Cal. Civil Code §1798.140	3
Conn. Gen. Stat. § 31-48d	6
Del. Code tit. 19 § 705.....	6
Tex. Bus. & Com. Code § 541.051.....	6

Other Authorities

Alicia Solow-Niederman, <i>Information Privacy and the Inference Economy</i> , 117 NW. U. L. REV. 357 (2022)	10, 11, 14
Aloni Cohen and Kobbi Nissim, <i>Towards Formalizing the GDPR’s Notion of Singling Out</i> , 117 PROC. NATL. ACAD. SCI. 8344 (2020).....	8
Arvind Narayanan and Vitaly Shmatikov, <i>Robust De-anonymization of Large Sparse Datasets</i> , IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2008).....	9
Boris Lubarsky, <i>Re-Identification of “Anonymized” Data</i> , 1 GEO. L. TECH. REV. 202 (2017).....	9
California Privacy Protection Agency, <i>Nation’s Largest Rural Lifestyle Retailer to Pay \$1.35M Over CCPA Violations</i> (September 30, 2025)	6
Ifeoma Ajunwa et. al., <i>Limitless Worker Surveillance</i> , 105 CAL. L. REV. 735 (2017)	7, 15
John Davisson, <i>Data Minimization: A Pillar of Data Security, But More Than That Too</i> , ELECTRONIC PRIVACY INFORMATION CENTER (June 22, 2023)	15

Kate Crawford and Jason Schultz, <i>Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms</i> , 55 B.C. L. REV. 93 (2014)	8, 9, 10, 11
Latanya Sweeney, <i>K-anonymity: A Model for Protecting Privacy</i> , 10 INT. J. UNCERTAIN. FUZZINESS KNOWL.-BASED SYST. 557 (2002)	9
Marcin Waniek et al., <i>Human Intuition as a Defense Against Attribute Inference</i> , 13 SCI. REP. 16088 (2023)	11
Mason Marks, <i>Emergent Medical Data: Health Information Inferred by Artificial Intelligence</i> , 11 UC IRVINE L. REV. 995 (2021)	12
Minsu Longiaru et al., <i>The “Privacy Trap”: How “Privacy-Preserving AI Techniques” Mask the New Worker Surveillance and Datafication</i> (2026)	12
Nadav Voloch and Ron S. Hirschprung, <i>Both Ends of Artificial Intelligence Impacting Privacy: A Review of Violation and Protection</i> , 9 FRONTIERS IN ARTIFICIAL INTELLIGENCE 1686454 (2026)	11, 13
Nicole Gross and Hannah van Kolfschooten, <i>Advertising to the Distressed: The Commodification of Mental Health Data in AI Chatbots</i> , JOURNAL OF MEDICAL ETHICS BLOG (Apr. 14, 2026)	14
Paul Ohm, <i>Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization</i> , 57 UCLA L. REV. 1701 (2010)	8, 9
<i>US State Comprehensive Privacy Laws Report 2025</i> , INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Oct. 27, 2025)	5
Web3 Foundation, <i>The Hidden Price of Free: What Your Data Is Really Worth</i> (May 25, 2026)	14
Yaqub Chaudhary and Jonnie Penn, <i>Beware the Intention Economy: Collection and Commodification of Intent via Large Language Models</i> , 5 HARVARD DATA SCI. REV. (Special Issue) (2024)	14

INTERESTS OF AMICI CURIAE¹

The Electronic Privacy Information Center (“EPIC”) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC regularly advocates in courts and legislatures for stronger protections for employee privacy. *See Worker Privacy*, EPIC (2026).²

Professor Seema N. Patel is an Associate Professor of Law at the University of California College of Law, San Francisco. Drawing on her years of litigation, policy advocacy, and teaching experience, including extensive collaboration with workers, labor unions, and worker centers, her scholarship centers on the relationship between technology and employment. *See Seema N. Patel*, U.C. L. S.F. (2026).³

ARGUMENT

Spirit Airlines has proposed, as part of the present bankruptcy proceeding, a liquidation of data that implicates the privacy rights of Spirit Airlines employees. Spirit Airlines is proposing to sell that data to Google for \$10 million. *See Notice of*

¹ Pursuant to FRBP 8017(a)(4)(D), *amici* state that no party’s counsel authored the proposed amicus brief in whole or in part; no party’s counsel contributed money that was intended to fund preparing or submitting the brief; and no person other than *amici*, their members, or their counsel contributed money that was intended to fund preparing or submitting the proposed amicus brief.

