Xailient

EBOOK

Navigating Biometric Privacy Regulations

A Comprehensive Guide

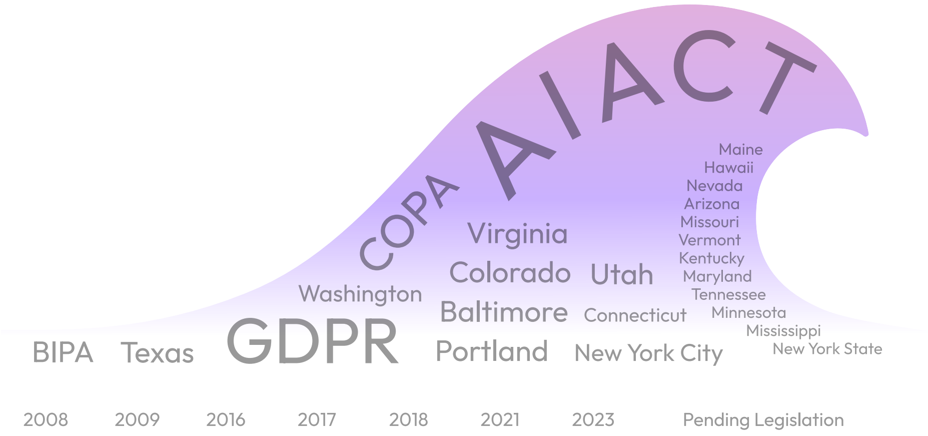
With this rise in technology comes the need for robust regulation to protect individuals' privacy rights and mitigate potential risks.

In today's digital age, the use of biometric data, particularly facial recognition technology, has become increasingly prevalent.

In this eBook, we will provide insights into compliance requirements and best practices as well as demonstrate how Orchestrait meets those requirements and best practices.

Table of Contents

Key Privacy Requirements for Smart Home Providers



A wave of regulations is spreading around the globe.

These regulations codify responsibility and have meaningful and significant penalties. Regulators are taking frequent and serious enforcement actions, issuing fines and in some cases compelling the deletion of data and/or of whole AI models.

Many of these laws follow the pattern of the GDPR in Europe, which sets standards based on 'the state of the art,' lowering the burden of proof for the regulator as no willful failure needs to be demonstrated.

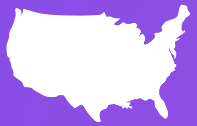
A privacy breach can itself be cited as evidence of a failure to comply. Don't get caught unprepared

Learn what's required →

US and International Legislation

12 states
13 pending

Legislation protects the privacy and rights of individuals and helps businesses avoid legal consequences and reputational damage. In effect in 12 states, **with 13 pending** legislation.



US:
California Consumer Privacy Act (CCPA); Biometric Information Protection Act (BIPA) and other local jurisdictions

EU and UK:
General Data Protection Regulation (GDPR)

Key Requirements:

Informed Consent

Obtain explicit and informed consent from individuals before collecting and using their facial data

Transparency

Communicate the purpose and scope of facial recognition technology to users

Data Security

Implement robust security measures to protect facial data from breaches

Minimization of Data Collection

Only collect facial data that is necessary for the intended purpose; avoid unnecessary retention of data

User Control

Provide individuals with control over their facial data, including options to opt-out or revoke consent

Regular Audits

Conduct regular audits to ensure compliance with privacy regulations and ethical standards

What Can Happen If I Don’t Comply?

$

20M€

in potential fines or 4% of global annual turnover

$5K

for damages or intentional violations per violation Contains private right of action:

Who is the Enforcer?

Most jurisdictions, such as the EU, the States of California and Texas, empower government officials such as their **Attorney Generals** to investigate and enforce the regulations.

Illinois is unique in creating a 'right of private action,' meaning that any person can file a lawsuit against companies operating in the state and seek to prove their case in court. Both meritorious and spurious lawsuits can lead to legal bills, and many companies have chosen not to operate biometric systems in the State of Illinois, even when they are compliant.

Orchestrait^{TM} enables granular configuration of AI features and data collection, beyond just at a state level - even at county or municipality level!

The European Union's AI Act

Most Important To Know:

It extends its regulatory reach extraterritorially, impacting organizations beyond EU borders.

