IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

STEVEN VANCE and TIM JANECYK, for themselves and others similarly situated,	)))	Case No. 20 C 577
Plaintiffs,	)))	Judge Charles P. Kocoras
v.	)))	Magistrate Judge Gabriel A. Fuentes
INTERNATIONAL BUSINESS MACHINES CORPORATION,	)))	**SECOND AMENDED CLASS ACTION COMPLAINT**
Defendant.	)))	**JURY TRIAL DEMANDED**
	))	**INJUNCTIVE RELIEF DEMANDED**

SECOND AMENDED 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 Second Amended Class Action Complaint against Defendant INTERNATIONAL BUSINESS MACHINES CORPORATION ("IBM") and allege the following:

INTRODUCTION

1.   Every individual has unique biometric identifiers by which he or she can be identified. One such biometric identifier is a person's facial geometry.

2.   As the Illinois General Assembly has found: "[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).

1

3.   Pursuant to Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS §14/1, *et seq.*, Illinois prohibits among other things, private entities from collecting, capturing, obtaining, disclosing, redisclosing, disseminating or profiting from the biometric identifiers or information of an individual without providing written notice and without obtaining a written release from the impacted individual or his authorized representative.   BIPA also requires private entities in possession of biometric identifiers to adopt retention and destruction policies and to take measures to prevent the release of that information.

4.   In violation of BIPA, at relevant times, Defendant IBM, a multinational technology company headquartered in the State of New York, collected, captured, obtained, disclosed, redisclosed, disseminated and profited from the facial geometric scans of thousands of Illinois citizens in violation of BIPA's requirements.   Specifically, using a set of images from the photo-sharing service Flickr, IBM collected, captured and otherwise obtained facial geometric scans of individuals depicted in approximately one million photos and built a database containing each of the scanned individuals' unique "craniofacial measurements."   IBM then, among other things, disclosed, redisclosed and otherwise disseminated to third parties the biometric identifiers and information in the database in order to profit.   IBM possessed the biometric identifiers and information without having adopted or made public any policy, written or otherwise, to govern the retention and destruction of thereof.

5.   Defendant IBM engaged in the above-described conduct: (a) without informing the impacted individuals, including Plaintiffs and members of the proposed class (the "Class Members"), that their biometric identifiers were being collected, captured, obtained, disclosed, redisclosed and otherwise disseminated; (b) without informing the impacted individuals in writing of the purpose of the collection, capture, obtainment, disclosure, redisclosure and dissemination of

the biometric identifiers and information; and (c) without seeking and obtaining written releases from such impacted individuals or their authorized representatives.

6.   In violation of BIPA, Defendant IBM also profited from its unlawful use of the biometric identifiers and information of Plaintiffs and Class Members. On information and belief, IBM used the biometric identifiers and information of Plaintiffs and Class Members to improve the accuracy of its own facial recognition products and to cement its market-leading position in artificial intelligence. From 2016 to 2018, IBM derived more revenue from artificial intelligence than any other company in the world. In 2018 alone, IBM's revenue from artificial intelligence products totaled more than $2.5 billion. Those products include IBM Watson Visual Recognition, which IBM clients can use to estimate the age and gender of people depicted in images and, in some instances, identify specific individuals. IBM owns the intellectual property developed by its researchers and will not disclose the data sets used to train its Watson products.

7.   As the Illinois General Assembly has found and the Illinois Supreme Court has confirmed, the harm to Plaintiffs and Class Members as a result of the BIPA violations alleged herein has already occurred.

8.   Further, as businesses worldwide compete to develop ever more advanced facial recognition technology, the race for data imperils the privacy of individuals everywhere. Public policy in Illinois provides that given the risks of unwanted data collection and disclosure, its citizens need the power to make decisions about the fate of their unique biometric identifiers and information. Defendant IBM's actions robbed Plaintiffs and Class Members of that power.

9.   Moreover, as a direct result of Defendant IBM's actions, each individualized scan of a person's facial geometry can be tied back to the Flickr account to which an originating photo was posted. This, in turn, made and continues to make it possible for third parties to connect the

biometric identifiers and information of Plaintiffs and Class Members that have been collected, captured, and otherwise obtained to other photos in which Plaintiffs, a member of the Class and/or others appear, subjecting Plaintiffs and Class Members to increased surveillance, stalking, identity theft, social engineering (a type of hacking technique) and other invasions of privacy and fraud. Moreover, as a direct result of IBM's actions, Plaintiffs' and Class Members' biometric identifiers and information are no longer under their control and are available to a potentially unlimited range of unknown individuals for whatever uses they please. These injuries, which are imminent and clearly impending, are in addition to the injuries Plaintiffs and Class Members have already sustained as a result of IBM's actions.

10.   Plaintiffs bring this Second Amended Class Action Complaint seeking: (a) statutory damages of $5,000 per BIPA violation, or, alternatively, if Defendant IBM acted negligently, $1,000 per BIPA violation, along with attorneys' fees and costs; (b) disgorgement of IBM's ill-gotten gains derived from the use of the unlawfully-acquired data; and (c) an injunction (i) barring Defendant IBM from any further use of individuals' biometric identifiers and information; (ii) barring IBM from continuing to collect, capture, obtain, disclose, redisclose, disseminate and profit from Plaintiffs' and Class Members' biometric identifiers and information; (iii) requiring IBM to delete and destroy all biometric identifiers and information in its possession, custody and control; and (iv) requiring IBM to claw back the biometric identifiers and information from any third parties to whom IBM disclosed, redisclosed and disseminated it.

PARTIES

11.   At relevant times, Plaintiff STEVEN VANCE was – and remains – an Illinois resident. Defendant IBM performed facial geometric scans of Plaintiff Vance from photos Plaintiff Vance had uploaded to Flickr.

12.   At relevant times, Plaintiff TIM JANECYK was – and remains – an Illinois resident. Defendant IBM performed facial geometric scans of Plaintiff Janecyk from photos Plaintiff Janecyk had uploaded to Flickr.

13.   Defendant IBM is a New York corporation with its corporate headquarters in Armonk, New York and a regional headquarters in Chicago, Illinois. IBM has a registered agent in Illinois.

JURISDICTION AND VENUE

14.   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 IBM'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 claims pursuant to 28 U.S.C. § 1367.

15.   This Court has personal jurisdiction over Defendant IBM because IBM used and disseminated data derived directly from Illinois-based Flickr accounts and exposed residents of Illinois to ongoing privacy risks within Illinois based on the collection, capture, obtainment, disclosure, redisclosure and dissemination of their biometric identifiers and information. Furthermore, many of the photographs IBM used for its unlawful collection, capture and obtainment of biometric identifiers and information were created in Illinois, uploaded from Illinois, and/or managed via Illinois-based user accounts, computers, and mobile devices. Because of the scope and magnitude of IBM's conduct, which included identifying the location of the

5

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.

fastcase®
Smarter legal research.