² <https://epic.org/issues/data-protection/workplace-privacy/>

³ <https://www.uclawsf.edu/people/seema-patel/>

Auction Results and Scheduled Hearing for the Deidentified Data, Docket No. 1463, Exhibit A (hereinafter “Sale Agreement”) § 1(a). That data includes information collected from Spirit Airlines employees during the course of their employment: payroll, training, discipline, travel, internal communications, and more. *See id.* at A-2. This data is slated to be sold after being “deidentified” by a third party—determined solely by Google—under standards designed for consumer data. *Id.* §§ 1(a)(ii), (3)(c).

In response to the proposed sale of large volumes of employee data without adequate privacy protections, the Association of Flight Attendants (“AFA”) has objected to this sale. *See Limited Objection of the Association of Flight Attendants-CWA, ALF-CIO to the Proposed Sale of the Deidentified Data, Docket No. 1489* (hereinafter “AFA Objection”). AFA correctly notes that certain categories of data are sensitive not because they directly reveal personally identifiable information, but because they allow inferences about individuals or small groups that contravene employees’ expectations of confidentiality. AFA reasonably asks the court to order the screening and removal of employee data before the sale is permitted to proceed. *Id.* ¶¶ 17-18.

Amicus agree with and support AFA’s objection to the sale. *Amicus* writes separately to emphasize two points: First, the risk of exposure by inference is greater than ever given recent advances in artificial intelligence. AFA’s concern that

confidential information could be exposed, even after deidentification, is very real. Second, proceeding with the sale as proposed would create perverse incentives for employers to over-collect employee data. If employee-confidential data can be sold as an asset, employers will be encouraged to collect as much data as possible and store it indefinitely—even if that data is not required for day-to-day operations. This in turn jeopardizes data security and puts employee privacy at risk unnecessarily.

I. The Sale Agreement does not adequately protect the privacy of AFA members.

Under the proposed agreement, a third party would deidentify the data at issue using standards drawn from the California Consumer Privacy Act (“CCPA”). Sale Agreement § 3(c). The CCPA standards require that deidentified data “cannot reasonably be used to infer information about, or otherwise be linked to, a *particular consumer*.” Cal. Civ. Code §1798.140(m) (emphasis added). The CCPA further provides that data owners cannot associate the information “with a *consumer or household*.” *Id.* (emphasis added). Google warrants that all consumer data sold under the agreement will be deidentified to Google’s “reasonable satisfaction,” Sale Agreement § 3(c), and that it will not “intentionally” reidentify data. *Id.* § 1(c).

As an initial matter, the guarantee to deidentify data does not clearly extend to employee data. Even if it does, while an important method to mitigate some risks to personal privacy, the guarantees in the Sale Agreement are far from sufficient to protect the privacy interests of Spirit Airlines employees. The Agreement places too

much power in the hands of the buyer, and none in the hands of the affected employees. Under the terms of the sale, Google has the power to determine what deidentification methods are used, how the data is handled, where it is stored, and who ultimately has access. Meanwhile, the employees get nothing more than an unenforceable promise from Google that some deidentification method will be applied. If Google were to reidentify employee data, intentionally or otherwise, there would be little recourse for affected AFA members. Furthermore, even if Google adheres to the commitments in the Sale Agreement and avoids reidentification, the data at issue could nevertheless be reidentified by third parties. Finally, even deidentified data could reveal information that employees reasonably believed would be held in confidence. In light of current technological trends, the level of deidentification required in the Sale Agreement is simply not sufficient to protect employee privacy.

