

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

REBECCA ROBERTS,
*individually and on behalf of all
others similarly situated,*

Plaintiff,

v

COOLER SCREENS INCORPORATED,

Defendant.

Case No.
2022CH01824

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Rebecca Roberts (“Plaintiff”), individually and on behalf of all other persons similarly situated, by and through undersigned counsel, brings this class action lawsuit for violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), against Defendant Cooler Screens, Incorporated (“Cooler Screens”). Plaintiff alleges the following facts based upon personal knowledge and/or the investigation of her counsel:

NATURE OF THE ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Cooler Screens in capturing, collecting, storing, and using Plaintiff’s and other similarly situated individuals’ biometric identifiers¹ and biometric information² (collectively, “biometrics”) without first obtaining informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

2. Cooler Screens, Inc. is the developer of “Smart Coolers,” which are interactive

¹ A “biometric identifier” is defined as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.

² “Biometric information” means “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” 740 ILCS 14/10.

digital displays currently replacing glass doors in retail store aisles³ and support “the world’s largest in-store digital retail media platform.”⁴

3. In November of 2018, Illinois residents were exposed to Cooler Screen’s Smart Cooler for the first time, as they began to be installed Walgreens locations. To a consumer unfamiliar with the Smart Cooler, it functions like a new-age television screen which displays advertisements for the items available for sale within the cooler. An example of a retailer’s Smart Cooler display⁵ appears as follows:

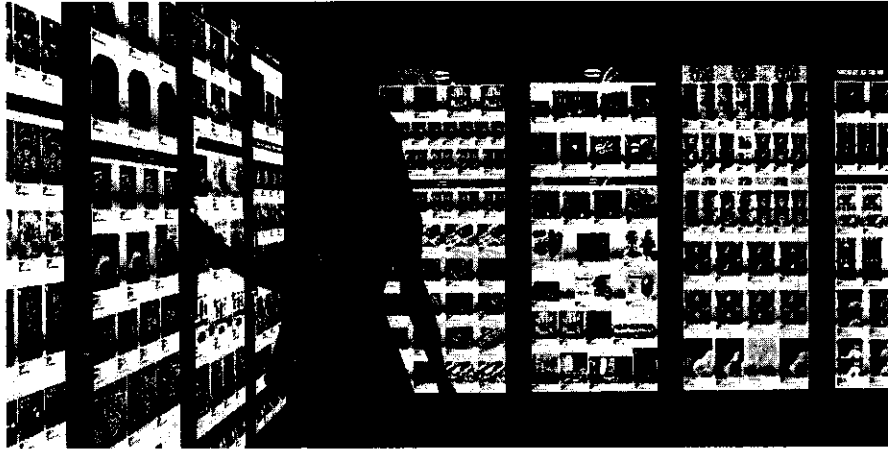


Figure 1

4. But Cooler Screens’ Smart Cooler is more than simply point-of-sale advertising – by bringing the dynamic nature of digitized marketing into the retail shopping experience, Cooler Screens has developed a new medium for deploying targeted advertising to consumers at their most vulnerable moment and increase the pressure to make an impulse purchase.

5. According to Cooler Screens, Inc.: “Over 75% of shopping in brick-and-mortar stores is impulse purchasing. Research shows that impulse decisions are highly influenced by in-store messaging, and that most of that in-store impulse shopping occurs at retail product containers,

³ Cooler Screens, <https://www.coolerscreens.com/> (accessed 2/23/22).

⁴ Cooler Screens, *Platform*, <https://www.coolerscreens.com/platform> (accessed 2/23/22).

⁵ Cooler Screens, *Ecosystem*, <https://www.coolerscreens.com/ecosystem> (accessed 2/28/22).

such as coolers and freezers.”⁶

6. The Smart Cooler employs a “camera which feeds images of each customer into a computer that guesstimates her sex and age. In addition, the system uses an iris tracker to detect exactly where the customer is looking.”⁷ The cameras in the Smart Coolers are extremely subtle, such that most consumers would not realize it is monitoring and analyzing her person – much less predicting which advertisements will most effectively influence her to purchase.

