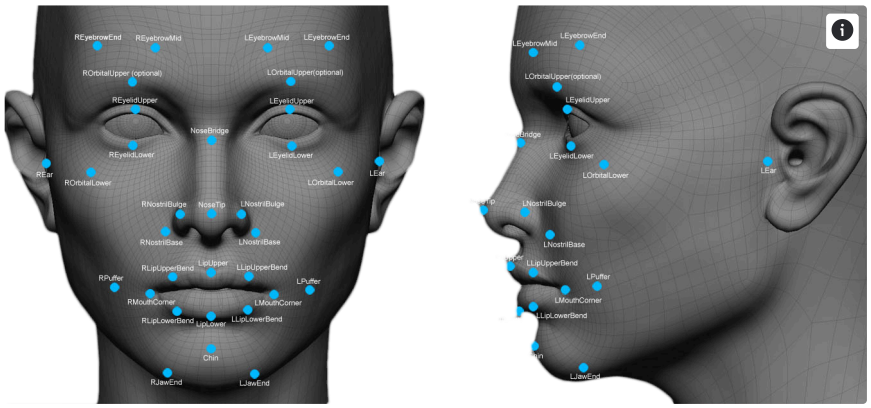
On facial recognition software: impacts on local, state, and personal levels of privacy

Journalism article by Jin YC, originally written in 2019. Edited June 2026.

In the 1960s, the first facial recognition systems were useless on their own. They required a human touch to identify and locate the parts of a face: ears, left and right eyes, nose and mouth.



Various facial recognition points used in a security camera product, by Rhombus.

Now, software has advanced enough that registered faces act as keys to smartphones and computers. Cameras can track specific faces from a crowd and all the associated details.

And they are **always** watching...

At the local level | At the state level | At the personal level

---

At the local level

“There’s something about your face that you can’t hide,” said Ben Ewen-Campen, Somerville’s recently re-elected city councilor for ward three. “We know too much about the biases and the inaccuracies [of facial recognition software]. It’s dangerous to be used currently.”

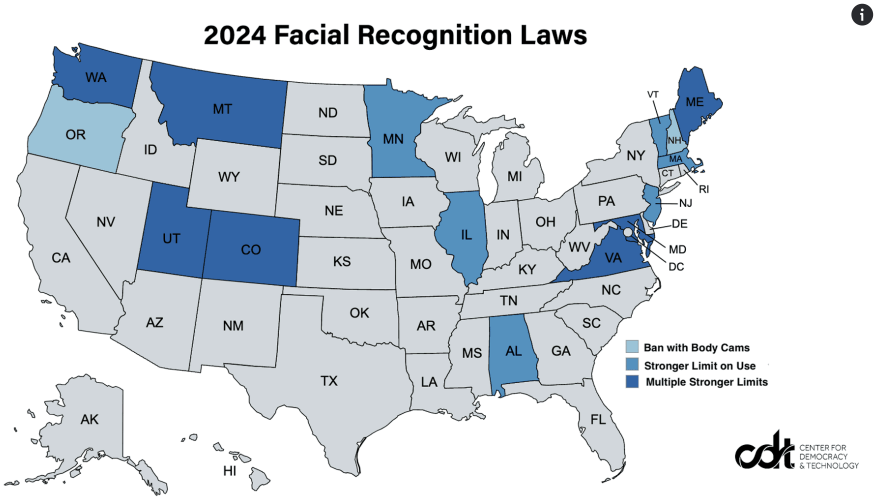
The Massachusetts government made it known to the public that it has been using facial surveillance technology without any legislative permission or restrictions since 2006, but did not elaborate on any deeper schemes.

City responses

On June 27, 2020 Somerville was the second city in the United States to ban the use of facial surveillance software in public spaces, shortly after San Francisco's ban passed on May 14. Since then, two other cities in California have followed suit in the wake of surveillance technology expansion, and cities within the state such as Cambridge are also working on passing local bills to ban the technology.