Compliance Mandated:

Within 6 to 24 months from enactment

Takes Effect:

2025

The EU AI Act introduces a nuanced categorization of AI systems based on risk levels.

Risk Levels:

- Prohibited AI
- High-Risk AI
- Limited Risk AI
- Minimal Risk AI

What It Prohibits:

Untargeted collection of face images

What Can Happen If I Don’t Comply?

Penalties of up to 7% of global annual turnover

Market surveillance authorities

Any individual can make complaints about non-compliance

Key Requirements for High-Risk AI Systems:

- ✓ Risk management and quality management
- ✓ In-field accuracy testing and monitoring
- ✓ Bias measurement & mitigation
- ✓ Auditable logs and/or other human oversight
- ✓ Data governance

Prepare for reality. Get compliant. →

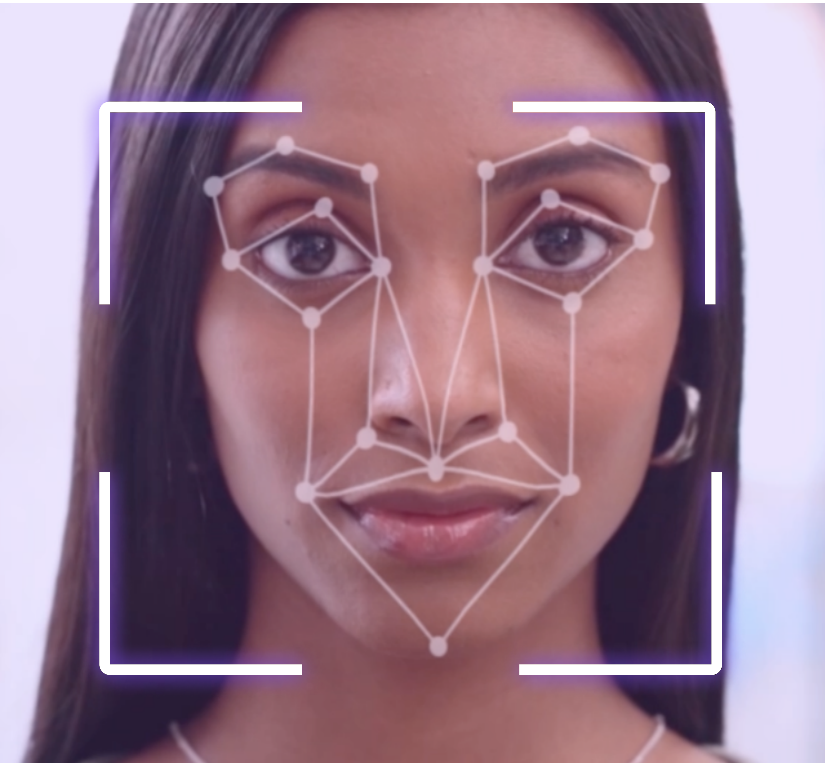
How Orchestrait™ Implements Privacy by Design into Face Recognition

Key Privacy Protections

By implementing privacy by design, Orchestrait™ allows you to implement face recognition technology into your smart doorbell while protecting the privacy of your users and other visitors to their homes.

