

1. Am I in a database?

No — not unless a retailer added you to their security list after an incident.

SAFR Guard does not build a general-purpose database of the public. There is no file with your name on it. There is no profile sitting somewhere waiting to be matched. If you have never been involved in an incident at a store using SAFR Guard, the system holds nothing about you.

2. Then what happened when I walked through the door?

A few separate things happened, and they get mixed together constantly.

The biometric. The camera converted your face into a set of measurements — a template. A string of numbers. It compared that template against the store's security list, found nothing, and deleted it. That happens inside the camera in under a second. It never reaches the cloud and it never reaches us.

The still image. A photo was captured, the same way a security camera captures one. It sits on the same clock as the store's ordinary security footage.

The video. The store's security camera recorded you, the same way every store you have walked into for the last thirty years has recorded you. That is CCTV. It existed before face matching and it would still be there if we disappeared tomorrow.

The list. Nothing was added to it.

3. How long do you keep any of it?

Different things sit on different clocks, so here is the whole picture in one place. We have not seen another vendor in this category publish this, which is part of why we are.

	If you are not on a security list	If you are a repeat offender
Biometric template	Less than 1 second	1 Year
Still image	Up to 30 days	1 Year
Video footage	Up to 30 days	Up to 30 days

If you are not on a list, the biometric template is gone in under a second — before it ever leaves the camera. The image and the video sit on the standard security footage clock so the retailer can review an incident if one happens. That is the same window retailers have used for closed-circuit video for years, and it is where the loss prevention industry as a whole operates.

If you are on a repeat offender list, the image and biometric template are held for a year. Repeat offense patterns run on a long cycle. A short window means someone who hits a store in March and again in November looks like a stranger both times, which defeats the entire point of a prevention system.

You may have seen a 30-day figure in coverage of our privacy policy. It is real. It is the image and video window in the table above, and we would rather print the whole table than have you find one row of it somewhere else. The reason that window exists is practical: if a retailer discovers days later that an incident happened, the footage and images are still there to review.

4. Who decides who goes on a list?

A retailer submits an image and a description of what happened, and the person submitting it signs a declaration, under penalty of perjury, that what they described actually happened. We review it to determine whether it is a safety or security incident. If it does not meet that standard, it does not go on.

That review step matters more than anything else in this system. The watchlist is where the real risk in this technology lives — not in the algorithm. A highly accurate system pointed at a carelessly built list still produces a bad outcome. So retailers do not add people unilaterally, and we do not treat an accusation as a decision. That signature is part of why. Someone at the retailer has to attach their own name to the submission, which makes it much harder for one employee to quietly add a shopper over an argument at the register.

Children are out of scope entirely. We suppress detections of anyone who appears to be under 14, and we do not allow enrollment of juveniles at all.

5. Does this go to the police? To ICE?

No. We have never shared retailer or shopper information with any government agency, including U.S. Immigration and Customs Enforcement. Not once.

Like every technology company, our privacy policy notes that we would have to respond to a valid court order or subpoena. We have never received one relating to SAFR Guard, so we have never disclosed anything under one. We are stating that plainly rather than burying it, because any company that does not mention the clause still has it.

6. If one store flags me, does that follow me everywhere?

Not automatically. Retailers can choose to share records with other participating retailers, and when they do it is deliberately narrow: incidents involving suspected violence or high-dollar theft, shared within the same geographic area. It is not a national list. It is not every incident. A single accusation at one store does not propagate across the country.

7. What if you are wrong?

It happens in this industry, and we are not going to pretend otherwise. The FTC's case against Rite Aid came down to a system flagging innocent shoppers and employees treating those flags as proof.

So the design starts there. An alert is not a verdict. A match runs through multiple verification steps, including a second algorithm, and a trained person makes the final call. The system does not stop anyone. It does not lock a door. It does not contact anyone. It tells an employee to pay attention, and everything after that is a human decision.

If you believe you are on a list and should not be, the sign on the door has a QR code. It goes to our privacy policy and our contact information. Ask us to delete your data and we will.

8. Is any of this legal?

Yes — and it is a fairer question than it sounds, because the answer is not identical everywhere. For example:

- In California, a senior attorney at the Electronic Frontier Foundation — an organization not in the business of defending surveillance technology — told a reporter that it does not appear to violate state privacy law. Under the CCPA you can opt out of the sale or sharing of biometric data.
- In Washington, state law includes an explicit carve-out for retailers using this technology to detect theft. The legal question in retail face matching was largely settled a while ago. The open question is whether a given company runs it responsibly. That is a harder question, and it is the right one to ask.

One last thing...

You knew to ask these questions because there was a sign on the door. We require that. Every retailer using SAFR Guard has to post one. Most of this industry does not — which is why you have walked past a lot of cameras you never thought to ask about.

For more information on SAFR Guard's stance on privacy, visit our SAFR Guard Privacy Center.

<https://safr.com/safr-guard-privacy-center/>