7. The technology monitors shoppers using its Customer Detection Hardware (“CDH”) and interprets the data collected from them using a “facial profiling system⁸,” which can detect the age, gender, and emotional response⁹ of over 3 million verified daily viewers.¹⁰

8. Multiple Smart Coolers can be linked together to form a single system using a “controller/data collector” (“C/DC”), which receives a data feed from various sensors embedded into each Smart Cooler. The C/DC not only links a set of Smart Coolers together, but also communicates with each Smart Cooler independently, analyzing the data stream it receives from each cooler and, depending on the type of customer standing before a particular door, predict which advertisements will most likely lead to a purchase.¹¹

⁶ USPTO, *Intelligent Marketing and Advertising Platform*, <https://uspto.report/patent/app/20190122263#D00000> (accessed 2/20/22).

⁷ Boston Globe, *Cooler Screens Display Cases Scan your Face Size to Size up Buying Habits* <https://www.bostonglobe.com/business/2019/03/10/cooler-screens-display-cases-scan-your-face-size-your-buying-habits/qNN4bCb7NYhhE7TE3GjxwK/story.html> (accessed 2/20/22).

⁸ *Id.*

⁹ Fast Company, *It's Not Just Google or Facebook: The Freezer Aisle is Ad Targeting You Now*, <https://www.fastcompany.com/90302382/its-not-just-google-or-facebook-the-freezer-aisle-is-ad-targeting-you-too> (accessed 2/23/22).

¹⁰ Cooler Screens, *Cooler Screens* (accessed 2/23/22).

¹¹ USPTO, (accessed 2/20/22).

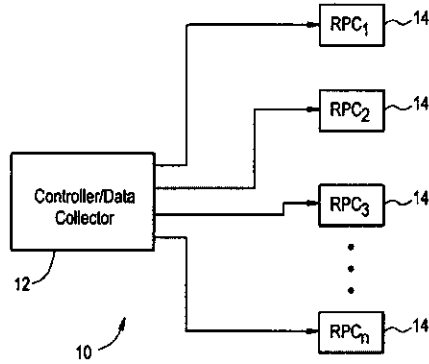


Figure 2
(The C/DC operates as a central hub for a set of Retail Product Containers ("RPCs"), normally coolers or freezers)

9. The entire Cooler Systems ecosystem is built around the concept that serving the right advertisement at the right time and *to the right consumer* will move the needle and sell more products. As part of this service, Cooler Screens performs a variety of analytics to accurately predict the success of an advertising campaign. Cooler Screens leverages this data and its analytics to pitch the optimal conditions and the optimal audience for specific advertising.¹²

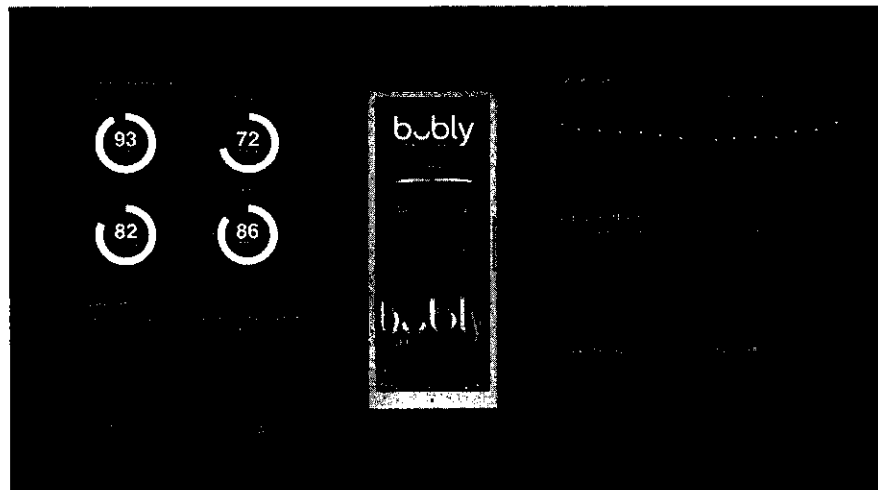


Figure 3

¹² Cooler Screens, *Platform*, (accessed 2/20/22).

10. However, Cooler Screens provides its advertising service in violation of Illinois law. BIPA has strict requirements regarding what disclosures must be made and how consent must be obtained *before* biometrics are obtained from the user. Cooler Screens does not provide sufficient disclosures and does not obtain consent. Further, Cooler Screens does not meaningfully explain how it retains the biometrics it obtains.