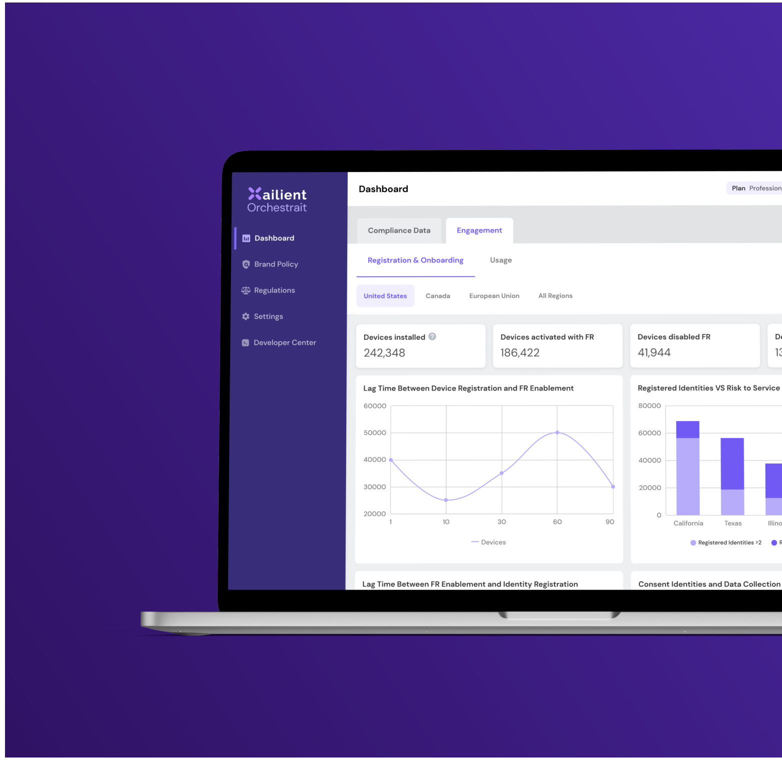
Orchestrait™ is designed to help you address the most advanced privacy frameworks, including the EU and UK General Data Protection Regulation ("GDPR"), the Illinois Biometric Information Protection Act ("BIPA"), and the California Consumer Privacy Act ("CCPA").

Our product includes key innovations that protect privacy and help you address the obligations you may have under the law.



Orchestrait Protects Privacy in Several Important Ways:

1. On-Device Matching
2. User Control
3. No Stranger Identification
4. Auditing and Improvement
5. Distributed Architecture
6. Customizable Control Dashboard



Devices installed
242,348

Devices activated with FR
186,422

Devices disabled FR
41,944

1 On-Device Matching

Face matching and identification occurs **only on your users' devices.**

Faceprints never move off of devices. Neither you nor Xailient ever store or have access to faceprints to identify individuals.

Our **Face Recognition Edge AI technology** analyzes photos on a user's device to enable users to identify visitors to their home without ever sharing an individual's faceprint or other biometric information with you or Xailient. This means that **you do not access or store any biometric information when you use our technology.**

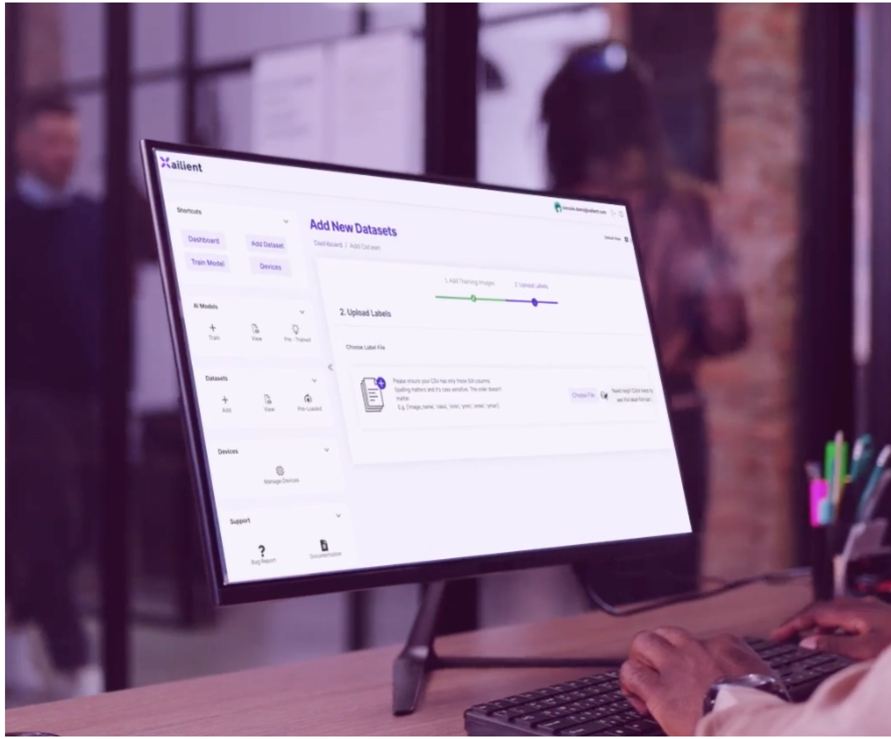
2 User Control

Users remain in complete control of their use of our face recognition technology.

