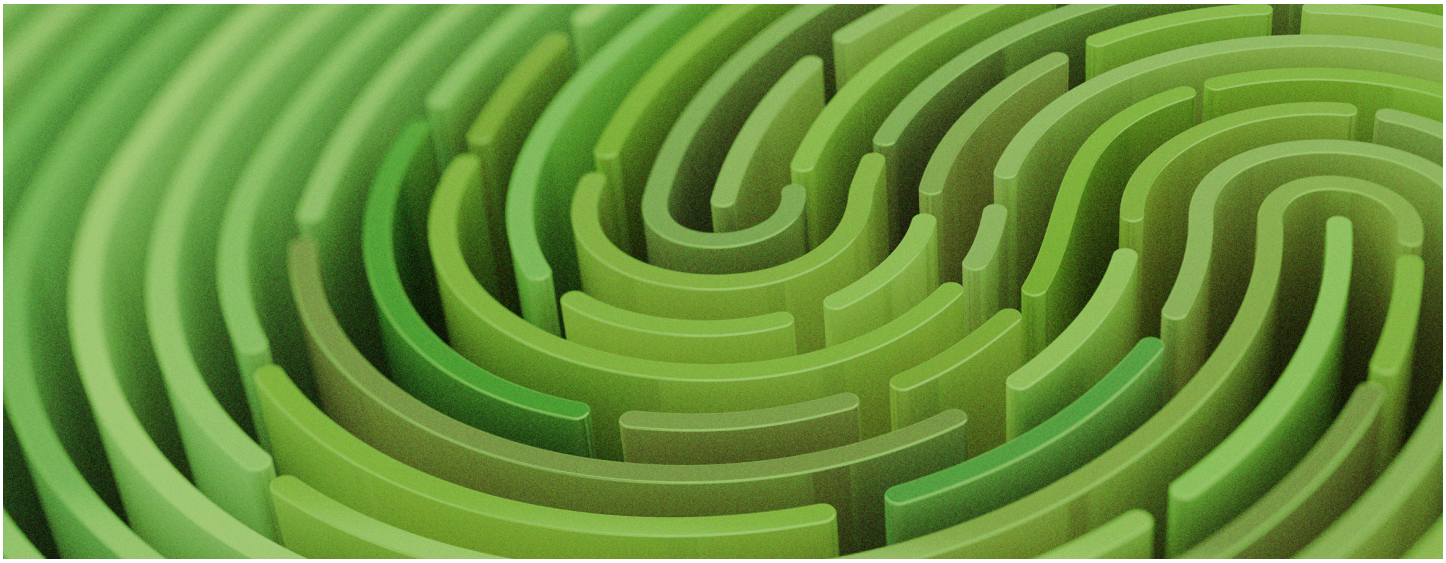


Biometric Information Privacy Laws, Uncertainty, and Consumer Experience: A Q&A with Anja Lambrecht

Anja Lambrecht, **Mark Gustafson**, and **Nathan Trujillo** — 6 MIN READ

Biometric privacy laws have given rise to a profusion of litigation and changed the way technology companies operate. Can they inadvertently end up hurting some of the very consumers they aim to protect?

Many biometric information privacy laws expose companies to sizable statutory damages awards. Partly in response, some companies have changed how they operate in certain states – for example, by restricting access to certain digital products or features. How are consumers navigating this new landscape, and what effects will this risk calculation have on future litigation?

To explore these questions, Analysis Group Managing Principal **Mark Gustafson** and Vice President **Nathan Trujillo** spoke with academic affiliate **Anja Lambrecht** of London Business School to discuss recent trends in biometric privacy litigation. Professor Lambrecht is an expert on the behavior of consumers in digital markets – in particular, how consumers evaluate and respond to products and services. In her work, she frequently addresses questions at

the intersection of privacy and digital marketing. Professor Lambrecht, Mr. Gustafson, and Dr. Trujillo discussed litigation risk for technology companies, its effects on the consumer experience, and what sources of information are relevant for experts in these matters.

Can you give us a sense of the risks faced by companies subject to biometric privacy laws?

Companies operating in states with these statutes face a great deal of uncertainty. To begin with, the scope of these laws can vary greatly from state to state, and it is sometimes unclear what constitutes a violation.

Also unclear in some cases is how damages accrue to the individual. This creates considerable risk for companies operating in these states. For example, until the Illinois legislature recently amended the Illinois Biometric Information Privacy Act, or BIPA, companies operating in Illinois faced the possibility of multiple violations per person – for example, an employee scanning their fingerprint each time they enter a workplace. This has prompted companies to exercise greater caution in states with biometric privacy laws.

How significant are the consequences for violation?

Biometric privacy litigation often involves allegations that an entity failed to provide proper notice or obtain the consent of consumers in the precise form required by the relevant law in order to collect and store biometric information. For some statutes, no showing of actual injury to consumers is required to bring a case. This can lead to situations in which companies accused of technical violations of the law can be subject to large statutory fines even if the alleged violations did not actually harm consumers.