11. Accordingly, Cooler Screen's conduct violates BIPA.

12. In promulgating BIPA over a decade ago, the Illinois Legislature declared 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.*

13. In recognition of these and other concerns over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity—like Cooler Screens—may *not* obtain and/or possess an individual's biometrics unless it first establishes a written and publicly-available retention schedule. 740 ILCS 14/15(a). Additionally, it must also: (1) inform the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) inform the subject or the subject's legally authorized representative 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) receive 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). The entity is expressly prohibited from selling, leasing, trading or otherwise profiting from the individual's

biometrics. 740 ILCS 14/15(c). Nor may the entity disclose, redisclose, or otherwise disseminate an individual's biometrics absent written consent. 740 ILCS 14/15(d).

14. Further, the entity must store, transmit and protect an individual's biometric identifiers and biometric information using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information. 740 ILCS 14/15(e).

15. In direct violation of BIPA, Cooler Screens is actively collecting, capturing, storing, using, and profiting from the facial geometry and associated personally identifying information (including biometrics) of potentially tens of thousands of persons, without providing notice, obtaining informed written consent, or publishing data retention policies.

16. Plaintiff, on behalf of herself and the class as defined herein, brings this action to prevent Cooler Screens from further violating the privacy rights of citizens within the state of Illinois, and to recover statutory damages for Cooler Screens' unauthorized collection, capture, storage and use of individuals' biometrics in violation of BIPA.

JURISDICTION AND VENUE

17. Defendant Cooler Screens is subject to the personal jurisdiction of this Court because it is headquartered in the State of Illinois and regularly transacts business within the State of Illinois. Further, the biometrics that give rise to this lawsuit (1) belong to Illinois residents, and (2) were collected by Defendant from customers shopping in front of Smart Coolers in Illinois.

18. Venue is proper in this County pursuant to 735 ILCS 5/2-101 because Defendant is a resident of this County and a substantial part of the events giving rise to Plaintiff's cause of action occurred in this County.

PARTIES

19. Plaintiff Rebecca Roberts is, and has been at all relevant times, a resident of Illinois.

20. Defendant Cooler Screens is an advertising and technology corporation based in Chicago, Illinois. Cooler Screens does business in the State of Illinois. Specifically, Cooler Screens has installed many of its Smart Coolers in the State of Illinois.

BACKGROUND

I. The Illinois Biometric Information Privacy Act

21. 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.

22. A “biometric identifier” is defined as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.

23. In turn, “biometric information” means “any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.” 740 ILCS 14/10.

24. 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 biometrics, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative 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).

25. Section 15(a) of BIPA also provides that:

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. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

Id. at 14/15(a).

26. Further, BIPA prohibits a “private entity in possession of a biometric identifier or biometric information” from “sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information.” 740 Ill. Comp. Stat. Ann. 14/15(c).

27. Nor may a private entity “disclose, redisclose, or otherwise disseminate an individual's biometrics absent written consent.” 740 ILCS 14/15(d).

28. Finally, BIPA places significant security requirements on private entities that acquire individuals' biometrics, stating that they must: “(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.” 740 ILCS 14/15(e).

II. Cooler Screens' BIPA-Violative Conduct

A. Cooler Screens Use of “face sensors or scanners” and iris tracking hardware amounts to a collection of biometrics.

i. Facial Detection, Generally

29. Facial detection “is the first and essential step for face recognition,” and is used as a preliminary step to detect faces in images. It is a part of object detection and is used in many areas, including biometrics.¹³ Facial detection “is used to detect faces in real time for surveillance and tracking of [a] person or objects.”¹⁴

30. Typically, facial detection technology uses algorithms and machine-learning to locate human faces within larger images.¹⁵ Face detection algorithms, such as the algorithm employed by Cooler Screens, Inc., begin by scanning a collected image to locate human eyes – one of the easiest features to detect. The technology then attempts to detect other features of the face, such as eyebrows, the mouth, nose, nostrils, and the iris.”¹⁶

31. When an algorithm has successfully classified a sufficient number of facial data points within an image (i.e., eyes, mouth, nose, nostrils, and iris), it applies additional tests to confirm the object within the image is, in fact, a face.¹⁷

32. In training an algorithm to recognize the types of features to identify as belonging to a face, thousands of images are “fed” to the algorithm for it to determine whether a feature belongs to a specific portion of a face, even between images of different faces (i.e., recognizing that an object is a “nose” in an image of Kim Kardashian as well as in an image of Abraham Lincoln). If data collected from subsequent images sufficiently track the mapped data points from

