REPRINT

CD corporate disputes

BIOMETRIC PRIVACY LITIGATION

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
OCT-DEC 2021 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

PERKINSCOIE
COUNSEL TO GREAT COMPANIES

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

EXPERT FORUM

BIOMETRIC PRIVACY LITIGATION

PANEL EXPERTS

Sunita Bali
Partner
Perkins Coie LLP
T: +1 (415) 344 7065
E: sbali@perkinscoie.com

Sunita Bali is a partner with the firm's privacy & security practice and has substantial experience litigating cases in California state and federal courts. She represents clients in biometric class action disputes and other complex commercial litigation matters and regularly defends companies against claims brought under California's Unfair Competition Law and False Advertising Law. She also has experience defending claims for breach of contract, fraud, tortious interference, trade secret misappropriation and copyright infringement.

Debra Bernard
Partner
Perkins Coie LLP
T: +1 (312) 324 8559
E: dbernard@perkinscoie.com

Debra Bernard is a litigator who focuses on class action defence of claims under the Illinois Biometric Information Privacy Act (BIPA), the Telecommunications Consumer Protection Act (TCPA) and other consumer and privacy claims, as well as other areas of commercial litigation. She provides counsel to clients in a number of industries, including technology, education, retail and consumer products. She is also nationally recognised for her work on the TCPA and Illinois BIPA and biometrics issues generally.

Susan Fahringer
Partner
Perkins Coie LLP
T: +1 (206) 359 8687
E: sfahringer@perkinscoie.com

Susan Fahringer has extensive experience representing some of the world's leading companies in privacy, intellectual property and complex commercial litigation. She has served as lead counsel in a broad array of privacy class actions, including cases involving the Biometric Information Privacy Act, the California Consumer Privacy Act, and many other privacy-based claims. She also counsels companies to help reduce their litigation risk, and she tailors her approach to align to the client's strategic and business goals.

Nicola Menaldo
Partner
Perkins Coie LLP
T: +1 (206) 359 3787
E: nmenaldo@perkinscoie.com

Nicola Menaldo defends and provides counsel to technology and retail clients on a wide range of issues central to their business needs, including privacy and data security, marketing, biometrics, scraping and web crawling, artificial intelligence and machine learning. Drawing on her subject matter experience, she regularly defends clients in privacy class actions that involve novel privacy and technology issues. She also helps clients with product counselling and compliance advice informed by her litigation experience.

Ryan Spear
Partner
Perkins Coie LLP
T: +1 (206) 359 3039
E: rspear@perkinscoie.com

Ryan Spear counsels some of the world's most innovative companies on cutting-edge privacy and security issues. He has extensive experience handling individual and class action cases involving biometric privacy laws, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and other laws governing privacy and security. He also routinely represents clients in cases involving free speech and online publishing, including cases arising under the Communications Decency Act and the First Amendment.

CD: Could you provide an overview of the rising application of biometrics in security systems and other areas? In what ways is the technology being deployed?

Bernard: Security is one of the key applications for biometric technology and is increasingly pervasive. For example, companies have begun using biometric technology to provide secure, touchless financial transactions, limit access to medications and controlled substances, screen airline passengers, screen attendees of large-scale gatherings, such as sporting events and concerts, secure buildings, prevent unauthorised entry and detect known threats, and monitor face-mask usage. Biometric technology is also increasingly used in consumer-oriented products such as smartphones, computers, locks, cars and vending machines. People also now have the option to use virtual 'try-on' features driven by biometric technology in retail settings, biometric-based remote proctoring in education settings, and biometric point of sale and timekeeping systems while at work.

CD: What are the key risks associated with using biometrics to identify a person by their intrinsic physical or behavioural traits? What privacy-related legal and regulatory considerations need to be made?

Fahringer: The legal landscape is fairly complex and developing quickly, but one thing is clear: there are some real legal risks, and they carry the potential for staggeringly high damages awards and penalties as well as injunctions that could be very disruptive to a company. In the US, consumer advocates have been vocal in their concerns about the collection, storage and use of biometric data, particularly in the context of government surveillance. The Federal Trade Commission (FTC) has indicated that it will scrutinise the use of biometric technology and exercise its power to protect against unfair and deceptive acts or practices in connection with that technology. An example of this is its recent settlement with Everalbum, which required that company to delete both biometric data and algorithms that were trained on the data. There are also a host of state and federal laws that regulate privacy and consumer data in general, although we do not yet have a comprehensive federal law targeting biometric data specifically. Most of the legal landscape has developed at the state and local level, where there is a growing body of law that specifically targets biometric data. These laws are not always consistent across jurisdictions, and they are evolving as we speak, so companies that touch biometric data and that operate anywhere in the US, including on the internet, need to be aware of the latest developments.

