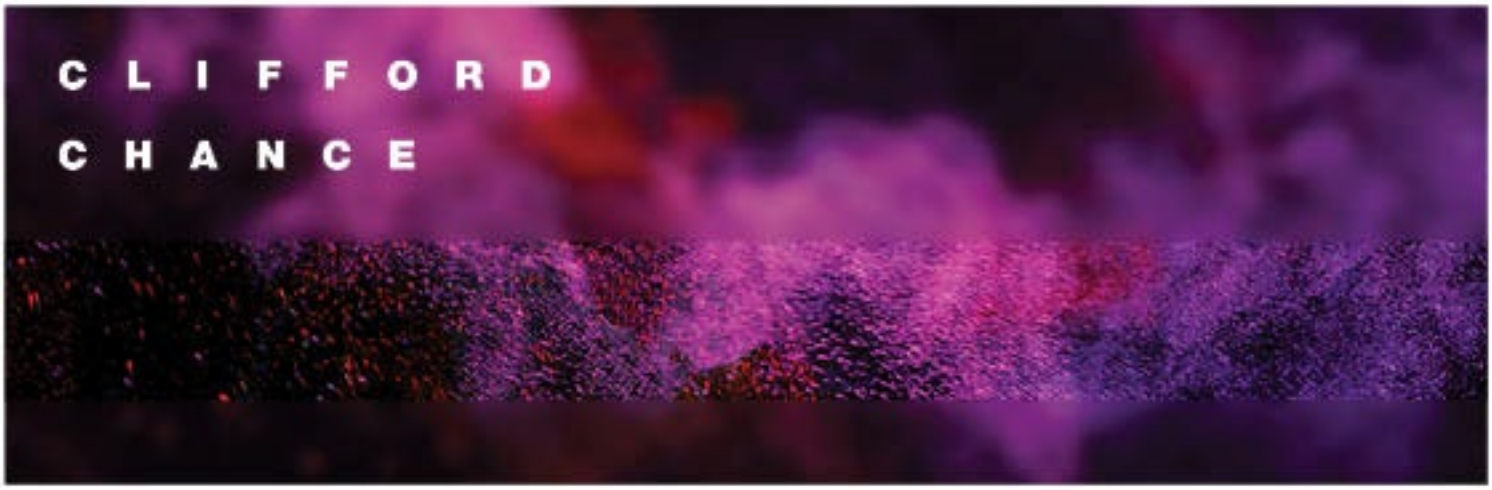

THE COMING WAVE OF BIOMETRIC CLASS-ACTION SUITS

Companies are facing more claims under the Illinois Biometric Information Privacy Act ("**BIPA**"), which regulates the collection and use of biometric data and provides individuals with a private right of action. Most recently, TikTok's parent company, ByteDance Ltd., agreed to pay $92 million to settle a class-action lawsuit relating to data privacy claims.

BIPA

Enacted in 2008, BIPA acknowledges that biometrics are unlike other security identifiers used to access sensitive information. Whereas a social security number can be changed if compromised, a fingerprint cannot. Once an individual's biometrics are compromised, the individual is at heightened risk for identity theft.

Under the Act, "biometric identifier" is defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." "Biometric information" means any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual.

The Illinois law provides that private entities may not capture, purchase or obtain a person's biometric identifiers or information unless they receive a written release from the individual to do so for a particular purpose. Private entities also may not disclose or disseminate biometric data without obtaining the requisite consent. Furthermore, private entities are required to destroy biometric data once the original use purpose is satisfied, or within three years of the individual's last interaction with the entity.

Perhaps most importantly in the age of apps, under BIPA, private entities may not sell, lease, trade or otherwise profit from a person's biometric identifiers or information. In today's world, when a company's success is heavily dependent on targeted advertising, biometrics provide valuable information for which companies are willing to pay a premium. A limitation barring companies from profiting off biometric data will impact third parties' marketing strategies.

In recent years, employees have also relied on BIPA to challenge employers' use of biometric information, like fingerprints, for time-keeping purposes.

The Illinois statute carries a penalty of $1,000 ***for each*** negligent violation and $5,000 ***for each*** reckless or intentional violation of the act. Potential damages can therefore rack up quickly.

The Class Action Suit and Proposed Settlement

The TikTok settlement stems from 21 separate class-action complaints filed in both California and Illinois last year. The suits were merged into a single complaint, alleging that TikTok extracts a "broad array of private data including biometric data and content" used by Defendants to track and profile customers for purposes of ad targeting and profit.