Ewen-Campen was the main councilor to sponsor Somerville's ban. State Police, while long having had access to data of criminal suspects, now are able to pull regular civilians' data into their database. Due to the normalization of this invasion of privacy, he believes it is important for communities to take a more critical look at local and federal government surveillance in general.

"We don't want to be using technologies that the community doesn't support," said Ewen-Campen. "Huge tech companies ... have incredibly detailed, invasive personal details. We really need state action for this [movement] to have any teeth."



U.S. Map view of states by facial recognition law limits for police body camera, from techpolicy.press

---

The progress of recognition software

Before 2012, facial recognition had since advanced from the 1960s. In 2006, results from the Face Recognition Grand Challenge, where science and engineers come together to improve existing algorithms, were 10 times more accurate than those used in 2002, and 100 times more accurate than those of 1995.

Even with these improvements, however, most technology was still largely unreliable. It was the development of neural nets that allowed the technology to advance sufficiently.

In 2012, when the design was originally tested, **Cornell University** researchers Andrew Ng and Jeff Dean created a system that could recognize cats from unlabeled images. This breakthrough allowed others to create databases for different forms of image identification and was published in their article about machine learning, "Building high-level features using large scale unsupervised learning."

How neural nets are trained

According to Symantec, known for their internet and computer security software "Norton," facial recognition software is generally trained on datasets of individual faces through the use of **neural nets**, a computational model based on the concept of a **human brain**.

🧠 By observing hundreds of thousands of different faces, these **neural nets** learn to:

- Recognize certain areas of the face, such as the two eyes, nose and month.
- Take the color of eyes, hair, and skin into account.

> After sufficient training, the software can make judgements based on the calculations and measurements built through the learning process.

These datasets, however, tend to be biased towards a largely Caucasian facial model.

The result of biases

"Some of the algorithms for people of color, specifically women of color, have very high error rates," said councillor Ewen-Campen, citing about a 20 to 30% error rate for women of color.

The city councilor said that while the main benefit of using the software is being able to identify and track potential criminals, there are no set regulations on the extent to which the federal and state governments can use this technology.

At the state level

Emiliano Falcón, the technology and civil liberties counselor of the **American Civil Liberties Union of Massachusetts** (ACLUM), described privacy as the "control that we have over our personal information."

As an immigrant native to Argentina, Falcón said that identities similar to his would immediately make them a potential target, even if they did not have any criminal history.

"Surveillance generally is directed towards minorities, religious dissidents, religious minorities like Muslims, like immigrants," he said, further stating though technology *should* be developed for liberty, it is often "directed towards these communities which are overpoliced."

Activist groups call for a pause

Currently, the non-profit organization is pushing the state government for a moratorium, a temporary prohibition, which would "press pause" on the usage of statewide technology throughout Massachusetts.

The **ACLUM**'s campaign is officially called "Press Pause on Facial Surveillance."

Press Pause campaign poster from the ACLU of Massachusetts

It is based around on two legislative bills:

1. **Bill S.1385**

   Focuses on establishing a moratorium on face recognition and other remote biometric surveillance systems.

   Petitioned by State Sen. Cynthia Creem, a Democrat overseeing the first districts of Middlesex and Norfolk counties.

2. **Bill H.1538**

   Works with Bill S.1385, following the goal of establishing regulations on the facial and biometric surveillance technologies.

   Presented by Rep. David Rogers, a Democrat who oversees the 24th Middlesex district.

What the bills would do

If the bills are passed, they would make it **illegal** for the state government and state officials to:

- Obtain or use any facial surveillance or biometrics technology without first gaining permission from the legislature.
- After gaining written approval, or a warrant, outline instances of use and follow approval instructions.
- Use this technology to submit data evidence to the courts, such as camera footage.

Activists such as Falcón hope that the moratorium will be implemented within the **ACLUM**'s current session. Until it is passed, however, the people of the Commonwealth are still exposed to privacy risks.

At the personal level

Since the legislative wheel can be slow to turn, activists are trying to inform the public that there are plenty of actions to be taken at the personal level as well.

How did surveillance get this far?