By default, face recognition is disabled until a user takes the affirmative step of enabling the feature.

Users get to decide if they want to use face recognition and whose photos they want to tag. Users can even control whether Xailient can use their images to audit and improve the accuracy of the system, and can disable their use of face recognition technology at any time.

By putting users in control, **Orchestrait™ empowers individuals** to use the technology in a manner that is sensitive to context.



3 No Stranger Identification

We designed the technology to identify an individual only from a small predefined group.

In no event will Orchestrait™ identify to a user somebody who the user hasn't already identified before.

Experts typically categorize face recognition technology as providing one-to-one authentication ("Is this Mary?") vs. one-to-many identification ("Who is this?").

Orchestrait™ takes a middle path, enabling identification of a face out of a limited gallery of pre-identified faces – one-to-a-few ("Who is this out of a household of four people?") – as opposed to a larger undefined audience.

This ensures that any individual whose identity is enrolled in the system has either expressly consented or is already known to the user, such as personal acquaintances (family, friends, services providers), mitigating the risk of surprise and privacy harm.

4 Auditing and Improvement

We continuously audit and improve our face recognition algorithms to make sure that the service we provide is accurate and free from unnecessary error or bias. This allows us to provide one of the most **accurate services on the market**, reducing the risk of misidentifying someone and causing privacy harm.

Because all face matching happens on a user's device, we **never use individual identities for auditing and improvement** purposes. Instead, we extract only the minimum information necessary – usually only a crop of an image and limited metadata, such as whether the image matched the reference photo – to train our models and verify their accuracy.

We never combine any information we collect from your users' use of the technology with information we collect on behalf of our other customers. You can direct us to disable our use of your information for auditing and improvement at any time.

5 Distributed Architecture

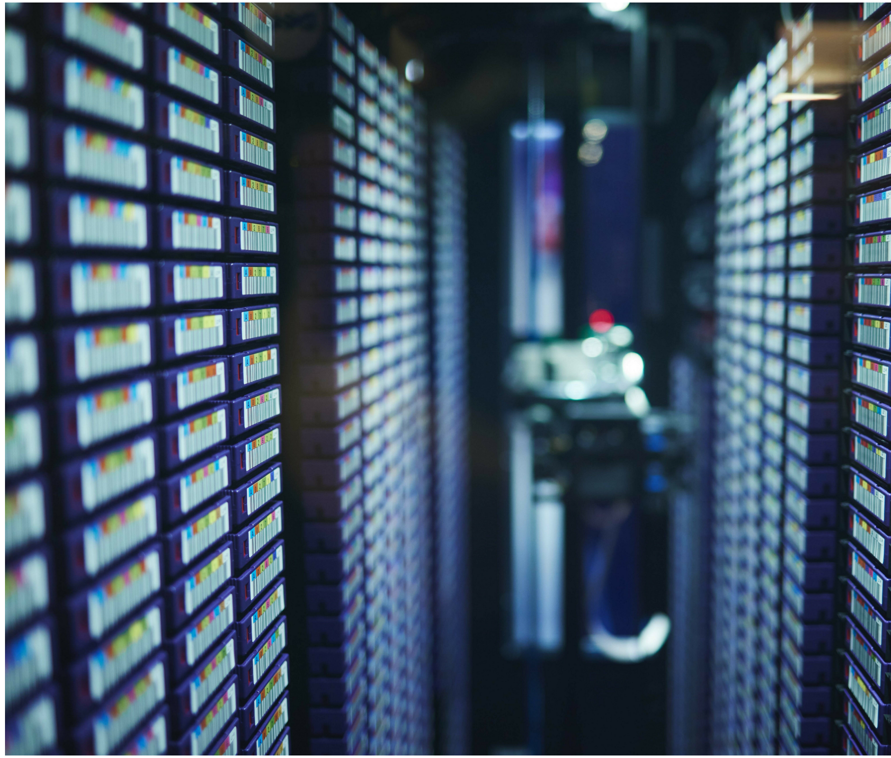
The system is distributed across different actors and devices so that face templates and identities are not stored together.

Orchstrait™ protects privacy by implementing **a decentralized architecture that distributes information** across logical partitions, preventing biometric information from being matched with identities anywhere other than on a user's device.

