In January, Google launched a new feature in its Google Arts & Culture app that allowed users to take a selfie and find out whether their face matched any of those in historical paintings. The new search tool was nothing more than a momentary amusement for most people, albeit one that was wildly popular. However, people in two states — Texas and Illinois — were left out of the fun because of state privacy laws restricting the use of facial recognition technology. Unfortunately, laws like these may ultimately cost consumers and businesses much more than just access to the latest trending apps.

Biometrics — quantifiable measurements about a person’s physical or behavioral characteristics, such as how someone looks, speaks or walks — are useful for many different types of applications. For example, they are used to increase efficiency, such as by automatically identifying individuals, and to increase security, such as by adding an additional layer of verification to a multi-factor authentication system. One company has even pioneered a wearable device that provides a new type of “always on” biometric, allowing users to authenticate themselves by their unique heartbeat.

Unfortunately, some privacy activists have vigorously opposed the growing ubiquity of biometrics since its earliest days. This opposition has led to the passage of laws like the
Biometric Information Privacy Act (BIPA), the state law that kept Illinoisans out of the recent Google app. This law, which was the first of its kind when the state passed it in 2008, requires companies to obtain prior written consent from individuals before using biometrics, as well as to provide written notification detailing the specifics of how they will collect, use and store that information.

Now a decade old, the law shows the unintended consequences of heavy-handed privacy regulations. Originally, proponents of the law were concerned about widespread identity theft and government surveillance. While these problems have not materialized in any state, BIPA has become a roadblock to even some rudimentary uses of biometrics in Illinois.

One problem is that even minor violations of the law can subject companies to steep penalties of up to $5,000 per infraction, even if there is no actual consumer harm. And since BIPA allows individuals to file private lawsuits for violations, it has opened the door to more than 30 class-action lawsuits against companies operating in Illinois in 2017 alone.

A number of tech companies have faced significant class-action lawsuits for potential violations. Facebook, for example, faces massive potential fines because of a feature on the social network that used facial recognition technology to automatically tag photos of friends. Shutterfly, a popular online photo publishing service, has already settled a BIPA class-action lawsuit for an undisclosed amount. The problem for these companies is that obtaining prior consent is impractical for certain applications, such as analyzing photos uploaded by users.

But it is not just tech companies who are caught in the crosshairs of this law. Many businesses are running afoul of the notification requirements as well. For example, some companies are upgrading their antiquated time and attendance systems to improve their employees’ work hours and replacing them with more advanced biometric systems. These biometric systems avoid problems such as “buddy punching” where one employee clocks in or out for their absent coworker. But implementing these systems successfully under BIPA has proven difficult, and a number of companies in Illinois now face lawsuits for using these time clocks for their employees.

While state privacy laws are often well-intentioned, as BIPA shows, their unintended consequences can be far-reaching. The Illinois legislator who originally introduced BIPA has tried to amend the law because he says he never intended to restrict many of these activities, but fixing legislation is never easy. Surprisingly, a number of states are considering copycat legislation that would similarly limit biometrics. This would be a mistake. Rather than imposing new restrictions on biometrics, states would better serve local residents and businesses by encouraging greater use of this technology to increase productivity and improve security.

http://www.govtech.com/opinion/When-Do-Privacy-Regulations-Go-Too-Far.html