SECUROS FACEX

Next generation facial recognition.

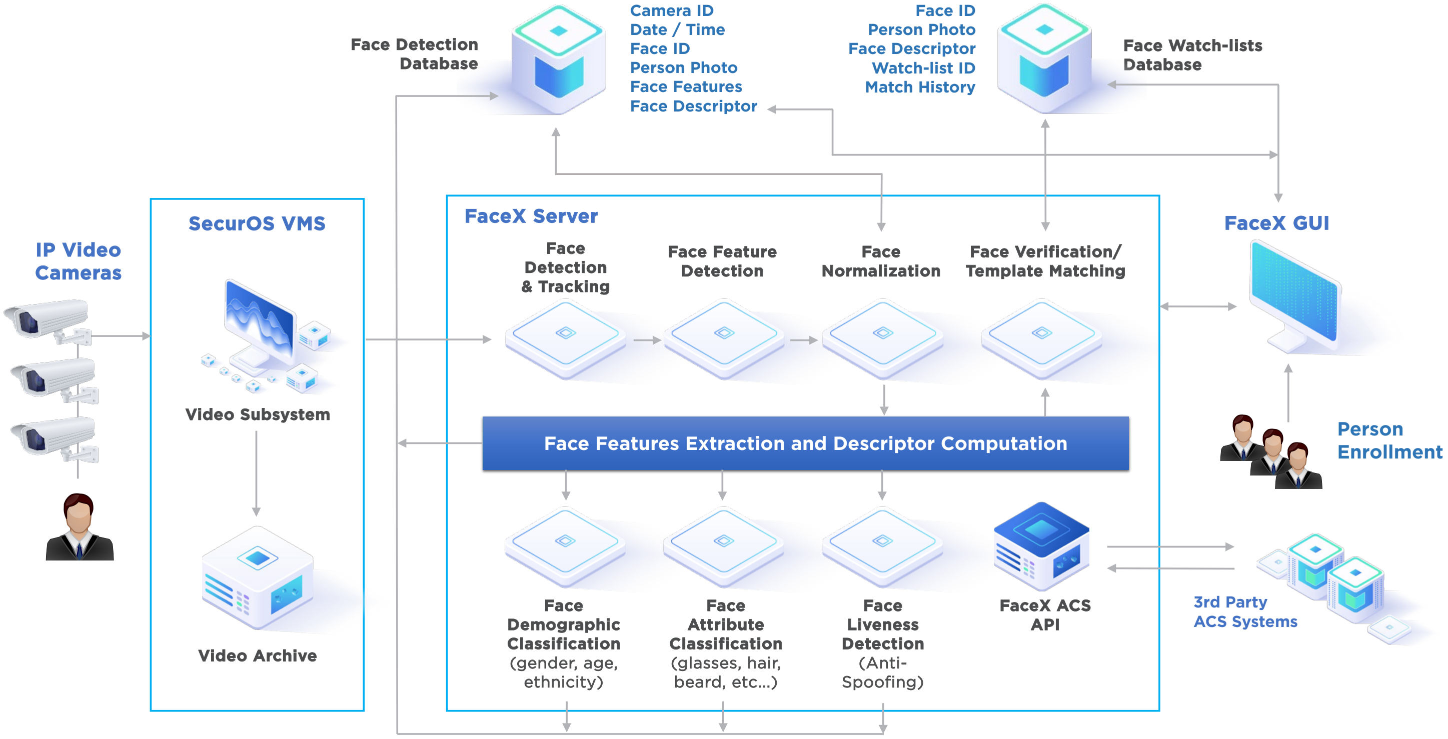
Technology Overview and How Personal Information Is Protected

Facial recognition can be used for various applications such as access control, recognizing known criminals or people of interest, and providing increased security for high risk facilities related to both inside and outside threats. However, due to a lack of understanding of the responsible use of the technology, many are worried about potential personal information litigation as well as how their faces will be used or stored.

Below are a few important points to note and understand regarding ISS' SecurOS FaceX facial recognition system along with options for responsible deployment.

How the FaceX system works:

SecurOS FaceX facial recognition is a software that measures details of a human face and creates a digital descriptor, stored as a numeric code, that identifies one human face as a virtually unique entity different from any other face. These numeric values are stored in a SQL database and used, in conjunction with the recorded video, to correlate the face in the video to its unique digital descriptor. The video is stored in archive files in ISS' proprietary format and the digital descriptors are stored in a SQL database with a time/date reference to one-another. The entire system has an encrypted and secure login process to ensure neither database nor the archive may be accessed by unauthorized users. An additional layer of encryption can be added to protect against unauthorized access by using Self-Encrypting Drives (SED). Video and metadata recording can be encrypted using these SED-compatible drives and controllers. SED technology relies on dedicated chips to encrypt all data with AES-128 or AES-256 and does not occupy CPU resources.



System Components:

1. **Recognition Algorithm:** Neural Network aided algorithms detect faces within a complex video image, perform calculations to create a unique descriptor, and store that metadata as a 2 KB data set in a SQL database table. This data set, outside of the system, has absolutely no meaning or reference to the actual person or identity.