> *If consumers lose access to products or features that they value, biometric privacy legislation can end up harming rather than enhancing consumer welfare."*
>
> ANJA LAMBRECHT

Give us an example of how this may play out with a specific state law.

Let's take BIPA. The first BIPA case to go to a verdict, in 2022, resulted in a $228 million judgment against BNSF, a freight railroad company. The case involved 45,000 truck drivers whose fingerprints were scanned using an automated gate system at BNSF's Illinois facilities. While the award was later vacated because of a legal issue, BNSF nevertheless ended up paying $75 million to settle the case prior to its retrial on damages.

Many other lawsuits brought under BIPA have been resolved through settlement. While some of these settlements can be large, they are often orders of magnitude less than the amounts that could be awarded at trial based on statutory damages.

How did the state respond?

As I mentioned previously, biometric privacy laws can sometimes be unclear, both on what constitutes a violation and on damages accrual. This leaves it up to the courts to interpret the law as best they can until legislators catch up. In February 2023, for example, the Illinois Supreme Court ruled in *Cothron v. White Castle System* that separate BIPA claims accrue for *each* individual with *each* violation of the law, as opposed to only in the first instance. The case involved a company that captured and stored fingerprint data each time an employee attempted to access their paystubs and computer. The *Cothron* ruling increased potential BIPA liability exposure exponentially, as the company could ostensibly be liable for hundreds of thousands or even millions of dollars in statutory damages for each individual.

Only after White Castle paid a multimillion-dollar settlement did the Illinois General Assembly amend BIPA to clarify that an entity that repeatedly violates BIPA's notice and consent requirement has committed a single violation, and each plaintiff is only entitled to a single recovery. While this reform to BIPA was likely welcomed by companies that want to offer products and services that use biometrics in Illinois, it may not be enough to outweigh the risk of offering those products and services in the state, particularly since plaintiffs are not required to show or even allege actual harm to bring suit.

So how have companies responded to the risks stemming from this uncertainty?

To preempt the threat of litigation, companies sometimes disable features that involve, or may involve, protected information in jurisdictions with biometric privacy legislation. For instance, technology companies have disabled product features in Illinois and Texas that use image and voice recognition to avoid the potential for costly lawsuits.

One example that comes to mind is the Google Nest Doorbell. A key security feature of this product is the familiar face detection function, which notifies the user when it detects people it doesn't recognize at the user's home. Google disabled this feature for consumers' Nest cameras in Illinois as a precaution. Likewise, Meta removed some of its augmented reality effects and applications, such as avatars and filters, from Facebook and Instagram in Illinois.

What are the consequences of choices like these?

When certain products or features are disabled, consumers can be the ones to pay the price. This is an important consideration from a public policy perspective: If consumers lose access to products or features that they value, biometric privacy legislation can end up harming rather than enhancing consumer welfare.

What facets of the technology are crucial for a litigation expert in these cases?

Consumer-level considerations are important for evaluating the potential for harm. As I mentioned earlier, not every state law requires a showing of injury, but in those jurisdictions where it's necessary, determining whether certain alleged violations of biometric privacy laws in fact harmed consumers requires a detailed understanding of consumer-level knowledge and expectations about their interactions with the at-issue products or technology.

Consumer expectations with respect to product functionality are also relevant to the ultimate question of harm in biometric privacy matters. What one individual considers a privacy violation may not be a privacy violation to another individual. Consumers with low privacy expectations, for example, may assign little value to privacy but a high value to a challenged product or feature. There may be others with high privacy expectations, but who value the challenged product even more. Privacy expectations are highly individualized and are shaped by multiple individual-specific factors.

These consumer expectations are also relevant to the question of harm. The use of technology is ubiquitous, and consumer familiarity with these features in one setting could largely offset or eliminate the potential for harm in another similar setting.

Heterogeneity in these expectations is directly relevant to questions of harm in class certification, particularly when the key questions of liability relate to disclosures about the type of biometric information being collected, and how it is being collected and stored. If consumers have different ideas of what they are agreeing to or getting from a service, it may play into the determination of whether they were harmed, or whether members of a putative class were all harmed in the same way.

What sources of data could an expert use in opining on such matters?

Much of my research centers on the empirical analysis of consumer experience with products or services. One source of data that can be especially useful is online user reviews of products. Online reviews are a powerful and trusted source of information for consumers. In the context of digital markets, consumers rely on the information in online reviews to help make purchase decisions.

Studying the content of online reviews can determine how consumers value the product and whether there is consistency or heterogeneity in the experience of users reviewing products with a feature that uses the challenged biometric technology. Online reviews can also illuminate what consumers expect from services or products. The insights gained from studying online consumer reviews can be relevant to whether consumers were harmed by the violation of laws governing their privacy, whether individually or as a class. ■