YES / (NO)

EXHIBITS

CASE NO. 2020 CH 833

DATE: 1/22/20

CASE TYPE: CLASS ACTION

PAGE COUNT: 18

CASE NOTE

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT – CHANCERY DIVISION

TIM JANECYK, individually and on behalf of all others similarly situated,

Plaintiff,

v.

INTERNATIONAL BUSINESS MACHINES CORPORATION, a New York corporation,

Serve Registered Agent:
CT Corporation System
208 S. LaSalle Street, Suite 814
Chicago, IL 60604

Defendant.

2020CH00833
Case No.

(JURY TRIAL DEMANDED)

CLASS ACTION COMPLAINT

Plaintiff Tim Janecyk ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, brings this class action complaint pursuant to 735 ILCS 5/2-801, *et seq.*, against International Business Machines Corporation, ("IBM" or "Defendant"), for violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), and in support thereof alleges as follows:

NATURE OF ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of IBM in collecting, storing, and using Plaintiff's and other

similarly situated individuals' biometric identifiers[1] and biometric information[2] (collectively, "biometrics") without informed written consent, in direct violation of BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "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." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics – particularly in the City of Chicago, which was selected by major national corporations as a "pilot testing site[] for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias" (740 ILCS 14/5(b)) – the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like IBM may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored, *see id.*; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used, *see id.*; (3) receives a written release from the person for the collection of his or her biometric identifiers or information, *see id.*; and (4) publishes publically available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15(a).

---

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry," among others.

[2] "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier used to identify an individual.

4. In direct violation of each of the foregoing provisions of § 15(a) and § 15(b) of BIPA, IBM is actively collecting, storing, using, and disclosing – without providing notice, obtaining informed written consent, or publishing data retention policies – the biometrics of millions of unwitting individuals whose faces appear in IBM's Diversity in Faces Dataset ("DiF Dataset"), which dataset consists of about a million photographs of faces IBM uses to develop and train its facial recognition technologies.

5. The photographs making up IBM's DiF Dataset— about a million in total— were provided to IBM by Yahoo, which, upon information and belief, took most, if not all, of the photographs from Flickr, which, during that time, was Yahoo's subsidiary. The Flickr users who uploaded their photographs to Flickr had no idea IBM would acquire the photographs for use in its DiF Dataset, or for *any* use at all. Neither the individuals appearing in the photographs nor the photographers taking the photographs had any knowledge of— and did not consent to— IBM's acquisition of the photographs and IBM's collection and distribution of their biometrics from the photographs.

6. Specifically, IBM has created, collected, and stored millions of "face templates" (or "face prints") – highly detailed geometric maps of the face – from about a million photographs that make up its DiF dataset. IBM creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in its dataset. Each face template that IBM extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person.

7. Plaintiff brings this action individually and on behalf of all others similarly situated to prevent IBM from further violating the privacy rights of those individuals appearing in

IBM's DiF Dataset, and to recover statutory damages for IBM's unauthorized collection, storage, and use of these individuals' biometrics in violation of BIPA.

PARTIES

8. Plaintiff Tim Janecyk is, and has been at all relevant times, a resident and citizen of Illinois.

9. Defendant IBM is a New York Corporation with its headquarters at 1 New Orchard Road, Armonk, New York 10504. Accordingly, IBM is a citizen of the state of New York.

JURISDICTION AND VENUE

10. This is a class action complaint for violations of BIPA, seeking statutory and actual damages.

11. No federal question is presented by this complaint. Plaintiff brings this complaint solely under state law and not under federal law, and specifically not under the United States Constitution, nor any of its amendments, nor under 42 U.S.C. § 1981 or 1982, nor any other federal statute, law, rule, or regulation. Plaintiff believes and alleges that a cause of action exists under state law for the conduct complained of herein.

12. This class action is brought on behalf of all Illinois individuals whose biometric information was created, collected, stored, or disclosed by IBM.

13. Venue is proper under 735 ILCS 5/1-108 and 2-101 of the Illinois Code of Civil Procedure, as a substantial portion of the transactions giving rise to the causes of action pleaded herein occurred in Cook County. Specifically, upon information and belief, the activities giving rise to the causes of action occurred within the Village of Tinley Park, Illinois, where plaintiff resides and engaged in transactions relevant to his claim. Further, the sole defendant does not

reside in Illinois and, accordingly, pursuant to 735 ILCS 5/2-101, this action may be brought in any Illinois county.

FACTUAL BACKGROUND

I. Biometric Technology Implicates Consumer Privacy Concerns

14. "Biometrics" refers to unique physical characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific "biometric identifiers" (*i.e.*, details about the face's geometry as determined by facial points and contours), and comparing the resulting "face template" (or "faceprint") against the face templates stored in a "face template database." If a database match is found, an individual may be identified.