¹³ See, Divyanch Dwivedi, *Face Detection for Beginners*, Towards Data Science (available at <https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9>) (last accessed 2/23/22)

¹⁴ *Id.*

¹⁵ See, generally, Corrine Bernstein, *Face Detection*, Search Enterprise AI (available at <https://searchenterpriseai.techtarget.com/definition/face-detection>) (last accessed June 2, 2021)

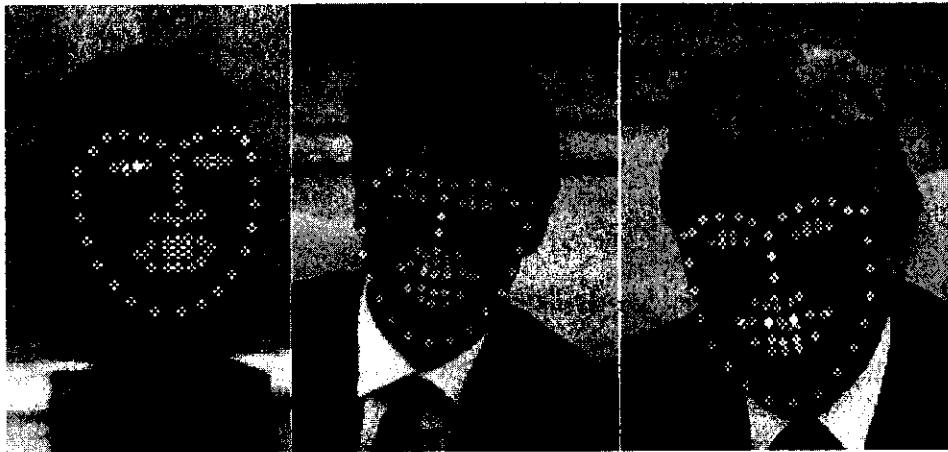
¹⁶ *Id.*; see, also, OpenCV, *Cascade Classifier*, (available at https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html) (last accessed June 2, 2021)

¹⁷ See, generally, Bernstein, *Face Detection*, fn 8, *supra*.

prior images of faces, the machine-learning algorithm can successfully detect whether an image contains a face.¹⁸

33. The above-described procedures rely on “facial landmark detection,” which is a method of identifying specific “landmarks” on the face (eyes, nose, cheeks, etc.) for facial detection.¹⁹ But facial landmark detection is capable of even more sophisticated analyses of the facial geometry scans it acquires, enabling technology companies like Cooler Screens to evaluate images and make judgments about the physical qualities of the person in the image.²⁰

34. Facial landmark detection is critical for technology employed by Cooler Screens, Inc., such as its iris-scanner, which is embedded in the Smart Cooler.²¹ Like facial detection more broadly, facial landmark detection necessarily relies on the expansive collection of facial data points (i.e., facial geometry) and analysis of those data points to divine unique attributes of the scanned individual, as illustrated below:²²



Zoomed output

Figure 4

¹⁸ See, generally, Bernstein, *Face Detection, supra*.

¹⁹ See, Oluwatosin, *Facial Landmarks and Face Detection in Python with OpenCV, supra*.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

ii. The Cooler Screens Experience

35. Cooler Screens was designed with the goal to create a “consumer experience” which generated a “continuous loop” of advertising and purchasing.²³ The Smart Coolers are intended to draw a shopper towards the Retail Product Container, engage with the customer, and ultimately supply the extra push to make an impulse purchase.

36. The system was deliberately designed to lure customers closer to the products³ and, as illustrated by Figure 5, initiate a continuous engagement loop with the products.²⁴

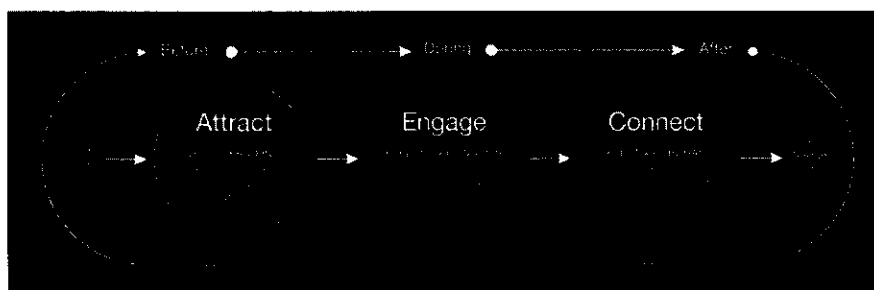


Figure 5

37. The cooler displays bright, exciting full-screen or multi-door ads when no consumers are nearby. as a consumer approaches the screen, it will replace the full-screen or multi-door advertisement with an image reflecting all items available within the RPC and their prices. The system also displays more subtle advertising as well, such as providing nutritional product information or whether the product is organic or locally produced.²⁵

38. The system is capable of displaying five types of advertising²⁶: full screen ads, multi-door/wall ads, banner ads, hotspot ads, and promotional labels, tags, and animations.