According to the complaint, the app attempts to ascertain users' race, gender and age by using biometric identifiers and facial recognition algorithms to map users' faces in their videos. The complaint also alleges that TikTok collects data regarding users' general habits, even when the app is not in use. This data includes user communications and internet browsing history, which is then shared with third parties, such as advertisers and other social media platforms like Facebook.

The complaint further alleges that data pertaining to U.S. users is sent to China, where it is subject to collection by the Chinese government.

The plaintiffs claim that TikTok's practices run afoul of numerous data privacy laws, including BIPA. While TikTok continues to deny the allegations, the proposed settlement agreement nevertheless contains the following terms:

- Unless expressly disclosed in its Privacy Policy and in compliance with all applicable laws, TikTok will not:
    - Collect or store users' biometric information or identifiers
    - Collect users' GPS data
    - Transmit U.S. users' data overseas
- TikTok will delete all pre-uploaded user generated content collected from unsaved or unposted content

The agreement remains subject to approval by U.S. District Judge John Lee of the Northern District of Illinois.

Trends in Litigation

Data privacy litigation in the biometrics space is expected to continue, as both consumers and legislatures become more protective of biometric information.

- **Other Suits** - TikTok is not the first social media company to be sued under BIPA. In 2015, a class-action suit was brought against Facebook in Illinois, alleging the company collected and stored digital scans of users' faces without prior notice or consent. Last year, Facebook attempted to settle the lawsuit for $550 million. U.S. Judge James Donato of the Northern District of California raised questions about the settlement figure, noting at a preliminary settlement hearing on June 6, 2020 that "[t]he Illinois legislature has said loud and clear this is meant to be an expensive violation." On February 26, 2021, a new settlement

agreement was approved, involving a payout of $650 million to be distributed amongst more than 1.5 million class members.

- **Other States** - Illinois is not the only state to have biometric data privacy laws; other states such as California, Washington, and Texas, have recently enacted legislation that regulates the collection and storage of such data. Illinois and California also provide plaintiffs with a private right of action, and New York may be close behind. Recently, lawmakers introduced the New York Biometric Privacy Act which, if enacted, will impose significant burdens on companies that collect and store biometric data.

Company Considerations

As courts continue to grapple with BIPA, companies should be mindful of the Act's gray areas which remain subject to interpretation. For example, terms like "biometric information" and "biometric identifiers" seem straightforward at first blush. However, in the context of data analysis and manipulation, they raise a multitude of questions. As explained in *Rivera v. Google*:

> The affirmative definition of "biometric information" does important work for [BIPA]; without it, private entities could evade (or at least arguably could evade) the Act's restrictions by converting a person's biometric identifier into some other piece of information, like a mathematical representation or, even simpler, a unique number assigned to a person's biometric identifier. So whatever a private entity does in manipulating a biometric identifier into a piece of information, the resulting information is still covered by [BIPA] if that information can be used to identify the person.[1]

Rivera addresses "biometric information's" far-reaching definition. However, it does not pinpoint the precise moment when biometric data is manipulated enough so as to render an individual unidentifiable. This raises questions about a private entity's obligations under BIPA in the context of data aggregation, particularly in instances where the underlying source material remains available to the private entity. It remains unclear whether biometric information, when aggregated at a group level, is subject to the "for profit" use restrictions set forth under 740 ILCS 14/15(c).

Another issue private entities must engage with is whether electronic consent is sufficient to satisfy the Act's requirements. As worded, BIPA requires "a written release" from individuals prior to collection of biometric data. Recently, a bill was introduced which seeks in part to add "electronic consent" to BIPA's definition of "written release." The proposed revision is telling of future hurdles companies will likely face in satisfying the current bill's consent requirements.

Lastly, the issue of standing remains a hotly contested point in BIPA litigation. BIPA, at its core, protects individual privacy interests in biometric data. Some state and federal courts have likened the injury suffered under a BIPA violation to the injury suffered in a tort claim for invasion of privacy.

---

1 *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017).

These courts have held that plaintiffs need not also allege some type of economic harm or data breach in order to bring a suit. Determinations of standing remain fact-specific, but in a growing number of jurisdictions, plaintiffs will find it easy to satisfy standing requirements, leaving private entities vulnerable to an onslaught of data privacy claims.

Companies that regularly handle biometric data need to think carefully about their data privacy policies in light of current open questions in the law regarding BIPA and in anticipation of future regulatory developments in the biometrics space.

CLIFFORD CHANCE

CONTACTS

Anthony Candido
Partner

T +1 212 878 3140
E anthony.candido
@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Taylor Dean
Associate

T +1 212 878 8175
E taylor.dean
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.