Biometric Data in the Days of Virtual Interaction and E-Learning

Amundsen Davis Data Privacy & Security Alert
April 7, 2020

Due to COVID-19, everyone has been adjusting to daily life from home, including the youngest family members. Education is coming in the form of rapidly-developing technology that provides cybernetic classes and hangouts and the submission of coursework or "attendance" virtually. More businesses now have employees working remotely, using technology to stay in touch with co-workers and conduct meetings. However, this interfacing by schools, dance/music classes and management or team meetings may come with legal risk. The requirements of privacy laws, take, even the Illinois Biometric Information Privacy Act (BIPA) protection of "voiceprints," are not being relaxed even in these unusual times. Any company should ask what consent and disclosures are in place before they engage in the next virtual connection.

A new class action lawsuit against Google, for use of the tech giant's educational platform, highlights this challenge. There, a parent claims that Google violated BIPA by collecting voiceprints, facial features and other personal identifiers of children. Google is also being accused of violating the Children's Online Privacy Protection Act (COPPA), which prohibits companies from collecting personal information from children under the age of 13 without parental consent. So while making remote working and learning resources available during this pandemic is undoubtedly necessary, companies must remember that federal and state privacy laws remain in full force.

If you are allowing for any recordings or interfacing that could involve facial or voice data, you should *first*:

- **Determine what biometric information you are collecting:** Under BIPA, biometric data is sensitive information that is biologically unique—such as iris scans, fingerprints, voiceprints and face geometry. Some of these identifiers can be captured simply through voice or video recording, so think through what information your company may be collecting to determine any necessary disclosures.
- **Evaluate what disclosures you currently have in place**: To comply with BIPA, companies must provide written notice to its users disclaiming what biometric information will be collected, stored, or used, as well as an explanation of the purpose of its collection and how long it will be kept.

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Biometric Privacy

Cybersecurity & Data Privacy

Additionally, prior to collection it is best to obtain *express written authorization* from consumers (students, employees, participants) to collect and store their biometric information.

- **Develop a publically available written policy**: Along with obtaining express consent, it is important to incorporate a public policy establishing a retention schedule and guidelines for destroying biometric information.
- **Do not forget about federal regulations:** While it may be difficult to keep up with the many changing state regulations, do not allow blanket federal policies to fall to the wayside. If you collect, use, or disclose any personal information from children under 13 years of age be sure to comply with COPPA by clearly posting privacy policies on your website or platform and obtaining parental consent. State privacy laws may add another layer of disclosure or consent. In fact, regardless of whether you interact with this age group, the Federal Trade Commission (FTC) and/or certain state laws recommend providing this disclosure as a precaution.