Neither the customer cloud nor the Xailient cloud ever receives an individual's faceprint; only face crops and metadata are transmitted to the cloud.

The audit cloud never receives any individual identity; it only obtains face crops and reference images to confirm whether or not there is a match. Only a user's device can combine identities with faceprints.

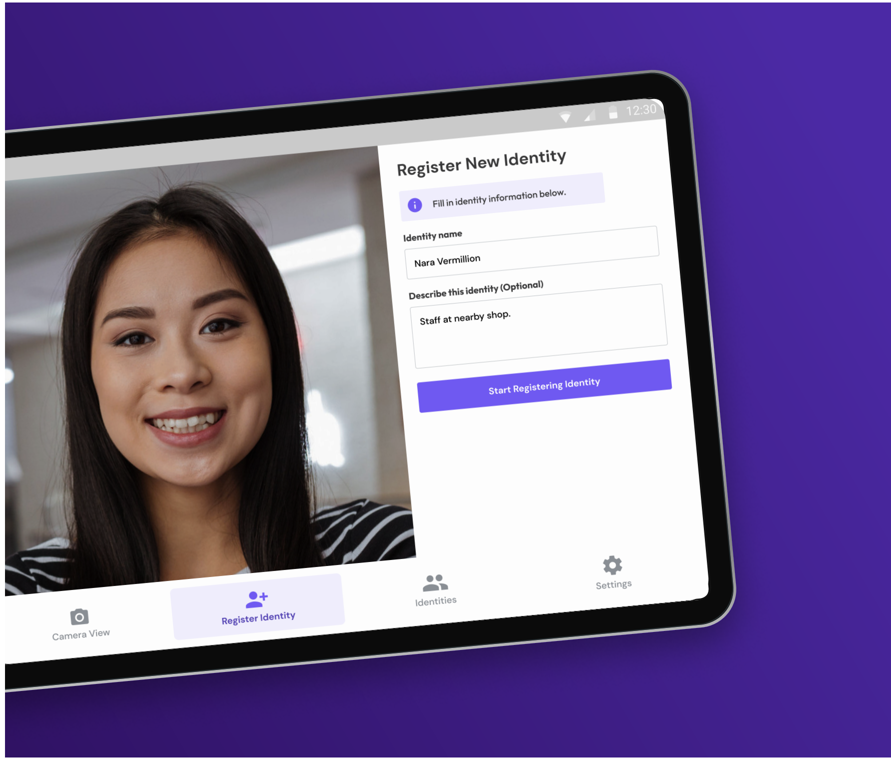
This is designed to minimize the risk of privacy or security incidents and to comply with privacy laws.



6 Customizable Control Dashboard

We provide an **easy-to-use dashboard of controls** that allows you to customize how you deploy our service in your key markets, depending on your needs and user expectations, as well as **guidance on how to inform your users** about your deployment of our product and the privacy features it includes.

For example, you can choose whether to allow us to collect information for auditing and/or improvement purposes. You can apply this choice across the board, or you can select different settings for different jurisdictions.



