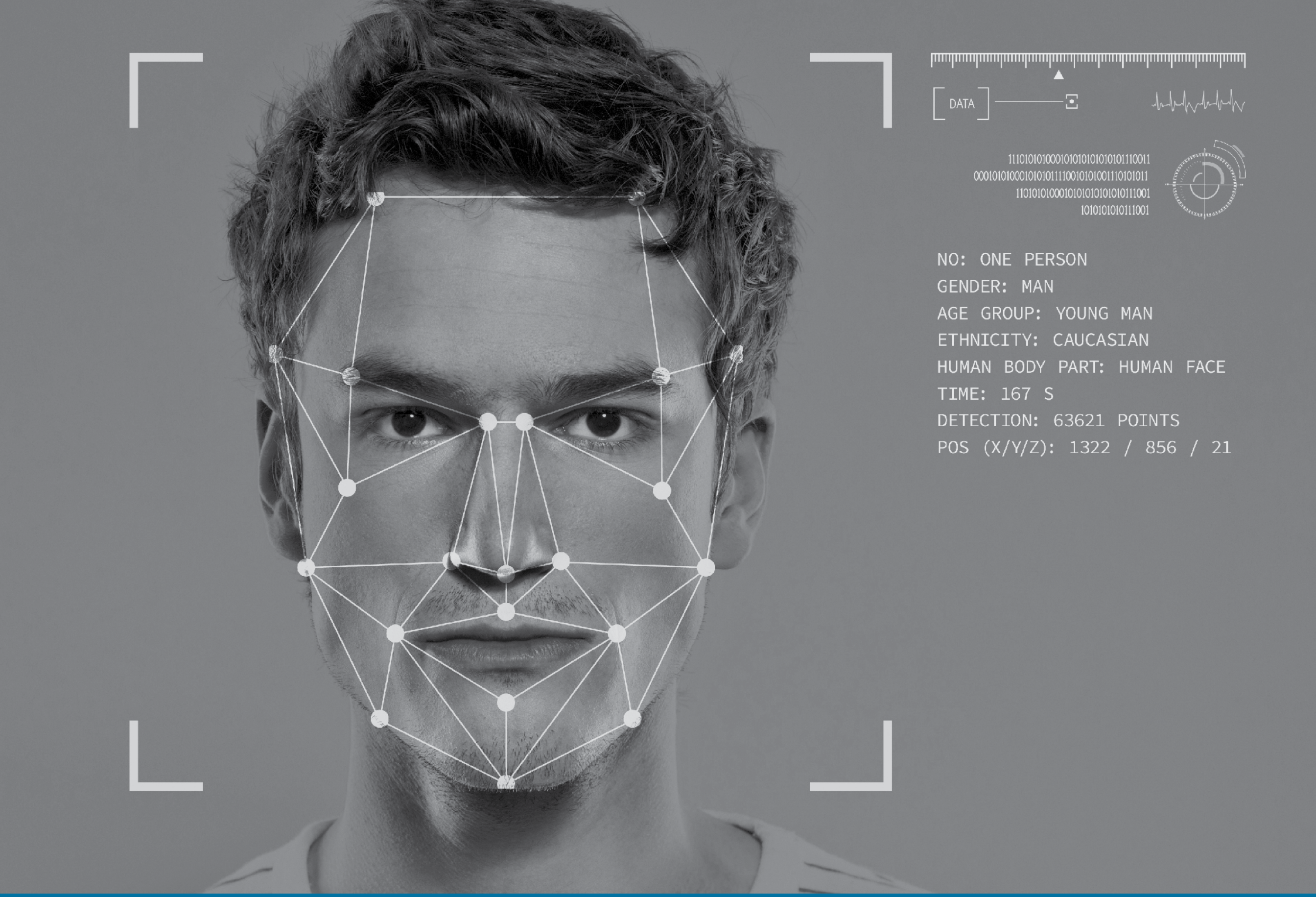


Facing the Future of Facial Recognition

Billy Easley

Imagine walking up to the automatic doors of your local convenience store only to find that, instead of opening, this time they remained tightly shut. This happened at a local Takoma, Washington convenience store earlier this year when the store started a facial recognition pilot program that compared images of known shoplifters to individuals who attempted to enter. If the store's camera and artificial intelligence matched an approaching individual with its database of facial images, the doors would not open.

When the Seattle Times interviewed patrons of the store, many of them were uncomfortable with the use of facial recognition technology. They argued that it was a privacy violation to be subjected to facial recognition without giving their consent or even being notified that they were under surveillance. In response, the store put up a sign stating that anyone who wanted to enter would have to abide by the facial recognition requirement. When the criticism continued to build, the company argued that their use of this technology was based on safety concerns for both their employees and consumers (in 2017, over 400 people were killed in retail stores, according to The D&D Daily, a retail trade publication).