A. The Sale Agreement provides little to no recourse for AFA members whose personal data is misused.

The Sale Agreement, as written, is a poor fit for protecting AFA members' privacy. As AFA points out, the Agreement is couched almost exclusively in terms of consumer, not employee, privacy rights. *See* AFA Objection ¶ 11. Section 3(c) of the Sale Agreement, which describes the deidentification requirement, requires only deidentification "in accordance with applicable laws" such as the CCPA and the HIPAA Privacy Rule. Sale Agreement § 3(c). However, it is not clear that

“applicable laws” require deidentification of the employee data at issue. Nearly all state data privacy laws are centered around consumers. *See US State Comprehensive Privacy Laws Report 2025*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Oct. 27, 2025).⁴ Privacy-protecting provisions in the Bankruptcy Code are limited to consumer data as well. *See* 11 U.S.C. § 101(41A) (defining “personally identifiable information” in terms of consumer interactions). The applicability of the proposed deidentification requirements to employee data is, therefore, ambiguous at best.

To the extent the Sale Agreement does require deidentification of employee data, Google is solely responsible for nominating a third party to deidentify the data and determining whether the process was adequate. Sale Agreement §§ 1(a)(ii), (3)(c). While Google promises that it (and any future recipients of the data) will not intentionally reidentify the data, AFA has no way to enforce this provision as a matter of contract law. *See Wilson v. Dantas*, 746 F.3d 530, 537 (2d Cir. 2014) (holding that third parties have no standing to enforce contract where contract expressly disclaims third party beneficiaries). And, although Google makes a “public commitment” not to reidentify data under “applicable data protection laws,” Sale Agreement § 1(c), nowhere in the Agreement does it concede that it would be subject to a suit under any such laws. Even if it did, AFA members would only be able to

⁴ <https://iapp.org/resources/article/us-state-privacy-laws-overview>

bring a suit in limited circumstances.⁵ This is not to say that state agencies would be completely powerless if Google misused employee data obtained via the proposed sale. *See, e.g.,* California Privacy Protection Agency, *Nation's Largest Rural Lifestyle Retailer to Pay \$1.35M Over CCPA Violations* (September 30, 2025)⁶ (fining business for failure to adequately protect job applicant data). However, AFA members themselves would have few options for enforcement on their own.

Even assuming that Google does comply with its public commitments under the Sale Agreement, the assurances it offers are a far cry from the comprehensive protections provided under state law. For example, many states now provide consumers the right to delete personal data, *see, e.g.,* C.R.S. § 6-1-1306(1)(d); Tex. Bus. & Com. Code § 541.051(b)(3). AFA members have no such option under the proposed sale. Other states require notice before collecting specific types of employee data. *See, e.g.,* Conn. Gen. Stat. § 31-48d; Del. Code Ann. tit. 19, § 705. It is unclear whether the affected AFA members had any such notice, let alone opportunity to object, as to the data collected here. Even if AFA members nominally consented to the collection of their workplace data, the power differential between

⁵ For example, the CCPA only provides for a private right of action in case of “unauthorized access and exfiltration, theft, or disclosure,” commonly called a data breach. *See* Cal. Civ. Code §1798.150(a)(1). If Google were to breach its promise not to reidentify data, AFA members would have no recourse unless that identifiable data were subsequently exposed to outside actors.

⁶ <https://cppa.ca.gov/announcements/2025/20250930.html>

employee and employer calls into question whether that consent would comport with the letter or the spirit of modern privacy laws. *See* Ifeoma Ajunwa et al., *Limitless Worker Surveillance*, 105 CAL. L. REV. 735, 733-744 (2017) (arguing that standard notice and consent is insufficient to protect against workplace surveillance).

All told, the Sale Agreement falls well short of adequately protecting AFA members' privacy interests. Although the Agreement references state privacy laws, it does not clearly state that Google is subject to the *enforcement* of such laws. Moreover, Google's public commitment to privacy does not actually provide AFA members with the full panoply of protections they would receive under state law. The Sale Agreement would need to be substantially modified to give the affected employees a real say in how that data is handled, used, and disclosed.