15. The use of facial recognition technology in the commercial context presents numerous consumer privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[3] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[4]

---

[3] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf (last visited Jan. 21, 2020).

[4] *Id.*

16. The Federal Trade Commission ("FTC") has raised similar concerns, and recently released a "Best Practices" guide for companies using facial recognition technology.[5] In the guide, the Commission underscores the importance of companies' obtaining affirmative consent from consumers before extracting and collecting their biometric identifiers and biometric information from digital photographs.

17. As explained below, IBM failed to obtain consent from *anyone* when it created its DiF Dataset.

II. Illinois's Biometric Information Privacy Act

18. In 2008, Illinois enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers[6] or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

740 ILCS 14/15 (b).

---

[5] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (last visited Jan. 21, 2020).

[6] BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (i.e., facial data obtained through facial recognition technology). *See* 740 ILCS 14/10.

19. Section 15(a) of BIPA also provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

20. As alleged below, IBM's practices of collecting, storing, and using class members' biometric identifiers and information derived from its DiF Dataset without informed written consent violate all three prongs of § 15(b) of BIPA. IBM's failure to provide a publicly available written policy regarding their schedule and guidelines for the retention and permanent destruction of individuals' biometric information also violates § 15(a) of BIPA. IBM's unauthorized disclose of biometrics to third parties also violates § 15(d) of BIPA.

III. IBM Violates Illinois's Biometric Information Privacy Act

21. Facial recognition technology is based on algorithms that learn how to recognize human faces and the hundreds of ways in which each one is unique. To do this well, the algorithms must be fed vast quantities of images of a diverse array of faces. To satisfy the ever growing demand for myriad high-resolution images of faces, unchecked companies have begun turning to the internet, where photographs are sometimes taken without the photographer's or subject's knowledge or consent. This has been called the "dirty little secret" of AI training sets. Researchers often just grab whatever images they can find "in the wild."

22. In 2014, Yahoo created the Yahoo Flickr Creative Commons 100 Million Dataset ("YFCC100M") as part of its Yahoo Webscope program, which was a reference library of scientific datasets. At release, the YFCC100M dataset purported to consist of 99.2 million

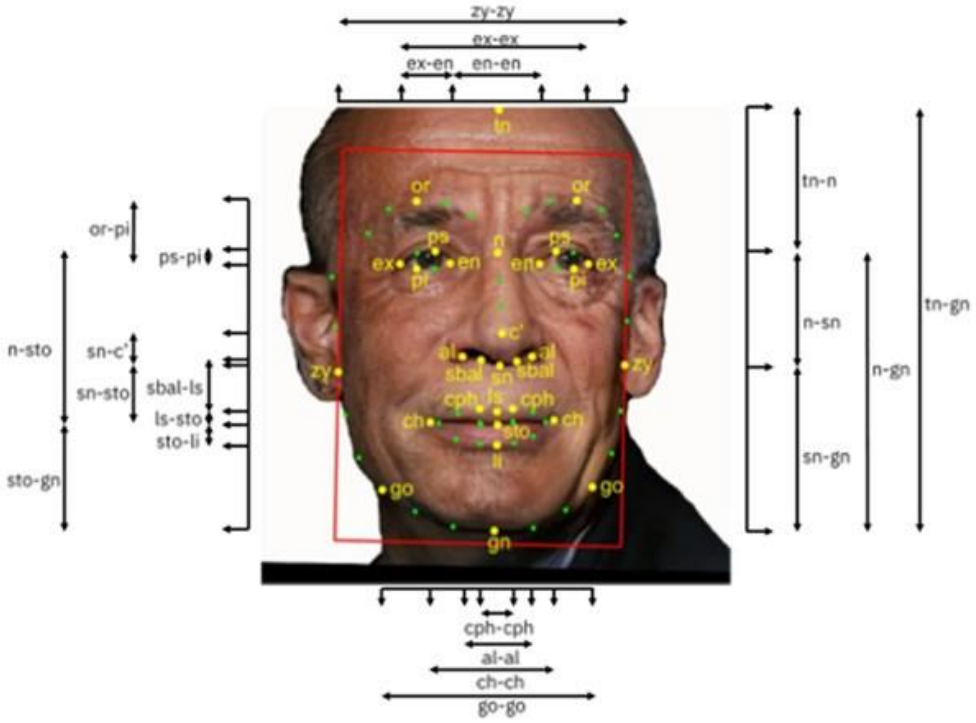
photographs uploaded to Flickr between 2004 and 2014. In addition to the photographs themselves, information uploaded to the YFCC100M dataset included the Flickr identifier, the user who created the photograph, the camera that took it, the time it was taken and uploaded, and the location where it was taken (if available). The title, description, and Flickr tags are also available, as are direct links to the photographs' Flickr page and content.