Spear: Two states – Texas and Washington – have enacted broad-based laws that specifically govern biometric privacy, and many other states are contemplating biometric privacy laws as well, but the Biometric Information Privacy Act (BIPA) is the one that gets the most attention. BIPA is the only statute that has a private right of action, so consumers can sue to enforce the law, and BIPA provides for substantial statutory damages – $1000 for each "negligent" violation and $5000 for each "intentional or reckless" violation. This can lead to enormous exposure, especially where there is a large potential class of plaintiffs. An example of this is Facebook's recent settlement of one of the earliest BIPA cases for $650m. Since the Texas and Washington laws do not include private rights of action, those laws are enforced exclusively by the attorneys general of those states. The Texas statute includes significant civil penalties – $25,000 per violation. Cities and municipalities are increasingly regulating the use of biometric technology by private actors, as well. Portland, Oregon recently enacted an ordinance prohibiting the use of facial recognition technologies by private companies, subject to narrow exceptions. New York City passed two ordinances: one requiring signage in commercial establishments where facial recognition is used, and the other regulating biometric data used for keyless access in certain dwelling buildings. Other cities and municipalities like San Francisco, Oakland and Boston have banned or limited the use of certain biometric technologies by government actors. This may set the stage for more regulation of private actors. And some states have long imposed some restrictions on the use of biometrics in the employment context.

"In the US, consumer advocates have been vocal in their concerns about the collection, storage and use of biometric data, particularly in the context of government surveillance."

Susan Fahringer, Perkins Coie LLP

Bali: As well as the legal risks, companies also need to be especially mindful about the optical risks. Biometric privacy is a hot topic and tends to draw outsized scrutiny from the public, press and lawmakers. Companies should be thoughtful about their approach to these issues and the potential impact that their data collection and use practices might have on how the public perceives them. Some of the steps that we suggest companies take to

reduce their legal risks can also help reduce these optical risks.

CD: How would you describe biometric privacy litigation activity? To what extent have you seen a rise in such cases since the onset of the coronavirus (COVID-19) pandemic?

Bernard: Biometric privacy litigation has absolutely exploded in recent years, thanks to BIPA. The statute was enacted in 2008, but plaintiffs' lawyers first took a serious interest in BIPA in 2015. Virtually all BIPA cases are putative class actions. Most involve finger-scanning technology used by employers for timekeeping and other purposes. But there are also cases involving face, voice and hand-based biometric technologies. Indeed, the case Facebook recently settled was one of the earliest and leading cases and involved facial recognition technology. We expect the BIPA-driven litigation boom to continue with more litigation, both as a result of new biometric privacy laws and creativity by plaintiff lawyers in developing new ways to assert biometric privacy claims.

CD: Could you highlight any recent cases which illustrate the challenges companies face? What lessons might we draw from their outcome?

> **"Biometric privacy litigation has absolutely exploded in recent years, thanks to BIPA."**
>
> *Debra Bernard, Perkins Coie LLP*

Spear: The Facebook case provides a great example of the challenges that companies face when they use technologies that arguably rely on biometric data. That case involved technology that sought to identify individuals who appeared in photos uploaded to its platform and made suggestions to users to 'tag' the photos with those names. The judge rejected many of Facebook's defences, including that it was not possible to accurately identify who was not subject to the Illinois statute and who was not given that users often travel or move locations over time.

Bali: Other recent cases highlight how broadly BIPA might apply. For example, a series of recent

cases also involves virtual 'try-on' features that enable consumers to virtually 'see' how glasses or makeup appear on their faces. Plaintiffs in those cases claim that the technology that virtually imposes glasses or makeup on faces is biometric and triggers BIPA's requirements. Similarly, in recent cases involving online proctoring companies, plaintiffs argue that technology that monitors whether students are receiving help on exams through face- or voice-based technologies implicate BIPA. Other defendants have been sued for using voice recognition features in call centres, using body scanning technologies for COVID-19 screening, verifying identification documents submitted online by comparing them to 'selfies' and even for receiving, or creating, datasets for machine learning that include photos of faces. In cases like these, that involve innovative technologies, some of the strongest defences will turn on the facts. This can make it difficult to dispose of the case before trial. For example, it is often unclear whether the data at issue constitutes 'biometric' data under the statute. Because courts sometimes treat that as a question of fact for trial, defendants can be forced to litigate a case for years, or to pay a significant amount to settle a case to avoid the uncertainty of trial, even where they have strong defences.

CD: In the event of litigation, what initial steps do in-house counsel and legal teams need to take? How important is it to asses potential damages and develop the right legal strategy?

Bernard: If a company is sued, it should, above all, not panic. In many ways, biometric privacy litigation is no different from other types of litigation. Once a company is sued, the initial steps are generally the same as in other litigation. It is important to preserve relevant documents, impose a litigation hold, and, since in many BIPA cases there may be insurance coverage, conduct an insurance policy analysis and, if appropriate, notify the carrier of a claim. The company should conduct a preliminary factual investigation, ideally in coordination with counsel to preserve the privilege, to understand the

> **"Biometric privacy is a hot topic and tends to draw outsized scrutiny from the public, press and lawmakers."**
>
> *Sunita Bali, Perkins Coie LLP*

underlying facts and to evaluate possible defences and formulate a defence strategy. Where the allegations involve online products, the company's terms of use and privacy policies should be reviewed to assess whether there are the requisite disclosures and consent and whether there is an applicable arbitration, choice of forum or other venue-related provision. The company should get a sense of relevant class size, because that will be a significant factor for the analysis of class certification defences and potential exposure. Understanding the scope of the company's exposure is a good place to start as it may inform early decisions, such as the selection of counsel or possible early settlement.

