Advancements in In-Cab Technology Leads to Privacy Concerns and Litigation

Article
Amundsen Davis Cybersecurity & Data Privacy Alert
October 14, 2024

Employers have long used in-cab cameras for a variety of concerns, including protecting the driver and the public from accidents resulting from inattentive driving. Reviewing the recordings serves as a valuable training tool and can provide key evidence after a collision. However, with the advancement of artificial intelligence (AI) and machine learning technologies, and in the wake of recent prosecution of driver cases pursuant to the Illinois Biometric Information Privacy Act (BIPA), employers using these devices may find themselves subject to heightened scrutiny. Employers must take a hard look at their current privacy practices, policies, and disclosures to provide a sought-after level of transparency to their drivers and reduce their litigation risk.

What Are AI-Enabled Dash Cams?

Unlike traditional video cameras that simply record footage, AI-enabled dash cams may be able to "recognize" certain features and body posture for indication that a driver is distracted, fatigued, or using their phone while driving. Data on callous driving behavior, such as close following distance, hard braking, lane departure, and harsh turns, can also be collected by the technology for employers to review upon accident or initiating a driver reprimand. Given these capabilities, it is no surprise that this technology has been favored by insurance companies and employers to enhance safety and assist in disputes.

What Are the Legal Concerns?

Drivers are making claims that, without proper disclosure and consent, AI-enabled dash cams invade their privacy. Notably, there is little guidance on whether the technology captures truly "private" or biometric data. Moreover, the claims are grounded in a failure to disclose the collection or to use certain terminology in the disclosures rather than harm being inflicted. No identities have been stolen or biometrics reproduced.

Recent victories in biometric class actions better define the scope of BIPA. As one federal court noted in *G.T. v. Samsung Electronics America, Inc*., the inclusion of the word "identifier" in BIPA legislation should not be ignored; principles of statutory

PROFESSIONALS

Isabelle Faust
Partner

Sofia Valdivia
Associate

RELATED SERVICES

Biometric Privacy

Cybersecurity & Data Privacy

Transportation & Logistics

construction lead to the conclusion that BIPA only covers scans capable of identifying an individual. Other courts are in accord with *Samsung.*

While these decisions are good news for employers navigating obligations under BIPA, employer-specific victories surrounding the use of in-cab technology are difficult to come by or short lived. For instance, in July 2022, an Illinois federal court denied a motion to dismiss a putative BIPA class action brought by a truck driver against his organization's dash cam provider for negligent collection of biometric data in *Karling v. Samsara Inc.* The plaintiff alleged that the dash cam extracted biometric images of drivers' faces and there was a failure to obtain a written release as required by law. The court found the plaintiff sufficiently alleged a cause of action. Not long thereafter, an Illinois state court dismissed Samsara from a similar lawsuit.

However, in *Guszkiewicz v. Beelman Truck Co.*, the plaintiff brought claims against the technology provider *and* the employer. The court found that the employer—not the dash cam provider—could be responsible for obtaining written consent from its employees pertaining to potential collection of biometric information. This case ultimately settled, leaving companies with little guidance on whether AI-enabled dash cams are considered to collect biometric information or identifiers.

What Steps Can Your Company Take?

Rather than shy away from technological advancements, companies must learn about the technology and take steps to mitigate potential litigation.

PROVIDE CLEAR DISCLOSURES AND POLICIES TO EMPLOYEES

While the caselaw has not provided clarity for employers, employees are concerned about what data is being collected about them and for what purposes. If your company hires drivers who drive through Illinois while using the technology, you should assess whether written consent is necessary. Even if you are unsure about whether you are subject to BIPA, you likely still want to consider providing your employees policies on dash-cam use. Providing clear disclosures and policies to your employees may help prevent future claims and complaints.

COMMUNICATE TRANSPARENTLY WITH EMPLOYEES

As with any recording device, transparency is key. Consider implementing notifications for when recording is in progress as well as periodically collecting notice acknowledgement from your drivers. Additionally, providing policies that outline the duration of dash cam use and reassuring employees of responsible use of the data shows that an employer is mindful of its drivers' privacy.

REVIEW VENDOR AGREEMENTS

Establishing clear guidelines with third-party service providers pertaining to video capture, storage, processing, access, and retention can help ease the concerns of drivers and prevent potential mishandling of employee data. Companies should also have a clear understanding of internal and vendor responsibilities for data storage, ownership, and usage.