Register New Identity

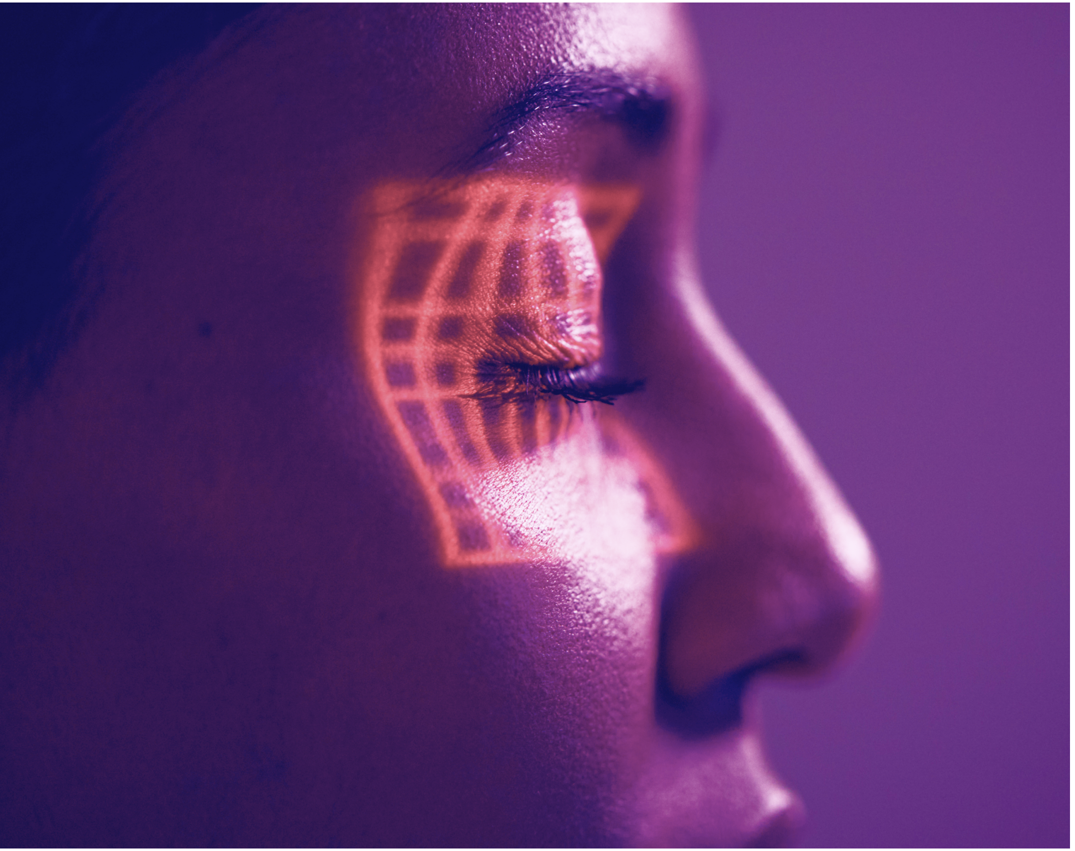
Fill in identity information below.

Identity name: Nara Vermillion

Describe this identity (Optional): Staff at nearby shop.

SECTION 3

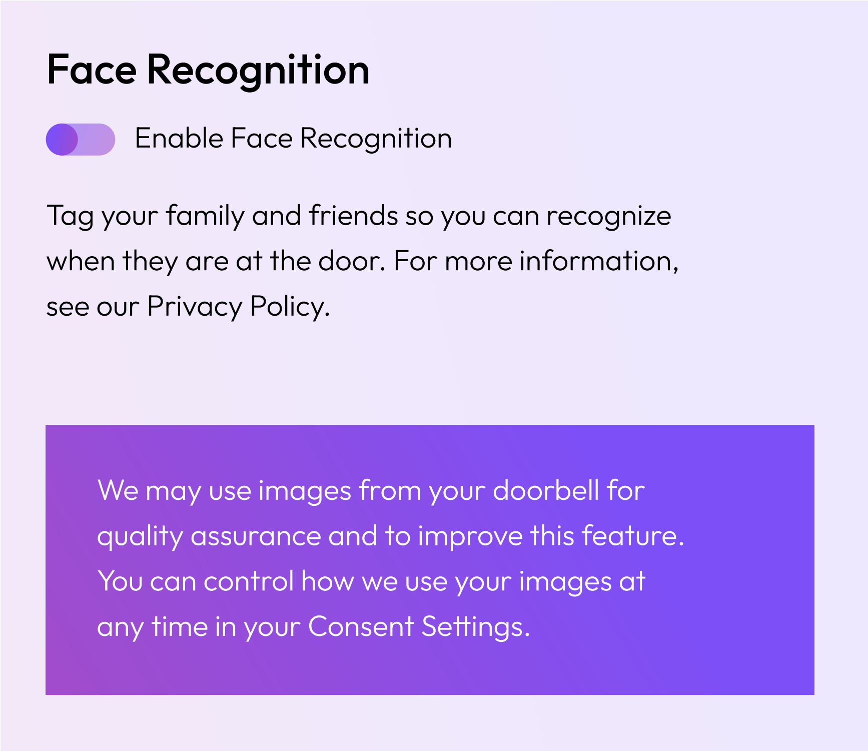
How To Implement the Solution



Opt-in to Enable the Face Recognition Feature

The following language provides an example of how you may present to users the opt-in language to enable the face recognition feature.