CD: What steps can companies take to reduce legal exposure and mitigate the risk of litigation when implementing biometric-based systems? What policies and procedures do they need to adopt for collecting, storing and processing biometric data?

Menaldo: Of course, there are many ways for companies to reduce their risks before they are sued, too. At a very high level, before adopting any use of biometric data or technology, companies should consult experienced counsel to assess the risks, particularly in the jurisdictions where the relevant products or services will be offered. Companies should also consider how they will comply with all requirements under applicable laws. For example, companies should consider not only how they will provide notice and obtain consent – issues that typically grab headlines – but also how they will ensure that covered data is used, shared, stored and disposed of as required by applicable law. Finally, companies should evaluate contracts to understand what other burdens and risks they may assume and should consider adopting heightened security measures for protecting such data before they begin collecting, using and storing it. Some other common risk-mitigation strategies include the following. Firstly, know your data. Create and maintain a comprehensive data map to ensure that you have full visibility into the data type you

> **"Of course, there are many ways for companies to reduce their risks before they are sued."**
>
> *Nicola Menaldo, Perkins Coie LLP*

collect, use and store. This is foundational to identify potential biometric privacy risks and compliance 'gaps' along with other privacy and data security issues. Secondly, know how the law applies to your data. Biometric privacy laws are often broadly and ambiguously written, and courts have done little to clarify that ambiguity. Companies are often surprised to learn that certain types of data may fall within the scope of those laws. Companies should err on the side of working with experienced counsel to determine what data they collect, use and store might be governed by biometric privacy laws.

Bali: Once a company has a sense of what data it has, what it does with the data and how the law applies, it should comply as much as it can and as quickly as it can. In many cases, it may be difficult to adopt every measure that is arguably required under every applicable biometric privacy law. But companies should not, as the saying goes, let the perfect be the enemy of the good. That is, they should do their best to adopt the most significant compliance measures as quickly as possible. Good-faith compliance efforts will both discourage potential plaintiffs and make regulatory scrutiny less likely. Companies should also consider jurisdictional complexities. State and local laws have created a patchwork of rules and requirements that vary from state to state and, in some cases, city to city. And those requirements may change unexpectedly in the future as more laws are enacted. Companies should take that complex and shifting legislative landscape into account. For example, companies may decide to avoid 'high-risk' jurisdictions, like Illinois, altogether. At the very least, companies should consider how their compliance obligations may vary depending on where their biometric-based products or services are offered, and potentially where the biometric data is stored.

"The less you collect and keep, the less exposure you will have. This is especially true in connection with biometric data."

Ryan Spear, Perkins Coie LLP

Spear: To minimise risk, companies should consider the following. Do not collect data you do not need, and do not keep data that you do not need to keep. The less you collect and keep, the less exposure you will have. This is especially true

in connection with biometric data. Be as selective as you can in what you collect and store. Here, as in many other contexts, data minimisation can be one of the most effective risk-mitigation strategies. Furthermore, consider adopting general risk-mitigation strategies. The same litigation risk mitigation strategies used in other contexts work just as well in this context. For example, entering into agreements with users that select single-party arbitration as the dispute resolution mechanism can reduce the risk and burden of private litigation.

CD: What are your predictions for biometric privacy litigation in the years ahead, particularly as the world becomes increasingly technologically-dependant and legislation in this area develops further?

Fahringer: We predict an increase in biometric privacy litigation across the board. We expect an increase in the complexity of the legal landscape, at least until we have a comprehensive federal biometric privacy law, which we do not expect to see anytime soon. We expect more jurisdictions to enact laws targeting biometric data, which might create tension between and among these laws where they differ from each other. We also expect to see an increase in the type of company that is targeted in biometric litigation, with lawsuits filed not just against consumer-facing companies but against business-to-business companies that are multiple steps removed from the consumer, as well as more companies that are located, and that operate, well outside Illinois. We also expect to see biometrics cases become more nuanced as the case law develops. And we expect to see an increase in the number of cases as more lawyers enter the fray and test the boundaries of BIPA.

Menaldo: Biometric technology is here to stay and has many beneficial and positive uses. It is integral to certain technology products, it is an effective means to improve security, it can enhance the consumer experience, it can facilitate financial transactions – which is even recognised in BIPA – and it provides contactless means to interact with products and services, which has become increasingly important in the age of COVID-19. But major privacy and misuse concerns remain, generating controversy, and legislators are trying to get their arms around it. The law moves slowly and is usually a step behind technology, but it is definitely moving, and we are not seeing laws taken off the books or amended to be less onerous or clearer. On the contrary, every year we see legislators across states seek to add laws to regulate biometric privacy. The only thing that is clear is that companies will need a really good compass to navigate these increasingly complex waters. CD