B. The Agreement does not adequately mitigate the risk of reidentification by third parties.

In addition to using the data itself, Google reserves the right to transfer the data to third parties on the condition that the recipients will “maintain and use the Deidentified Data in deidentified form [and] will not intentionally associate the Deidentified Data with any person or household.” Sale Agreement § 1(c). Increasing the number of entities that have access to the data would naturally increase the risk that someone will, intentionally or unintentionally, reidentify some portion of the employee data at issue. The primary mitigation against this risk is the deidentification of the data—to Google's satisfaction—under “applicable laws . . .

and prevailing industry standards.” *Id.* § 3(c). This is insufficient to protect the AFA members against reidentification.

One issue with this approach is that Google’s designated deidentification agent cannot foresee how the data in question will interact with other data that has been, or will be, released. Reidentification often involves singling out an individual—that is, querying data to find a set of characteristics that result in a group of one—then using external information to identify that individual. *See* Aloni Cohen and Kobbi Nissim, *Towards Formalizing the GDPR’s Notion of Singling Out*, 117 PROC. NATL. ACAD. SCI. 8344 (2020). The more characteristics of an individual that are made public, the easier it is to single them out. *See id.* at 8346; *see also* Kate Crawford and Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014) (explaining how large amounts of deidentified data “can generate a predictive model of what has a high probability of being [personally identifiable information]”).

Furthermore, Google’s reference to “prevailing standards” does not account for evolving reidentification techniques. Early data privacy techniques focused on removal of specific fields from datasets to prevent information from being linked to individuals. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706-16 (2010) (describing the prevalent “release-and-forget” approach to deidentification). Then

Latanya Sweeney famously identified a former Massachusetts governor's medical records from publicly available (and ostensibly deidentified) data. *See* Latanya Sweeney, *K-Anonymity: A Model for Protecting Privacy*, 10 INT. J. UNCERTAIN. FUZZINESS KNOWL.-BASED SYST. 557 (2002). Later, two researchers reidentified large portions of an anonymous Netflix dataset. Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2008). In 2014, a data scientist used pictures of celebrities entering and leaving taxis to reverse the pseudonymization of New York City's medallion data. Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202 (2017). In each of these examples, experts believed the data in question was sufficiently deidentified—until it was shown that it was not.

Google's commitment to follow current laws and standards only goes so far in assuring privacy for AFA members whose data is scheduled to be sold. The history of data privacy suggests that, over time, advances in computing will render current protections less effective. *See* Ohm, *supra*, at 1740-41 (describing how advances in reidentification undermine existing data protection laws); Crawford & Schultz, *supra*, at 106-08 (describing inability of existing data protection laws to address "Big Data"). The only way to truly ensure that AFA members' personal data is not exposed is to prohibit the sale of that data entirely.

C. Deidentification of employee data does not adequately protect against exposure of sensitive information by inference.

Finally, even if the employee data at issue could be adequately deidentified, inferences drawn from the deidentified data could still intrude on AFA members' privacy. Indeed, one of AFA's primary objections is that neither the Agreement nor any governing law adequately protects confidential employee information. AFA Objection ¶¶ 10-12. That concern is well founded, especially in light of recent advances in data analysis techniques. Modern artificial intelligence ("AI") systems are often able to infer sensitive information about individuals and discrete groups, even from deidentified data. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 378-87 (2022). The Sale Agreement does little to guard against such possibilities.

AI processes like machine learning and large language models are the latest in a long line of computing techniques harnessing the power of large datasets. For decades, "Big Data" has enabled data processors to both place anonymous users in groups and predict how members of those groups will act. *See* Crawford & Schultz, *supra*, at 96. This gives rise to "predictive privacy harms," whereby data processors infer information that would normally be sensitive, confidential, or legally protected. *Id.* at 97-99. For example, an individual's purchasing patterns might be correlated with a specific medical condition. That individual might then be screened into—or

out of—particular advertisements or opportunities. *Id.* at 100-01 (describing how predictive analytics could be used to discriminate in housing opportunities).