"I feel that since 9/11 in particular, Americans have become accustomed to reductions in their civil liberties in the name of fighting terrorism," said Alex Marthews, the National Chair of **Restore the Fourth**.

He is an expert of the privacy violations around the nation, and an avid advocate for the restoration of the **Fourth Amendment**.

4. The U.S Constitution's **Fourth Amendment** concerns a citizen's right to privacy and protection from unlawful searches and violations.

Marthews works with his non-profit organization to restrain facial surveillance and push for surveillance oversight ordinances, both at the statewide and national level, while also advocating for small personal actions.

He describes the proliferation of technology and access to information as an “endless feast of digital communication” for police in particular.

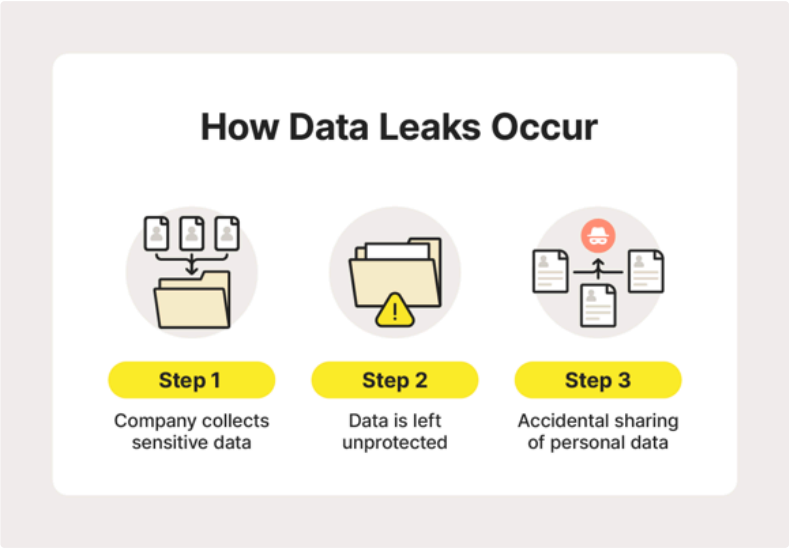
Where the security vulnerabilities lie

Marthews explained that a possible, probable way that an individual’s information could be compromised was through the use of a **smart fridge**.

1. Manufacturers might not take the effort to design products to encrypt their data strongly.
2. The unencrypted (or weakly encrypted) data is shared with the manufacturer.
3. If the manufacturer is compromised, this data is now a possible venue for privacy invasion.

But smart fridges are not the only convenient product that could be potential hotpots of personal data.

Products such as the **Google Home** and **Amazon Alexa** are equipped with microphones that are constantly listening and relatively easy to access. Cameras that are installed as an additional measure of security may very well serve the opposite purpose.



A visual explanation of how data leaks may occur, by Norton

“It shows that we can easily and thoughtlessly walk into a zone where there’s no zone of privacy left,” said Marthews. His concerns lie with privacy as a whole, and he believes that establishing boundaries for facial recognition software is only a start to the actions that the community needs to take.

Advice from an activist

Marthews highly advises people wary of mass surveillance to adopt personal habits that **minimize their digital trace**.

Simply adopting **end-to-end encryption** in one’s text communications would make a large difference. One such alternative app is **Signal**.

End-to-end encryption, or **e2e encryption**, is where the data within the messages are only decipherable to the communicating users’ devices.

- **Note**: While iPhone iMessages are already end-to-end encrypted, the Signal app is a messaging platform alternative to people without iMessage who are concerned about privacy.

Marthews also recommended the **State of Surveillance** website, an excellent “getting started” resource for digital privacy. On the website, there are guides for:

- Changing browser privacy settings
- Which email services offer strong privacy protections
- How to use VPNs
- And more

“The more sand we can throw in the gears of what they’re trying to do,” said Marthews, “the harder it will be for them to implement a statewide surveillance system.”

“But even if we fail,” he said, well aware that he could be a target for those he is working to hold accountable. “We don’t want to go down without a fight.”