²³ Cooler Screens, *Experience*, <https://www.coolerscreens.com/experience> (accessed 2/28/22).

²⁴ *Id.*

²⁵ Tech Crunch, *Cooler Screens Raises \$80M to Bring Interactive Screens into Cooler Aisles*, <https://techcrunch.com/2020/10/05/cooler-screens-series-c/>, (accessed 2/20/22). *see also* Cooler Screens, *Platform*, (accessed 2/20/22).

²⁶ Cooler Screens, *Platform*, (accessed 2/20/22).

39. The system is also capable of ensuring the advertising on the screen represents accurate information, such as updated prices, promotional bargains, and accurate representations of inventory within the RPC.²⁷

iii. **Cooler Screens Collects Scans of Facial Geometry**

40. Each Smart Cooler delivers a variety of information to the C/DC through various sensors, including what Cooler Screens calls “Customer Detecting Hardware.” This hardware includes “one or more proximity sensors (such as heat maps), cameras, facial sensors or scanners, and eye-sensors.”²⁸

41. In particular, the system detects the presence of a customer using a proximity sensor, and when in close range of the cooler door, will begin collecting images of the consumer using its cameras. It will also capture information about the consumer using its face sensors or scanners, and its eye-sensors.²⁹

42. Along with other sensors within the Retail Product Container, the customer’s physical appearance will be collected and analyzed and then associated the customer’s behavior, tracking whether a product was viewed or selected. Sensors in the Smart Cooler “can tell how close shoppers are to the screen and can also gauge if they’ve seen an ad, what they’re looking for, if they open and close a door, and if they’ve gone for a diet coke or a kombucha.”³⁰

43. The system will collect images of the consumer within the C/DC and perform a local analysis of the image to determine the customer’s age, sex, and, and emotional state.³¹ Specifically: “[a] camera feeds images of each customer into a computer that guesstimates

²⁷ Marketing Brew, *Are Cooler Screens the Fridge of the Future*, <https://www.morningbrew.com/marketing/stories/2021/10/25/are-cooler-screens-the-fridge-of-the-future> (last accessed February 20, 2022)

²⁸ USPTO, at 0035 (accessed 2/20/22).

²⁹ *Id.*

³⁰ Marketing Brew, (accessed 2/20/22).

³¹ USPTO, (accessed 2/20/22).

his or her sex and age. In addition, the system uses an iris tracker to detect exactly where the customer is looking. Do the eyes come to rest on a bottle of Mountain Dew, or does the shopper fancy a Diet Snapple?”³²

44. “The cameras analyze faces to make inferences about the shoppers’ age and gender. First the camera takes their picture, which an AI system will measure and analyze, say, the width of someone’s eyes, the distance between their lips and nose, and other micro measurements. From there, the system can estimate if the person who opened the door is, say, a woman in her early 20s or a male in his late 50s. It’s analysis, not recognition.”³³

45. Further, the Smart Cooler system requires its cameras to satisfy certain metrics in order to provide its analytics:

For example, its cameras “should have a depth of view of 20 feet or more, range of field of view of 170 degrees with 150 degrees of facial recognition ability. Preferably software is employed in association with the cameras to monitor shopper interactions, serve up relevant advertisement content on the displays, and track advertisement engagement in-store.”³⁴

46. The Customer Detection Hardware monitors the customer and feeds its data to the C/DC via a wired or wireless connection.³⁵ The C/DC analyzes the data feed locally, but also transmits the data remotely for additional analysis in the cloud which permits Cooler Screens to “push more relevant/targeted content, tailored for the consumer.”³⁶

47. Critically, a customer in a store that has installed a set of cooler screens has no ability to avoid collection of her biometrics as the system is constantly in operation, and, even

³² Boston Globe, (accessed 2/20/22).

³³ The Atlantic, *Now your Groceries See you, Too*.