23. The photographs Yahoo took to create the YFCC100M dataset were taken from Flickr users without their knowledge or express consent, and were made publicly available to entities such as IBM.

24. In January of 2019, IBM released its DiF Dataset, which consists of photographs IBM obtained from the YFCC100M dataset. In creating its DiF Dataset, IBM culled through the photographs in the YFCC100M dataset to remove photographs it did not want to consider, such as photographs without faces, photographs that were not in color, or photographs with significant blur.

25. After culling the photographs to be used in its DiF Dataset, IBM processed the photographs to capture the biometrics of the faces appearing therein. Specifically, for every detected fact it extracted both pose and 68 key-points and processed each one by extracting at least ten facial coding schemes, including: 1) Craniofacial Distances (which characterize all the vertical distances between elements in a face: the top of the forehead, the eyes, the nose, the mouth, and the chin); 2) Craniofacial Areas (measures corresponding to different areas of the cranium, such as eye fissures and lips); 3) Craniofacial Ratios; 4) Facial Symmetry; 5) Facial Regions Contrast; 6) Skin Color; 7) Age Prediction; 8) Gender Prediction; 9) Subjective Annotation; and 10) Pose and Resolution.

26. The below figure illustrates the data points IBM employed as the basis for its extraction of class members' craniofacial measures for the first three coding schemes, *supra*.



27. Even more alarmingly, upon information and belief, IBM has released the highly confidential biometrics of the individuals whose faces appear in the photographs to the public, under the guise of advancing facial recognition research.

28. Unbeknownst to the Class members, and in direct violation of § 15(b)(1) of BIPA, IBM extracted geometric data relating to the unique points and contours (*i.e.*, biometric identifiers) of each face, and then used that data to create and store a template of each face – all without ever informing anyone of this practice.

29. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, IBM never informed Illinois residents who had their face templates collected of the specific purpose and length of term

for which their biometric identifiers or information would be collected, stored, and used, nor did IBM obtain a written release from any of these individuals.

30. In direct violation of § 15(a) of BIPA, IBM does not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying any of these biometric identifiers or information.

31. In direct violation of § 15(d) of BIPA, IBM disseminated this biometric information to third parties.

IV. Plaintiff Janecyk's Experience

32. Plaintiff is an accomplished photographer, having focused his work in portraiture and street life photography. Plaintiff has pioneered a certain style of portraiture that involves taking extreme close-ups of faces, often placing a wide-angle lens less about twelve inches from the subject's face. Plaintiff has taken many thousands of such photographs, and has taught several related photography classes.

33. Many of Plaintiff's subjects include strangers Plaintiff approaches on the streets in and near Chicago. While introducing himself to individuals, Plaintiff often assures them that he is taking their photographs as a hobbyist, that their photographs will not be used by other parties, and that the photographs will not be used for a commercial purpose. Plaintiff must sometimes invest time into building a relationship of trust before subjects will allow photographs— for instance, Plaintiff has spent several days building relationships with weary subjects at rallies and other sensitive events.

34. In 2008, Plaintiff signed up for a Flickr account in the Village of Tinley Park, and has since then uploaded in excess of a thousand of his photographs to Flickr.

35. Upon information and belief, IBM included at least seven of Plaintiff's photographs in its DiF Dataset. Once such photograph appearing in IBM's dataset, appearing below, depicts Plaintiff's own face.

36. As with other photographs in its DiF Dataset, IBM has, upon information and belief, captured biometrics from Plaintiff's photographs appearing in the dataset— including the picture of Plaintiff appearing above— by automatically locating and scanning Plaintiff's face, and by extracting geometric data relating to the contours of his face and the distances between his eyes, nose, and ears – data which IBM then used to create a unique template of Plaintiff's face.

37. The resulting unique face template was used by IBM, upon information and belief, for research purposes, to disseminate to other third-parties, and to further develop facial recognition technology.

38. Plaintiff's face template was also used to recognize his gender, age, and race.

39. Plaintiff never consented, agreed, or gave permission – written or otherwise – to IBM for the collection or storage of his unique biometric identifiers or biometric information.

40. Further, IBM never provided Plaintiff with, nor did Plaintiff ever sign, a written release allowing IBM to collect or store his unique biometric identifiers or biometric information.

41. Likewise, IBM never provided Plaintiff with an opportunity to prohibit or prevent the collection, storage, use, or dissemination of his unique biometric identifiers or biometric information.

