BLANKROME

Biometric Privacy

SEPTEMBER 28, 2020 • NO. 2

Recent Amazon Biometric Privacy Ruling Shows Power of Successful Personal Jurisdiction Challenges in BIPA Class Actions

Relying on a successful personal jurisdiction defense, Amazon Web Services ("AWS") and Pindrop Security, Inc. ("Pindrop") recently defeated a biometric privacy lawsuit claiming they captured voice data during phone calls placed through AWS' Amazon Connect service in violation of the Illinois Biometric Information Privacy Act ("BIPA").

The opinion—McGoveran v. Amazon Web Services, Inc., *2020 WL 5602819 (S.D. Ill. Sept. 18, 2020)—is the latest in a series of victories for BIPA defendants, and demonstrates the power of personal jurisdiction challenges to procure outright dismissals where the conduct allegedly giving rise to a BIPA violation occurs outside Illinois.*

OVERVIEW OF VOICEPRINT DATA

Voiceprinting, also known as voice biometrics, is the use of biological characteristics—one's voice—to verify an individual's identity without requiring a passcode or answers to secret questions.

Unlike traditional passcodes, however, in the event of a data breach there is nothing an individual can do to prevent someone from using his or her voiceprint to gain access to compromised accounts.

PERSONAL JURISDICTION AS A BASIS TO DISMISS BIPA CLAIMS

Pindrop offers voiceprint biometric services for call centers to confirm the identity of callers. AWS provided cloud storage services under the brand Amazon Connect for Pindrop to store its collected voiceprint data.

In *McGoveran,* three plaintiffs sued AWS and Pindrop for alleged BIPA violations stemming from the collection and retention of their voiceprint data from multiple calls made to a John Hancock call center located in Massachusetts, which used Amazon Connect with Pindrop biometric voiceprint authentication.

After the filing, AWS and Pindrop moved to dismiss for lack of personal jurisdiction. The Southern District of Illinois agreed with AWS and Pindrop, granting their respective motions and dismissing both defendants.

In its opinion, the court first addressed plaintiffs' argument that AWS consented to jurisdiction when it requested the court compel discovery from plaintiffs prior to asserting its personal jurisdiction defense. According to the plaintiffs, this constituted a request for affirmative relief that waived any personal jurisdiction objections.

The court rejected this argument, finding the rule sought to be applied by the plaintiffs—that personal jurisdiction is waived if a defendant creates an expectation it will defend a suit on the merits—was inapplicable. In doing so, the court first noted AWS gave no indication of any intent to defend the suit on the merits. More importantly, the discovery AWS sought pertained to information regarding arbitration, which showed just the opposite—*i.e.,* that AWS believed federal court was an improper venue for the plaintiffs to resolve their dispute, and that AWS would not be litigating the merits of their claims in court.

After disposing of the consent argument, the court turned its attention to whether plaintiffs had made a *prima facie* showing of personal jurisdiction over AWS/Pindrop sufficient to avoid dismissal. Because the plaintiffs conceded general jurisdiction was lacking, the court focused its analysis on whether the defendants were subject to specific personal jurisdiction in Southern District of Illinois.

On this issue, the court rejected plaintiffs' principal argument that defendants were subject to specific jurisdiction because they collected/possessed the voiceprint data of Illinois citizens who placed phone calls while in the state. The court reasoned plaintiffs' initial dialing of the phone while in Illinois—the only activity at issue that took place in the Prairie State—was insufficient by itself to confer specific jurisdiction.

In addition, the court also found neither defendants' relationship with a third party located out of state (John Hancock) nor that third party's contacts with Illinois could be used to establish personal jurisdiction.

Thus, in the absence of any evidence AWS or Pindrop specifically targeted Illinois citizens when providing their voiceprinting services, and because the litigation did not arise from contacts AWS or Pindrop themselves created with Illinois, the court concluded it lacked personal jurisdiction over both defendants. This resulted in the dismissal of the entire action.

TAKEAWAYS

Employers using biometric fingerprint time and attendance systems have been the primary target of BIPA class action litigation for some time. Recently, the scope of BIPA targets has expanded to include companies utilizing facial recognition technology. It is likely the plaintiffs' bar will continue its attempt to further expand the scope of BIPA targets in the coming months and years.

At the same time, many companies across several industries will also face increased exposure in the area of biometric privacy as they turn to contactless biometric solutions to minimize risks associated with COVID-19 and similar health threats.

Combined, it is clear companies will face much greater class action litigation risk in connection with Illinois' biometric privacy statute moving forward.

This expanding exposure due to allegations of improper collection, use, storage, and dissemination of biometric data has given companies significant cause for concern—and for good reason. As just one example, Facebook recently agreed to pay $650 *million* to settle a longstanding BIPA class action lawsuit stemming from its alleged improper use of facial recognition software on its social networking site.

Fortunately—as *McGoveran* shows—defendants sued for alleged BIPA violations that took place exclusively outside Illinois may be able to utilize the personal jurisdiction defense to quickly extricate themselves at an early juncture in the litigation.

ACTION STEP: DATA MAPPING & INVENTORY

To successfully challenge BIPA suits based on personal jurisdiction, companies must be able to show plaintiffs' claims arise out of biometric-related activities that took place exclusively beyond the state borders.

For this reason, it is critical all companies that use biometric data in their business operations conduct thorough data mapping and inventory exercises—which entails mapping and inventorying every piece of biometric data collected, used, and/or sold by the company, as well as its data processing practices. Completing this exercise will allow companies to develop a comprehensive understanding of where its collection of biometric data takes place, as well as what part(s) of the organization it passes through and where it is used and stored thereafter.

When done properly, this data flow diagram and data storage inventory can be used to provide persuasive support for a personal jurisdiction challenge in the event the company's biometrics practices are contested in a BIPA (or similar biometric privacy) class action litigation.

Further, in addition to proactively laying the groundwork for successful personal jurisdiction challenges, data mapping can also aid companies in: (a) proactively managing/safeguarding biometric data; (b) building out privacy disclosures that are essential to complying with BIPA and similar biometric privacy laws; and (c) satisfying BIPA's data destruction requirements.

HOW WE CAN HELP

As leaders in the biometric privacy space, Blank Rome's dedicated Biometric Privacy Team can provide key counseling and guidance regarding the collection, use, and storage of all types of biometric data, as well as today's new wave of biometric privacy laws. We can also assist in developing tailored, comprehensive biometric privacy compliance programs that ensure continued, ongoing compliance not just with current biometrics regulations, but anticipated laws as well—allowing you to stay ahead of this constantly evolving legal landscape.

For additional information, please contact:

Jeffrey N. Rosenthal, Philadelphia Office
Partner and Team Lead, Biometric Privacy
215.569.5553 | rosenthal-j@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Biometric Privacy
513.362.8711 | doberly@blankrome.com