<https://www.theatlantic.com/technology/archive/2019/01/walgreens-tests-new-smart-coolers/581248/> (accessed 2/20/22).

³⁴ USPTO, at 0036 (accessed 2/20/22).

³⁵ *Id.*

³⁵ *Id.*

³⁶ *Id.*, at 0053.

more invasive, the system is designed in such a way that a consumer has no obvious warning a camera, face scanner, and iris tracker are collecting and analyzing her image.

iv. **Cooler Screens Provides No Notice and Obtains No Consent from the Consumer**

48. However, Cooler Screens takes no steps to provide notice to consumers, or anyone for that matter, that it collects biometric identifiers or biometric information. In fact, Cooler Screens' Privacy Policy does not even mention the acquisition of biometrics.³⁷

49. Not only does it fail to notify the public it collects scans of face geometry, but it also fails to include a retention policy for biometric data and fails to include guidelines for the destruction of biometric data – both of which are required under 740 ILCS 14/15(a).³⁸

50. Cooler Screens takes no effort to obtain informed written consent from consumers as required by 740 ILCS 14/15(b). Cooler Screens provides no written notice that its Smart Cooler and associated equipment collect biometric information or biometric identifiers, the specific purpose and length of term for which the biometric data will be stored or used and does not attempt to obtain a written release from the subject of the scan of face geometry.

B. Cooler Screens Scans Facial Geometry to Serve Targeted Advertising

51. Cooler Screens is quite transparent about the purpose of its technology, as illustrated by its own language:

“The intelligent marketing and advertising platform disclosed herein effectively prides for at least the following: the convergence of a brick and mortar retail establishment with e-commerce; in-store promotions as an electronic marketplace; real time and algorithmic-driven pricing and promotions; *self-learning/machine-learning artificial intelligence algorithm-driven advertising which is personalized to a given consumer; behavior response and external data (i.e. weather, events, competition, etc.);* and smart-

³⁷ Cooler Screens, *Privacy Policy*, <https://www.coolerscreens.com/privacy-policy>, (accessed 2/20/22) (effective date January 7, 2020).

³⁸ *Id.*

sensor and digital merchandising for planogram compliance, automatic-restock, in-store audits, etc.”³⁹

52. In fact, Cooler Screens’ entire business model is based on the collection and analysis of consumers’ faces and predicting their purchasing interests based on its estimates of gender, age, and mood, and serving relevant advertising. Its ecosystem is built around the concept that serving the right advertisement at the right time and to the right consumer will move the needle and sell more products.

53. According to Cooler Screens’ patent applied for in 2019 and granted in 2020, the company developed an “intelligent marketing and advertising platform”(“IMAP”), which is designed to capture and evaluate data in order to provide the consumer with the most effective advertisement to obtain a purchase.⁴⁰ Upon detecting the presence of a customer, the customer-facing camera will direct the C/DC to display the planogram of available items and will suggest banner ads and hot spots depending on what information it gleans from the analysis of the customer.⁴¹ Cooler Screens illustrates this functionality on its website:

³⁹ USPTO, (accessed 2/20/22) (emphasis added).

