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

JOHNNY FLORES, ARIEL GOMEZ and DERRICK LEWIS, for themselves and others similarly situated, Plaintiff, v. MOTOROLA SOLUTIONS, INC., and VIGILANT SOLUTIONS, LLC, Defendants.	)	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **INJUNCTIVE RELIEF DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Johnny Flores, Ariel Gomez and Derrick Lewis, by and through their attorneys Loevy & Loevy, brings this Class Action Complaint against Defendants MOTOROLA SOLUTIONS, INC. ("MOTOROLA") and VIGILANT SOLUTIONS, LLC ("VIGILANT"), on behalf of themselves and all other similarly situated individuals ("Plaintiffs"), and as follows:

INTRODUCTION

1. Every individual has unique features by which he or she can be identified using a set of standard quantitative measurements. For example, the shape of and distance between tiny ridges on each person's finger are unique, so measures of these features—an example of "biometric" data—can be used to identify a specific individual as the person who made a fingerprint. Similarly, each person also has a unique facial geometry composed of, among other measures, distances between key facial landmarks and ratios between those distances. Once a picture of person's face is scanned and those 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, and potentially in any of the billions of cameras that are constantly monitoring our daily lives. Unlike fingerprints, however, facial biometrics are readily observable and, thus, present an even graver and more immediate danger to privacy, individual autonomy, and liberty. This fact about human facial geometry, the technologies that record it, and the opportunities for surveillance those technologies enable present grave challenges to traditional notions of privacy that people have expected since time immemorial.

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).

3. Pursuant to Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS §14/1, *et seq.*, Illinois prohibits private entities from, among other things, collecting, capturing, obtaining, disclosing, redisclosing, disseminating or profiting from the biometric identifiers or information of an individual without providing written notice and without obtain 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, Defendants Motorola and Vigilant collected, captured, obtained, disclosed, redisclosed, disseminated and profited from the facial geometric scans of hundreds of thousands of Illinois citizens in violation of BIPA's requirements. Specifically,

Vigilant, with Motorola later joining, collected and presently maintain a "gallery" of over 18 million booking photos or "mugshots" which is expanding all the time. The "gallery" includes at least tens of thousands of Illinois residents (many of whom were innocent and/or have had their records expunged by court order). Defendants have extracted the facial biometrics of each of person without permission.

5. In particular, Defendants performed a scan of the facial geometry of each depicted individual, stored the resultant biometric identifiers and information in a proprietary database (the "Biometric Database"), and disclosed, redisclosed, and otherwise disseminated those biometric identifiers and information to third parties in order to profit.

6. Defendants possess the biometric identifiers and information of the individuals in its Biometric Database without having adopted or made public any policy, written or otherwise, to govern the retention and destruction of thereof.

7. Defendants engaged in the above-described conduct: (a) without informing the impacted individuals that their biometric identifiers and information 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 or dissemination of the biometric identifiers and information; and (c) without seeking or obtaining written releases from such impacted individuals or their authorized representatives.

8. In violation of BIPA, Defendants have also profited, and continues to profit, from their unlawful collection, possession, disclosure, and dissemination of the biometric identifiers and information of Plaintiffs and members of the proposed class (the "Class Members"). For a fee, Defendants offer law enforcement agencies and others throughout the country the

opportunity to access and use their Biometric Database as a "facial search engine" allowing the identification of persons in the database. Defendants also incorporate the Biometric Database into their other facial recognition products thereby allowing the identification and tracking in real time and near-real time of millions of people—including Plaintiff and Class Members—wherever they may go.

9. To be included in Defendants' Biometric Database, a person merely had to have been arrested. To Defendants, it did not and does not matter whether that arrest resulted in a conviction or had been made in error or whether the booking photo has been expunged. Thus, like the guests of the Hotel California, Plaintiffs and the Class Members can never leave, at least not until this Court grants the requested relief.

10. As the Illinois General Assembly has found and the Illinois Supreme Court has confirmed, the harm to Plaintiffs and Class Members has already occurred.

11. 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.

12. As a direct result of Defendants' actions, Plaintiffs' and Class Members' biometric identifiers and information are no longer under their control and are now available to a potentially unlimited range of unknown individuals—both employees and clients of Defendants—who can surveil Plaintiffs and Class Members now and in the future. The injuries described herein are imminent and certainly impending.

13. Plaintiffs bring this Class Action Complaint seeking: (a) statutory damages of $5,000 per BIPA violation, or in the alternative, $1,000 per BIPA violation, from each of the Defendants, along with attorneys' fees and costs; (b) disgorgement of Defendants' ill-gotten

gains derived from the unlawful collection, possession, sale, disclosure, redisclosure, and dissemination of the unlawfully-acquired data; and (c) an injunction ordering that Defendants delete the data from its database.

PARTIES

14. Plaintiff Derrick Lewis is an Illinois resident. At times relevant to this case, Mr. Lewis was incarcerated at the Illinois Department of Corrections and at the Cook County Jail, including on charges of which he was innocent and convictions which have been vacated on the basis of innocence and expunged. Those entities made his and all detainees' booking photograph(s) searchable on their websites. On information and belief, Defendants are in possession of Mr. Lewis' booking photograph(s), have used it to extract his biometric identifiers and are currently in possession of his biometric identifiers and information.

15. Plaintiff Johnny Flores is an Illinois resident. At times relevant to this case, Mr. Flores was incarcerated at the Illinois Department of Corrections on a charge of which he was innocent. He was released in November of 2018 and is challenging his conviction in a post-conviction proceeding. A booking photograph of him remains on the Illinois Department of Corrections website to this day. On information and belief, Defendants are in possession of his booking photo(s), have used it to extract his biometric identifiers and are currently in possession of his biometric identifiers and information.

16. Plaintiff Ariel Gomez is an Illinois resident. At times relevant to this case, Mr. Gomez was incarcerated at the Illinois Department of Corrections on a charge of which he was innocent. After 20 years of incarceration for a crime he did not commit, his conviction was vacated and the charges against him dismissed. On information and belief, Defendants are in

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.