The experience of this Takoma community is a small-scale illustration of an incoming national conversation about commercial use of facial recognition technology. And these conversations will only become more commonplace as larger retail stores, like Target and Walmart, are already using similar technology to track inventory and to prevent criminal activity. Apple's iPhone X allows users to unlock their cell phone by looking at their phone instead of inputting a password. Security companies are using facial recognition technology because it's more reliable and less cumbersome than the traditional password system. The American public benefits from the rollout of facial and biometric devices through increased convenience and enhanced security. However, it's natural for consumers to feel anxious about this new technological innovation and to question its purpose. Lawmakers can respond to these fears by educating the public about the benefits of this rapidly evolving technology. They should also avoid banning the collection and use of biometric data. Adopting such a top-down approach would strangle the development of innovative uses of this technology. Instead, lawmakers should consider passing laws that: (1) require notice and consent from consumers before biometric data can be used for specific purposes, excluding security purposes; (2) allow state attorneys general to sue if they determine companies have violated those requirements; and (3) require a violation to have resulted in harm before it can be prosecuted. These three principles will ensure that regulations will protect privacy without sacrificing technological innovation.

Lawmakers, communities, and privacy advocates have generally focused their skepticism about this technology on state and federal government use of facial recognition, rather than commercial use, and for good reason - when a convenience store uses facial recognition technology, the worst it can do is bar you from entering. When the government uses facial recognition, it can use that data as the basis to detain you or to deny you certain benefits or privileges.

Federal law enforcement agencies, including the Department of Homeland Security and Immigration and Customs Enforcement, have already started to deploy facial recognition tools to supplement their activities, but there are no comprehensive regulations guiding their use. States have also entered into agreements with federal entities to incorporate facial recognition technology into state law enforcement functions. The growing use of this technology resulted in Congress holding two hearings where lawmakers on the House of Representative's Oversight Committee shared a bipartisan desire to create explicit, limiting guidelines on data collection. Days after the committee's first hearing, privacy advocates, including the American Civil Liberties Union, asked Congress to impose a moratorium on the gathering of facial recognition data by federal agencies until regulations were signed into law.

In the midst of a contentious political environment, reining in government use of facial recognition is a rare bipartisan issue that could result in legislation being enacted.

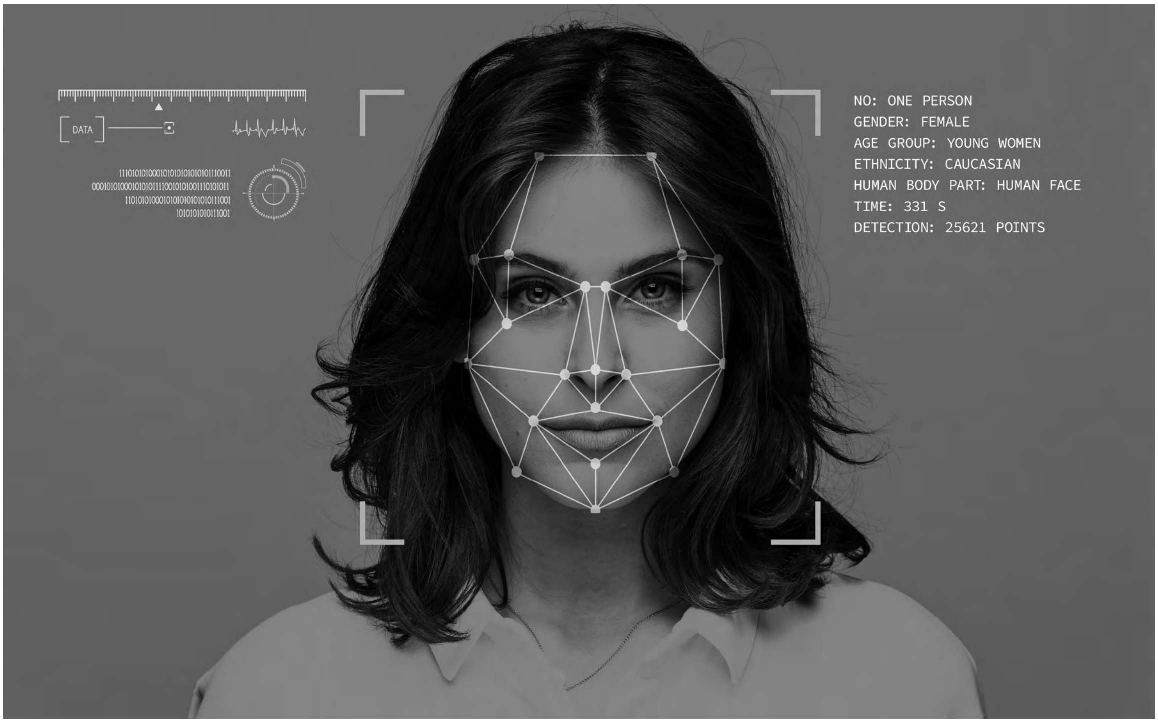
States legislatures have been far more focused on regulating commercial, rather than governmental, collection and use of biometric data. Biometric identifiers include a multitude of data points beyond facial recognition, including fingerprints, retina scans, or even an individual's voice. These regulations, called Biometric Information Privacy Acts (BIPAs), govern the collection and use of an individual's biometric identifiers by commercial entities.

