IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE

STEVEN VANCE and TIM JANECYK, for themselves and others similarly situated,

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

No. _____

CLASS ACTION COMPLAINT

JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiffs STEVEN VANCE and TIM JANECYK, on behalf of themselves and all other similarly situated individuals ("Plaintiffs"), by and through their respective attorneys, bring this Class Action Complaint against Defendant Microsoft Corporation ("Microsoft") and allege the following:

INTRODUCTION

1. Facial recognition technology – once a thing only seen in movies – now threatens to end individual privacy. Public and private entities increasingly deploy facial recognition products to determine a private citizens' identities, as well as other personal information, such as their addresses, phone numbers, whereabouts and acquaintances.

2. Unlike the way facial recognition technology is depicted in the movies, the actual technology is plagued by a major problem – it is inaccurate, especially when it comes to correctly identifying women and people of color.

3. In recent years, an "arms race" has developed amongst for-profit companies seeking to become market leaders in the facial recognition arena. Critical to winning this battle

has been to the ability to claim a low identification error rate – *i.e.*, the for-profit companies want to herald the accuracy of their products, including accuracy in identifying woman and people of color.

4. In its effort to improve its facial recognition technology, Defendant Microsoft violated Illinois' Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), by, among other things, unlawfully collecting, obtaining, storing, using, possessing and profiting from the biometric identifiers and information of Plaintiffs Vance and Janecyk and all other similarly situated Illinois residents and citizens (hereinafter, the "Class Members").

5. Plaintiffs bring this Class Action Complaint seeking: (a) statutory damages of $5,000 per BIPA violation, or, alternatively, if Defendant Microsoft acted negligently, $1,000 per BIPA violation, along with attorneys' fees and costs; (b) disgorgement of Defendant's ill-gotten gains derived from the use of the unlawfully-acquired data; and (c) an injunction (i) barring Defendant from any further use of Illinois citizens' and residents' biometric identifiers and information; (ii) barring Defendant from continuing to collect, obtain, store, use, possess and profit from Plaintiffs' and Class Members' biometric identifiers and information; and (iii) requiring Defendant to delete and destroy Plaintiffs' and Class Members' biometric identifiers and information.

PARTIES

6. At relevant times, Plaintiff STEVEN VANCE was – and remains – an Illinois resident who lived in the Northern District of Illinois. Defendant Microsoft collected, obtained, stored, used, possessed and profited from Plaintiff Vance's biometric identifiers and information – namely, facial geometric scans of Plaintiff Vance.

7. At relevant times, Plaintiff TIM JANECYK was – and remains – an Illinois resident who lived in the Northern District of Illinois. Defendant Microsoft collected, obtained, stored, used, possessed and profited from Plaintiff Janecyk's biometric identifiers and information – namely, facial geometric scans of Plaintiff Janecyk.

8. Defendant Microsoft is a Washington corporation based in Redmond, Washington.

JURISDICTION AND VENUE

9. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class. Because it is estimated that the Class will have thousands of members and Defendant Microsoft's intentional and reckless violations of BIPA are punishable by statutory damages of $5,000 per violation, the amount in controversy is well in excess of $5,000,000. This Court has supplemental jurisdiction over the state law claim pursuant to 28 U.S.C. § 1367.

10. This Court has personal jurisdiction over Defendant Microsoft because it is at home in the Western District of Washington. As alleged above, Microsoft is a Washington corporation headquartered in Redmond, Washington.

11. Venue is proper under 28 U.S.C. § 1391(b)(1) because Defendant Microsoft resides in the Western District of Washington.

FACTUAL ALLEGATIONS

Biometric Identifiers

12. Every individual has unique features by which he or she can be identified using a set of standard quantitative measurements, commonly referred to as "biometric identifiers."

13. For example, the shape of and distance between tiny ridges on each person's finger are unique, so measures of those features can be used to identify a specific individual as the person who made a fingerprint.

14. Each person also has a unique facial geometry composed of, among other measures, distances between key facial landmarks and ratios between those distances.

15. Once a picture of a person's face is scanned and its biometric measurements are captured, computers can store that information and use it to identify that individual any other time that person's face appears on the internet, in a scanned picture or footage from any of the billions of cameras that are constantly monitoring the public's daily lives.

16. Unlike fingerprints, however, facial biometrics are readily observable and, thus, present a grave and immediate danger to privacy, individual autonomy and liberty.

The Illinois Biometric Information Privacy Act

17. Through BIPA, Illinois strictly regulates the collection, obtainment, storage, and use of biometric identifiers and information.

18. Under BIPA, biometric identifiers include a scan of an individual's face geometry. 740 ILCS § 14/10.

19. Under BIPA, biometric information is "any information . . . based on an individual's biometric identifier used to identify an individual." 740 ILCS § 14/10.

20. According to the Illinois General Assembly: "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS § 14/5(c).

21. Pursuant to BIPA, a private entity is, among other things: (a) prohibited from collecting or otherwise obtaining an individual's biometric identifiers and information without providing written notice and obtaining a written release; (b) prohibited from profiting from an individual's biometric identifiers and information; and (c) required, to the extent it is in possession of biometric identifiers or information, to develop a written policy, made available to the public, that establishes a retention schedule and guidelines for permanently destroying such identifiers and information. 740 ILCS § 14/15.

22. BIPA provides for a private right of action and allows a prevailing party to recover liquidated damages in the amount of: (a) $1,000 or actual damages, whichever is greater, for negligent violations of its provisions; and (b) $5,000 or actual damages, whichever is greater, for intentional or reckless violations of its provisions. 740 ILCS § 14/20. BIPA also allows for the recovery of attorneys' fees and costs and injunctive relief. 740 ILCS § 14/20.

Facial Recognition Technology

23. Facial recognition is a form of computer artificial intelligence, the goal of which is to "create systems that detect, recognize, verify and understand characteristics of human faces."[1]

[1] Michele Merler, *et al.*, *Diversity in Faces*, IBM Research AI (Apr. 10, 2019) ("*Diversity in Faces*").

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.