⁴⁰ *Id.*

⁴¹ *Id.*

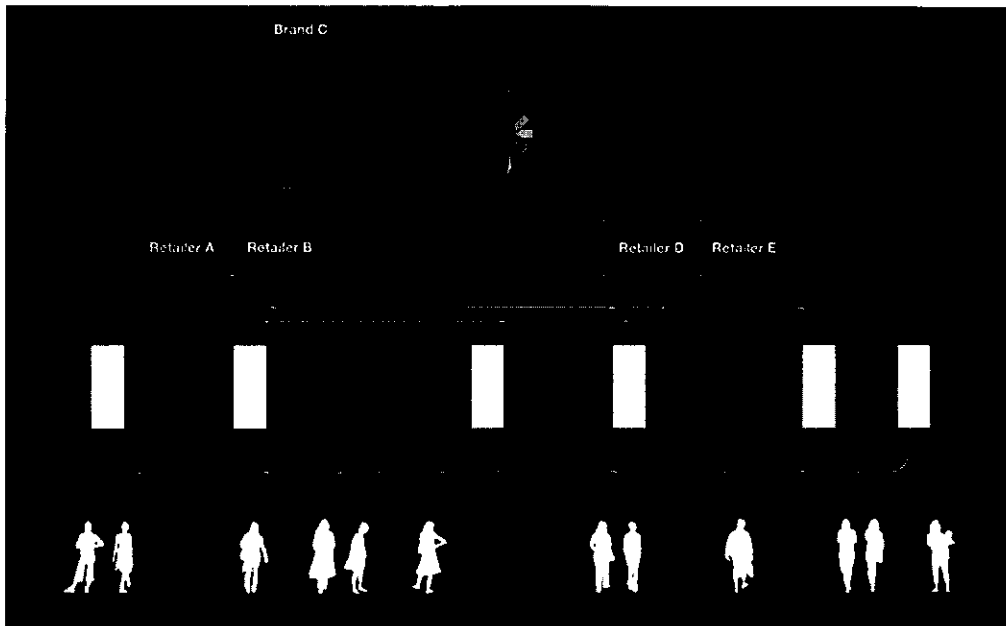


Figure 6

54. The system is further designed to improve as consumers repeatedly engage with it. Cooler Screens engages in sophisticated analytics of the data it collects, including the demographic data it collects on retail shoppers, the types of ads displayed for particular demographics including the location of the retail establishment, the time of day, and the frequency with which the advertisement led to a purchase.⁴²

55. “If, for example, Pepsi launched an ad campaign targeting young women, it could use smart-cooler data to see if its campaign was working. These machines can draw all kinds of useful inferences: maybe young men buy more Sprite if it’s displayed next to Mountain Dew. Maybe older women buy more ice cream on Thursday nights than any other day of the week. The tech also has “iris tracking” capabilities, meaning the company can collect data on which displayed items are the most looked at.”⁴³

⁴² Cooler Screens, *Platform*, (accessed 2/20/22).

⁴³ The Atlantic, (accessed 2/20/22).

56. Cooler Screens then works with advertisers to provide analytics of the type of advertising displayed and report back how well the advertisement transitioned a consumer to make an actual purchase.⁴⁴ This gives the system the ability to employ strategies similar to those used in the online marketing platform which allows suppliers to monitor mouse movements and page and advertisement clicks. Instead of monitoring a consumer's online behavior, however, the Smart Cooler monitors the consumer's physical attributes and predicts which ad may be most effective.⁴⁵

57. "The Cooler Screens system instantly analyzes all of this data, then starts displaying ads on the cooler door. A middle-aged woman might see a suggestion that she pick up a pint of Ben & Jerry's ice cream to go with her Diet Coke; a twenty-something male could be enticed with a discount on frozen pizza."⁴⁶

Plaintiff's Experience

58. Plaintiff often shops at the Walgreens on 1200 N Dearborn St in Chicago, Illinois. At some point during the last year, the traditional transparent glass doors on the refrigerators were replaced with Cooler Screens' Smart Cooler. Since that time, Plaintiff has made frequent trips to this Walgreens and stepped in front of a Cooler Screens Smart Cooler where her biometrics were obtained by Cooler Screens without her consent.

59. Plaintiff is an Illinois resident who had her biometrics taken by Cooler Screens' Smart Cooler while in the state of Illinois. Plaintiff's only option to avoid the Smart Cooler was to not shop in her neighborhood Walgreens at all. Plaintiff was not aware the Smart Cooler was capturing her age, gender, and mood in order to target her with advertisements.

⁴⁴ Cooler Screens, *Platform*, (accessed 2/20/22).

⁴⁵ Boston Globe, (accessed 2/20/22).

⁴⁶ *Id.*

60. In the course of shopping at Walgreens, Plaintiff was scanned by Cooler Screens Customer Detecting Hardware and analyzed by Cooler Screens' software in a manner substantially similar—if not identical—to the processes set forth in paragraphs 29-57.

61. In so doing, Defendant's technology scanned, captured and collected Plaintiff's facial geometry—along with any other biometrics—and stored this data.

62. Defendant did not inform Plaintiff in writing that it was capturing and collecting her biometrics, the purpose and length of time for such collection, nor did Defendant obtain Plaintiff's written consent before capturing her biometrics. Plaintiff never consented, agreed or gave permission—written or otherwise—to Defendant for the collection or storage of Plaintiff's biometrics.

63. Likewise, Defendant never provided Plaintiff with the requisite statutory disclosures nor an opportunity to prohibit or to prevent the collection, storage or use of her biometrics.

64. By collecting her biometrics without Plaintiff's consent, Defendant invaded Plaintiff's statutorily protected right to privacy in her biometrics.