These BIPA laws usually have six components: First, they require any individual, corporation, or organization that obtains biometric data to receive written, affirmative consent before they can collect an individual's data. Second, they require companies to disclose for what purposes they're gathering the biometric data and how long they will maintain it. Third, they impose a reasonable standard of care upon any company that obtains biometric data, which creates a new legal duty to protect the information. Fourth, they require biometric data to be destroyed after a period of time. Fifth, they bar companies from selling biometric data to third parties unless an individual gives their consent. Finally, they create enforcement provisions, which usually means granting the state attorney general authority to sue companies that violate the law.

Three states have already passed BIPAs: Illinois, Washington, and Texas. A number of states are also considering similar laws, including Alaska, Connecticut, Massachusetts, Michigan, Montana, New Hampshire, and New York. There are some critical differences between these laws and state legislators should find them instructive as they determine what types of regulations should govern facial recognition policy.

For instance, Illinois's BIPA was the very first to be signed into law and also the only one to include a private cause of action. Under the law, an Illinois resident can sue if they believe their biometric data was collected or used in ways that violated the law; for instance, if Apple didn't receive consent from an individual before taking a face geometry scan for the iPhone X's Face ID system. Illinois's law requires that an individual must prove that they have been "aggrieved" by a violation before they can be compensated under its BIPA. However, the Illinois legislature did not offer any guidance about what conduct rises to the level of harm. As a result, consumers have sued companies for clear technical violations of the law even if they weren't actually harmed. The result was a flood of litigation from plaintiffs and inconsistent court decisions regarding what types of legal claims violated Illinois's BIPA.

Howe v. Speed-way, Rivera v. Google, Vigil v. Take-Two Interactive, and *Monroy v. Shutterfly* are all examples of cases where federal judges struggled to answer the same question: if a company failed to receive affirmative consent from a consumer before collecting their biometric data, but there was no clear evidence of harm, should the plaintiff still be awarded civil damages? In other words, is the collection of biometric data, by itself, harmful to a consumer? In



Rivera, Google's Photo feature used facial recognition to identify individuals who were uploaded by users, which is similar to Facebook's feature allowing users to recognize mutual friends in their photos. Two people who were tagged in Google's Photo feature sued the company but acknowledged that they had not suffered any financial harm. The court eventually decided to dismiss the case due to lack of harm, but no company would want to expose themselves to dozens of similar cases and legal liability.

This unstable legal and regulatory market has already had a negative impact on Illinois's business environment and caused companies to not offer certain services in the state. For example, Nest, a doorbell-camera service that can use facial recognition to inform homeowners who is at their front door does not allow that service in the state of Illinois out of an abundance of caution. Other services that use voice recognition are also not offered in the state.

Illinois offers the clearest lessons for state legislators considering similar regulations: first, biometric data policies should focus on regulating activity that harms consumers, instead of broadly restricting the collection of data. The public should know when their data is being monetized or shared to third parties without their permission. Washington's law reflects this principle by only regulating the collection and use of biometric data if it is gathered for a "commercial purpose." Washington's BIPA defines commercial purpose as "a purpose in furtherance of the sale, lease, or distribution of biometric data to third

parties for the purpose of marketing goods and services which are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier." This focus on the purpose of the data collection also allows policymakers to explicitly allow biometric collection that benefits consumers, like data gathered for security purposes. For instance, Nest allows for facial recognition services in the state of Washington because the state's BIPA has a security carveout.

Second, state legislators should empower state attorneys general to prosecute violations of biometric laws. As noted above, Illinois is the only state that allowed for private causes of action. Both Texas and Washington legislators declined to include similar provisions.

Finally, biometric regulations should only allow for litigation if there is a reasonable likelihood that a violation resulted in actual harm. It is a long-standing principle of American law that a case cannot move forward unless a plaintiff can prove that they have standing. Put simply, that means an individual must prove to a court they have been impacted or injured by the defendant's actions before a case can proceed. The Supreme Court emphasized the importance of this requirement in 2016 when it reversed the Ninth Circuit Court of Appeals for not requiring a plaintiff to demonstrate what concrete injury they had suffered before deciding the case. Standing requirements are necessary because they separate the wheat from the chaff; courts can use them to filter out cases where no one can point to an actual harm and therefore there can be no real remedy.

Commercial facial recognition laws present a difficult task for lawmakers. They must respond to constituent fears about the collection of their data without unduly restricting technological innovation or punishing companies for conduct that doesn't harm consumers. It may not be sufficient for lawmakers and businesses to point out the commercial benefits to consumers, which include increased convenience and security. There may need to be targeted regulation of biometric data collection that responds to reasonable concerns about how this data is used. These regulations should be narrowly written and not include broad restrictions or bans on commercial use of biometric data. They should focus on ensuring that consumers are notified and give their consent before biometric data can be collected based on the purpose of the collection, with specific exemptions for security purposes. They should allow for state attorneys generals to sue for violations of the law. They should also require that plaintiffs prove that they suffered actual harm before a case can move forward. If state lawmakers adopt these principles, they can protect the privacy of their constituents without harming American innovation.

Billy Easley is a Senior Policy Analyst with Americans for Prosperity, a part of the Stand Together Network