2. **Face Detection Picture:** From the video image, all detected faces are isolated and cropped to be independently stored as thumbnails for future reference. Those thumbnail images are also stored in a SQL database table with an internal reference to the 2 KB digital descriptor. The thumbnails have no reference to the actual person or identity.

3. **Security Camera Video:** Most facilities are recording video from their cameras. The face detection picture has a time/date stamp allowing reference to the recorded video. That recorded video is important as it provides the context of the detection/recognition. It provides clues about what the person is wearing, doing, carrying, etc.

4. **Watch-lists:** These can be employee profiles tied into the recognition system allowing the enrolled/authorized person to enter a secure area. Watch-lists can help identify known criminals, terrorists, sex offenders, terminated/disgruntled employees, active/expelled students, missing children related to sex trade or momentarily lost children and elders. Essentially, watch-lists allow the system to provide notice when specific people have been detected.

Facial Detection vs. Facial Recognition

Facial Detection
SecurOS FaceX uses neural networks to find faces among all the elements of a video image. The Facial Recognition algorithm takes measurements of the face to create a virtually unique numeric descriptor (biometric template) for each face in each video image. Because video cameras take many pictures per second and because people can appear in many cameras throughout the day, each person could easily have thousands or even millions of slightly different descriptors associated with their face (every digital image recorded by a camera is unique). Those descriptors are stored in a designated table in a SQL database. The 'detection' pictures are cropped out of video frames and stored in a separate table, as well as in a SQL database with an ID that allows the system to reference the associated template. Lastly, those pictures are correlated to the recorded video via time/date stamps.

Facial Recognition
A picture or video image may be used to determine any time that a face was detected in the system. Those pictures could be loaded momentarily or accessed via a stored database for ongoing recognitions. The system creates a descriptor from the picture and compares it to all the stored descriptors or incoming/live templates. Based on the similarity between descriptors as templates, the system creates a recognition/similarity percentage. Highly similar descriptors become 'Recognitions'. Those recognitions and detections can be scheduled to be deleted automatically based on administrator preference, corporate guidelines and state or regional regulations.

Risk Management

Security risks?

1. The metadata is specific to the system and has no value outside the system.

2. The system doesn't provide any user or programming interfaces to use biometric descriptors, i.e. even extracted from the system biometrics cannot be used.

3. The thumbnails have no reference to 'identity' or personal info.

4. The recorded video has the same risk as any other surveillance video system. There is nothing unique about the video recorded for general surveillance versus that recorded for facial recognition.

5. The watch-lists may or may not contain personal information. These lists should be secured according to organization policies based on the specific information that they contain. The watch-lists are the property and responsibility of the entity developing and maintaining them.

Legal risks?
To date, Illinois has the most stringent biometric laws. That said, even those laws are easily managed with responsible use of the technology. The Illinois Biometric Information Privacy Act states:

- Private entities collecting biometric identifiers or biometric information must have a written policy, made publicly available, that sets a retention schedule for destroying such information when the initial purpose of collection has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.

- When an individual's biometric identifier or biometric information is first collected, the individual must: be informed that the biometric data is being collected, be told of the "purpose and length of term" of the biometric data collection, and provide a written release.

- Biometric data can't be sold, and it can't be disclosed unless the individual concerned consents to the disclosure (or certain other exceptional circumstances apply – e.g., required by law).

So, while these requirements pose a challenge, they only provide stipulations for the use of the technology. They do not ban the technology.

What steps should be taken:

1. Organizations should write a policy stating the intended use for facial recognition technology and how the data will be destroyed at the appropriate time. This concept is not new. In fact, most organizations already have policies related to their Electronic Access Control system usage along with their surveillance system. Proper policy should be standard fare.

2. Proper signage and authorizations should be incorporated.

    a. For organizations using Facial Recognition as a credential for access control, it should be offered as a convenience option for employees. It should be an opt-in system.

    b. Adding 'authorization' language to the visitor management system during check-in will make this a seamless process for visitors and vendors/contractors.

    c. Adding signage in and around the building, similar to the signs used to indicate Video Surveillance is being used will cover those passing through or around the building.

3. Do not sell any Facial Recognition Data! If it is being used for commercial purposes, MANY other rules and regulations would apply. As long as this is not being done, your use of Facial Recognition should be easily justifiable and defensible.

Summary of important points:

1. Personal information is stored only when the customer decides to store it in a watch-list.

2. The customer decides what information to store in the profile for each entity in the watch-list. i.e. first and last name can be omitted leaving only abstract ID in the watch-list to refer to a person in any database separate from the facial recognition system.

3. If sensitive information is stored in profiles, the watch-list database should be secured in the same way as any other sensitive data would be according to corporate guidelines.

4. Each Face Detection results in one digital descriptor. Those descriptors have no meaning outside of the system. Digital descriptors have NO STORED ASSOCIATION to personal information.

5. Face Detection pictures have NO STORED ASSOCIATION to personal information.