Like prior Big Data processing techniques, AI uses massive amounts of data to detect patterns that would elude a human viewer. *See* Solow-Niederman, *supra*, at 380. Various AI applications are vulnerable to different forms of privacy attacks, from inference of sensitive information to leakage of the underlying data. *See* Nadav Voloch and Ron S. Hirschprung, *Both Ends of Artificial Intelligence Impacting Privacy: A Review of Violation and Protection*, 9 FRONTIERS IN ARTIFICIAL INTELLIGENCE 1686454, 17 tbl.2 (2026). Depending on how Google uses the employment data—a topic that is not addressed or limited in the Agreement—any number of these privacy harms could manifest. *Amici* focuses on one particularly likely harm: attribute inference.

Attribute inference is the process of analyzing public, non-sensitive data about an individual to infer non-public, sensitive characteristics of that individual. *See* Marcin Wanick et al., *Human Intuition as a Defense Against Attribute Inference*, 13 SCI. REP. 16088 (2023). As early as 2012, retail chain Target developed an algorithm that predicted whether a shopper was pregnant based on their buying patterns. Crawford & Schultz, *supra*, at 94. A 2019 University of Pennsylvania study showed that it was possible to predict, with reasonably high certainty, certain medical diagnoses by analyzing individuals’ social media posts. *See* Mason Marks, *Emergent*

Medical Data: Health Information Inferred by Artificial Intelligence, 11 UC IRVINE L. REV. 995, 1007-09 (2021). Inferred attributes can be used for various purposes, from risk assessments to vulnerability-based marketing. *See id.* at 1013-30.

The same could easily happen to a former Spirit employee whose data is transferred to Google and used in an AI system. An individual's email and Teams communications might reveal a propensity to file HR complaints. Their timecard data might place them in the category of "likely to take time off around religious holidays." Even if the individual were never identified by name, their employment data could be used to predict attributes that might then be used to deny them employment opportunities or undermine worker interests. *See* Minsu Longiaru et al., *The "Privacy Trap": How "Privacy-Preserving AI Techniques" Mask the New Worker Surveillance and Datafication* 6-10 (2026).⁷ Nor is the potential for harm limited to future employment. If an employee's financial or medical information can be inferred, it could affect their ability to qualify for loans, find affordable insurance, obtain future employment, and have peace of mind.

Because of the risk of attribute inference and other privacy attacks, the deidentification required in the Agreement falls far short protecting AFA members' privacy. Even if the employee data were perfectly anonymized—which *amici* doubt is realistic—it could be used to generate inferences that could be used, without their

⁷ <https://datasociety.net/wp-content/uploads/2026/06/The-Privacy-Trap.pdf>

consent, for anything from application screening to targeted advertising. This is not to say privacy is a lost cause in the modern age. Researchers have developed techniques for minimizing attribute inference and other forms of data-driven privacy attacks. *See* Voloch & Hirschprung, *supra*, at 11-19 (summarizing research on privacy-protective artificial intelligence). However, the Agreement as it stands does not require such precautions, and only Google knows how it will handle employee data. Accordingly, the court should either bar the sale of the employee data at issue or, at the very least, impose stronger privacy protections on employee data to address AFA's concerns.

II. Allowing the sale of employee information would create incentives for other businesses to over-collect employee data.

For all the reasons described above, Google's proposed purchase of confidential employee data would impose significant privacy risks on AFA members. That alone is reason enough to bar the sale of that data or, at least, modify the Sale Agreement to provide more robust privacy protections. However, *amici* also have other, more holistic concerns: the commodification of personal data, the incentives it creates for employers, and the impact it has on privacy and security.

As explained above, modern AI systems require massive amounts of data to operate. AI developers acquire that data however they can, including by purchasing from other data collectors. Personal data is among the most valuable: the average American's information output is worth an average of \$6,563 per year, according to

one recent estimate. See Web3 Foundation, *The Hidden Price of Free: What Your Data Is Really Worth* (May 25, 2026).⁸ This has led to the commodification of all sorts of personal data, from expressions of intent to confessions of mental health concerns. See, e.g., Yaqub Chaudhary and Jonnie Penn, *Beware the Intention Economy: Collection and Commodification of Intent via Large Language Models*, 5 HARVARD DATA SCI. REV. (Special Issue) (2024); Nicole Gross and Hannah van Kolfshoeten, *Advertising to the Distressed: The Commodification of Mental Health Data in AI Chatbots*, JOURNAL OF MEDICAL ETHICS BLOG (Apr. 14, 2026).⁹ As Google’s proposed purchase shows, workplace data is no exception.