CLASS ALLEGATIONS

65. Plaintiff brings this action pursuant to Illinois Code of Civil Procedure Section 2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

All individuals who are Illinois residents who had their biometrics collected, captured, received, or otherwise obtained, by Defendant in the State of Illinois during the statutory period.

66. **Numerosity**: the number of persons within the Class is substantial, believed to amount to thousands of persons or more. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Accordingly, utilization of the class action mechanism is the most

economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from advertisements and self-identifying affidavits.

67. **Commonality & 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 Defendant captured, collected, or otherwise obtained Plaintiff's and the Class's biometrics;
- (b) whether Defendant properly informed Plaintiff and the Class that it captured, collected, used, and stored their biometrics;
- (c) whether Defendant obtained a written release to capture, collect, use, and store Plaintiff's and the Class's biometrics;
- (d) whether Defendant discloses, rediscloses, or otherwise disseminates Plaintiff's and the Class's biometrics absent consent; and
- (e) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

68. **Typicality and Adequate Representation**: Plaintiff, who like other members of the putative class, had her biometrics captured and retained by Defendant, has claims that are typical of the class. Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex privacy class action litigation. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of such a Class. Neither Plaintiff nor her counsel have any interest adverse to, or in conflict with, the interests of the absent members of the 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.

69. **Propriety of Class Treatment**: 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 invest the time and expense necessary 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 and legal issues. By contrast, the maintenance of this action as a class action 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 compliance with BIPA.

CLAIMS FOR RELIEF

COUNT I VIOLATION OF 740 ILCS 14/15(b) Failure to Obtain Informed Written Consent and Release Before Obtaining Biometrics

70. Plaintiff incorporated the foregoing allegations as if fully set forth herein.

71. BIPA requires a private entity in possession of biometrics to publish a retention schedule and guidelines for the destruction of biometric data. Cooler Screens publishes a privacy policy on its website which applies to a user of the website in addition to any person who interacts with the Smart Coolers.

72. Cooler Screens patent and features indicate analysis of the consumers' physical person is collected to provide relevant advertising.

73. Cooler Screens has no statements related to retention periods for any data nor does it include statements related to the destruction of any data collected by its website or its coolers.

74. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometrics as described herein; (3) statutory damages of \$5,000 for each intentional and/or reckless violation of BIPA or, in the alternative, statutory damages of \$1,000 for each negligent violation of BIPA; and (4) reasonable attorneys' fees and costs and other litigation expenses. *See* 740 ILCS 14/20.

COUNT II
VIOLATION OF 740 ILCS 14/15(b)
*Failure to Obtain Informed Written Consent
and Release Before Obtaining Biometrics*

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

76. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] 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).

77. Defendant fails to comply with these BIPA mandates.

78. Defendant systematically and automatically captured, collected, used, stored and disseminated Plaintiff's and the Class's biometrics without first obtaining the written release required by 740 ILCS 14/15.

79. Defendant never informed Plaintiff and the Class in writing that their biometrics were being captured, collected, stored, used and disseminated, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s) and length of term for which their biometrics were being collected, stored, used and disseminated as required by 740 ILCS 14/15.

80. By capturing, collecting, storing, using and disseminating Plaintiff's and the Class's biometrics as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometrics as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

81. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, storage, use and dissemination of biometrics as described herein; (3) statutory damages of \$5,000 for each intentional and/or reckless violation of BIPA or, in the alternative, statutory damages of \$1,000 for each negligent violation of BIPA; and (4) reasonable attorneys' fees and costs and other litigation expenses. *See* 740 ILCS 14/20.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the proposed Class, respectfully requests 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 her counsel as Class Counsel;

- B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;
- C. Awarding statutory damages of \$5,000.00 for each and every intentional and reckless violation of BIPA, or alternatively, statutory damages of \$1,000.00 for each and every negligent violation of BIPA;
- D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Defendant to comply with BIPA;
- E. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses;
- 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 DEMAND

Plaintiff demands a trial by jury on all claims and issues so triable.

Dated: March 3, 2022

Respectfully submitted,

s/ Courtney E. Ross

Plaintiff's Attorney

Courtney E. Ross (Bar No. 6340021)
CARNEY BATES AND PULLIAM, PLLC
519 W. 7th St.
Little Rock, AR 72201
T: 501.312.8500
cross@cbplaw.com

Counsel for Plaintiff and the proposed class