42. Nevertheless, IBM took copies of Plaintiff's photographs, used them in its DiF Dataset, located Plaintiff's face in the photos, scanned Plaintiff's facial geometry, created a unique face template corresponding to Plaintiff, and shared the biometric data with third parties, all in direct violation of BIPA.

CLASS ALLEGATIONS

43. **Class Definition**: Plaintiff brings this action pursuant to 735 ILCS 5/2-801, individually and on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All citizens of Illinois who had their biometric identifiers, including scans of face geometry, collected, captured, received, or otherwise obtained by IBM from photographs in its Diversity in Faces Dataset.

The following are excluded from the Class: (1) any Judge presiding over this action and members of his or her family; (2) IBM, IBM's subsidiaries, parents, successors, predecessors, and

any entity in which IBM or its parent has a controlling interest (as well as current or former employees, officers, and directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and IBM's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

44. **Numerosity**: The number of persons within the Class is substantial, believed to amount to millions of persons. It is, therefore, impractical to join each member of the Class as named plaintiffs. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation.

45. **Commonality and Predominance**: There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member include, but are not limited to, the following:

(a) whether IBM collected or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

(b) whether IBM properly informed Plaintiff and the Class that it collected, used, and stored their biometric identifiers or biometric information;

(c) whether IBM obtained a written release (as defined in 740 ILCS 1410) to collect, use, and store Plaintiff's and the Class's biometric identifiers or biometric information;

(d) whether IBM developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, whichever occurs first;

(e) whether IBM used Plaintiff's and the Class's biometric identifiers or biometric information to identify them;

(f) whether IBM wrongfully disclosed Plaintiff's and the Class's biometric identifiers or biometric information to third parties; and

(g) whether IBM's violations of BIPA were committed intentionally, recklessly, or negligently.

46. **Adequate Representation**: Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Neither Plaintiff nor his counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff is able to fairly and adequately represent and protect the interests of such a Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

47. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent, or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system, and protects the rights of each member of the Class. Plaintiff

anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiff and the Class)

48. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

49. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b) (emphasis added).

50. IBM is a New York corporation and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

51. Plaintiff and Class members are individuals who had their "biometric identifiers," including scans of their face geometry, collected, captured, received, or otherwise obtained by IBM from photographs that IBM included in its DiF Dataset from within the state of Illinois. *See* 740 ILCS 14/10.

52. Plaintiff and Class members are individuals who had their "biometric information" collected by IBM (in the form of their gender, age and location) through IBM's collection and use of their "biometric identifiers."

53. IBM violated BIPA by systematically and automatically collecting, using, and storing Plaintiff's and Class members' biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

54. IBM violated BIPA by failing to properly inform Plaintiff or the Class in writing that their biometric identifiers and/or biometric information were being "collected or stored" in connection with IBM's DiF Dataset, and failing to inform Plaintiff or Class members in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)-(2).

55. IBM violated BIPA by not publicly providing a retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information of Plaintiff or Class members, as required by BIPA. *See* 740 ILCS 14/15(a).

56. IBM violated BIPA by wrongly disclosing the highly sensitive biometric identifiers and/or biometric information of Plaintiff or Class members with third parties. *See* 740 ILCS 14/15(d).

57. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, IBM violated BIPA and the rights of Plaintiff and each Class member to keep private these biometric identifiers and biometric information.

58. Individually and on behalf of the proposed Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring IBM to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) statutory damages of $5,000.00 for each of the intentional and reckless violations of BIPA pursuant to 740 ILCS 14/20 (2), or alternatively, statutory damages of $1,000.00 pursuant to 740 ILCS 14/20(1) if the Court finds

that IBM's violations were negligent; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, Tim Janecyk, individually and on behalf of the proposed Class, respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that IBM's actions, as set forth above, violate BIPA, 740 ILCS l4/1, *et seq.*;

C. Awarding statutory damages of $5,000.00 for each and every intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000.00 pursuant to 740 ILCS 14/20(1) if the Court finds that IBM's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an order requiring IBM to collect, store, and use biometric identifiers or biometric information in compliance with BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

Dated: January 22, 2020

By: */s/ Katrina Carroll*
Katrina Carroll
kcarroll@carlsonlynch.com
Kyle A. Shamberg
kshamberg@carlsonlynch.com
Nicholas R. Lange
nlange@carlsonlynch.com
CARLSON LYNCH LLP
111 West Washington Street, Suite 1240
Chicago, Illinois 60602
Telephone: (312) 750-1265
Firm ID: 63746

Counsel for Plaintiff and the Putative Class