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

ISELA CARMINE, on behalf of herself and all others similarly situated,	)	
Plaintiff,	)	
	)	Case No. 20-cv-4589
vs.	)	
MACY'S RETAIL HOLDINGS, INC.,	)	Jury Demanded
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Isela Carmine, on behalf of herself and a putative class ("Plaintiff" or "Carmine"), brings this Class Action Complaint against Macy's Retail Holdings, Inc. ("Macy's") and alleges the following:

Introduction

1. A New York Times article published on January 18, 2020 introduced Americans to the then relatively unknown company Clearview AI, Inc ("Clearview"). The article described a dystopian surveillance database, owned and operated by a private company and leased to the highest bidder.

2. On February 27, 2020, BuzzFeed News released an article based on a review of Clearview's documents, revealing that Clearview is working or contracted with over 2,200 law enforcement agencies, companies, and individuals around the world.

3. The same article and subsequent reporting by several news outlets revealed that Defendant Macy's, among other private businesses and government entities, was using Clearview's surveillance database to aid in its operations.

4. Macy's has run the identities of over six thousand individual customers through the database.

5. Clearview AI's database includes the photographs, and personal and private data, including names, home addresses, and work addresses, of millions of Americans. Clearview acquired the billions of data points by "scraping" or harvesting the data from publicly available internet-based platforms such as Facebook, Instagram, and Twitter.

6. Clearview's database is unique – it has run every one of the 3 billion photographs it has acquired through facial recognition software to extract and index the unique biometric data from each face. The database thus also contains the biometric identifiers and information of millions of Americans. Any private citizen can be identified by uploading a photo to the database. Once identified, the end-user – here Macy's – then has access to all of the individual's personal details that Clearview has also obtained.

7. Macy's acquisition and use of consumer's biometric information and identifiers is illegal in Illinois.

8. Macy's practice of identifying and tracking their customers using Clearview's illegal surveillance database is unfair and directly violates each customers' right to privacy.

Parties

9. Plaintiff Isela Carmine is a natural person and resident of this district. She maintains an active presence on social media, including Facebook and Instagram. She also uses Venmo to make and accept payments to other individuals. Carmine is a regular customer at Macy's.

10. Defendant Macy's Retail Holdings, Inc. is a Delaware corporation, doing business in Illinois, with twenty-one department stores in the state.

Jurisdiction

11. This Court has jurisdiction under 28 U.S.C. § 1332(d)(2) and the Class Action Fairness Act ("CAFA") because there are 100 or more members of the class, the parties and putative class members are minimally diverse and the aggregate amount in controversy is greater than $5,000,000.

12. This Court has personal jurisdiction over Macy's because they conduct a substantial amount of business here which forms the basis of Plaintiff's claims. Macy's operates multiple stores in Illinois and is registered to do business in this state.

13. Venue is proper here under 28 U.S.C. § 1391(b)(2) because a substantial amount of the acts and omissions giving rise to the claims occurred in Illinois.

Macy's Surveillance and Clearview's Database

14. Clearview 'scrapes,' 'harvests,' or otherwise obtains information and photos of millions of Americans from the internet, in particular social media platforms like Facebook and Instagram. That is, they use automated software or processes to obtain massive amounts of data without the consent or knowledge of the platform users.

15. Macy's stores are equipped with video surveillance that captures the images of its visitors and customers.

16. Macy's sends or has sent pictures of persons who have visited its stores to Clearview, to identify the people in the pictures and obtain their personal information.

17. Clearview then runs the photos through facial recognition software which identifies the photos that contain faces.

18. The faces are then processed by Clearview's software, and their biometric data is extracted. The biometric data is a collection of vectors and/or other data points that allows faces to be classified, searched and indexed.

19. Clearview's database links the biometric data to the other data Clearview has scraped so an end-user, like Macy's, can find out where the photos came from along with a significant amount of personal and private details about a given individual.

20. In short, anyone with access to the database, including a reseller of the database or end-user, can upload a single photo and identify the person in real-time. A single picture on the internet means that any private citizen can immediately be identified and tracked.

21. Clearview sells or leases access to the surveillance database to public and private entities, for profit. Clearview additionally contracts with third parties, like Macy's, to sell or lease access to the surveillance database.

22. Macy's has a paid contract with Clearview.

23. The pictures and images from video surveillance at Macy's are uploaded to Clearview's database. If there is a match, the results identifying individual shoppers based on their facial geometry are sent back to Macy's.

The Illinois Biometric Information Privacy Act ("BIPA")

24. More than ten years ago, the Illinois Legislature recognized the promises and perils of biometric identification technology. It passed the Biometric Information Privacy Act, 740 ILCS § 14/1 *et seq.*, to establish and safeguard Illinois' residents absolute right to control their biometric data.

25. BIPA regulates both biometric identifiers and biometric information. *See, id.*

26. Under the act, a "scan of…face geometry," is a biometric identifier. *Id.* at § 14/10.

27. Biometric information is any information derived from a biometric identifier, regardless of how it is captured, stored, or shared. *Id.*

28. The positive ID's that Macy's received back from Clearview are biometric information, as they are based on the biometric data Clearview has harvested and are used to identify individuals.

29. Once the photo is positively identified based on the biometric information in Clearview's possession, the positive identification of those photos become biometric information.

30. Under the act, a private entity, like Clearview or Macy's, in possession of either biometric identifiers or information must develop a written policy, available to the public, establishing a retention schedule and guidelines for permanently destroying the information or identifiers. *Id.* § 14/15(a).

31. Defendant has not provided any policy whatsoever establishing either a retention schedule or guidelines for permanently destroying the biometric data.

32. Under the act, a private entity like Macy's is prohibited from collecting, capturing, or otherwise obtaining a person's biometric information or identifier unless it first: a) informs the subject in writing that the information or identifier is being collected or stored; b) informs the subject in writing of the specific purpose and length of term for which the information or identifier is being collected, stored, or used;, and, c) receives a written release from the subject of the information or identifier. *Id.* at § 14/15(b).

33. Macy's had not at any relevant time informed Plaintiff or any member of the Class (described below) any of the information required under § 14/15(b). Neither the Plaintiff nor members of the putative Class executed a written release to Macy's.

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.