Putting a dollar value on workplace data creates a clear incentive: employers should collect and retain as much data on their employees as possible. See Solow-Niederman, *supra*, at 394-95 (describing “mounting incentives to acquire data and apply [AI] technology in more spheres of life”). However, these incentives are not without cost. The best way to secure data is to not collect unnecessary information in the first place. Accordingly, the principle of data minimization states that entities should not collect data beyond what is necessary for specific, identifiable operations. See John Davisson, *Data Minimization: A Pillar of Data Security, But More Than*

⁸ <https://web3.foundation/hidden-price-of-free/web3-foundation-hidden-price-of-free-white-paper.pdf>

⁹ <https://blogs.bmj.com/medical-ethics/2026/04/14/advertising-to-the-distressed-the-commodification-of-mental-health-data-in-ai-chatbots/>

That Too, ELECTRONIC PRIVACY INFORMATION CENTER (June 22, 2023). ¹⁰

Monetization of employee data encourages employers to violate the principle of data minimization and collect as much information as possible, on the chance that it will be worth something down the road.

Monetization of employee data creates particularly perverse incentives, because employees are a captive audience. Where a social media user or business customer might at least nominally “consent” to data collection in return for accessing a service, an at-will employee has virtually no leverage against their employer. *See* Ajunwa et al., *supra*, at 774. Moreover, while the monetary value of worker data is realized by the employer, the increased risk of a data breach and resulting loss of privacy is borne largely by the employees. Thus, the incentives to capture employee data are drastically one-sided.

The Sale Agreement, at least as it now stands, would be a clear signal to other employers to over-collect workplace data and put their employees’ privacy at risk. *Amici* urge the Court to consider this impact when deciding whether to include confidential employee data in the proposed sale.

¹⁰ <https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/>

CONCLUSION

As stated above, the Sale Agreement as written puts AFA members at risk of having personal information exposed, either through reidentification or inference, while giving those same members no say in how their data is handled, used, or shared. Moreover, the sale would incentivize risky data collection behaviors by other employees, encouraging them to over-collect employee data on the hopes of future monetization. For these reasons, *amici* respectfully urge the Court to exclude the challenged categories of employee data from the sale or, in the alternative, to modify the Sale Agreement to provide greater protections against misuse and more control by AFA members.

Dated: October 1, 2026

Respectfully submitted,

/s/ Thomas McBrien

Thomas McBrien
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, D.C. 20036
Tel: 202-483-1140
Email: McBrien@epic.org

Mason A. Kortz #MA0057
Cyberlaw Clinic
Harvard Law School
1557 Massachusetts Avenue, 4th Floor
Cambridge, MA 02138
Tel: 858-922-1990
Email: mkortz@law.harvard.edu

Counsel for proposed amici curiae

CERTIFICATE OF COMPLIANCE

Pursuant to the FRBP 29(a)(4)(F), I hereby certify that this brief complies with the type-volume limitations of FRBP 8017(a)(5) and 8015(a)(7)(B) because it contains 3,553 words as calculated by the word count feature of Microsoft Word 365, exclusive of the sections exempted by FRBP 8015(g).

Dated: October 1, 2026

Respectfully submitted,

/s/ Thomas McBrien

Thomas McBrien
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, D.C. 20036
Tel: 202-483-1140
Email: McBrien@epic.org

Mason A. Kortz #MA0057
Cyberlaw Clinic
Harvard Law School
1557 Massachusetts Avenue, 4th Floor
Cambridge, MA 02138
Tel: 858-922-1990
Email: mkortz@law.harvard.edu

Counsel for proposed amici curiae