Example Language:

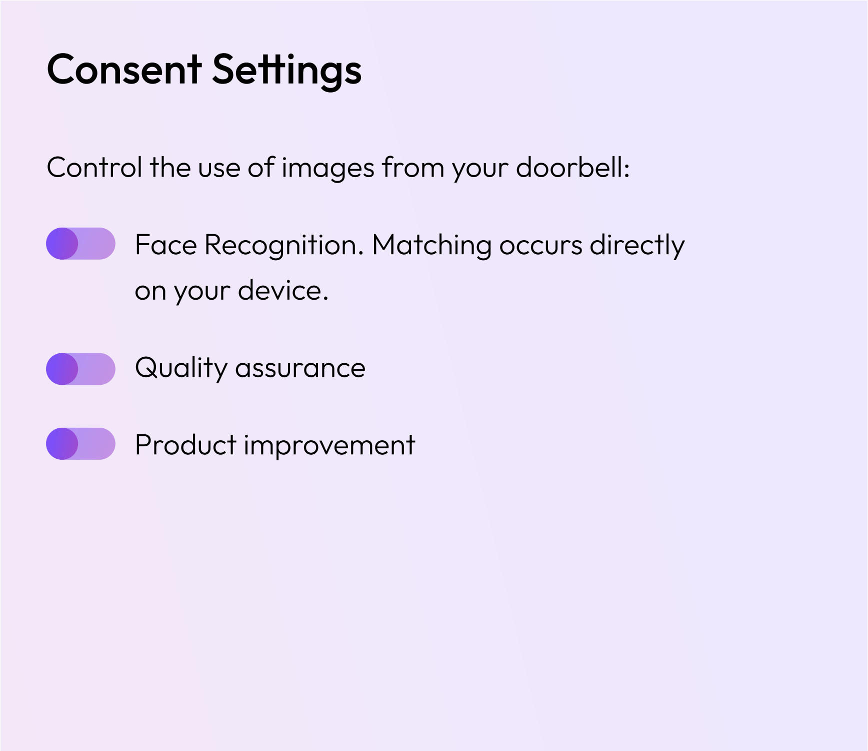


Face Recognition

● Enable Face Recognition

Tag your family and friends so you can recognize when they are at the door. For more information, see our Privacy Policy.

We may use images from your doorbell for quality assurance and to improve this feature. You can control how we use your images at any time in your Consent Settings.



Consent Settings

Control the use of images from your doorbell:

● Face Recognition. Matching occurs directly on your device.

● Quality assurance

● Product improvement

Provide Option to Revoke Identities

The following is an example of the user experience you may offer users to enable them to remove identities from the system

Manage your tagged family and friends:

[Name 1] – Edit / Remove

[Name 2] – Edit / Remove

[Name 3] – Edit / Remove

[Name 4] – Edit / Remove

Please note that if the user disables the Face Recognition Feature, it will pause all face recognition activity, including tagging. When the user enables the feature again, the tagging will resume.

How to Explain our System's Operations to Your Users:

1 What Data does the System Collect?

When a user enables Face Recognition, the user will be able to select photos from the image library on their phone or from the image library on their doorbell camera as reference images to identify people who come to the door.

Face Recognition works by generating a scan of face geometry (known as a faceprint) from the reference image, and using the faceprint to determine if someone approaching the door is the same person as in the reference image. This matching occurs exclusively on the user's device and the faceprint is never shared off the user's device. The only information that is collected off the device is a copy of the reference image and face images captured by the doorbell, whether the images produced a match, and a unique ID number.

2 How is the Data Used?

Face Recognition notifies users when individuals that were identified by the user are at the door. All matching occurs on the user's device. In addition, copies of face images are collected off the device (a) for quality assurance purposes, including to verify the accuracy of the system, and (b) to develop and improve the Face Recognition feature.

Users can disable the use of face images for quality assurance and feature improvement at any time, while continuing to use the Face Recognition service, within the Consent Settings.

3 What Choices do Users Have?

Face Recognition is disabled by default. This feature is available only to users who opt-in to enable Face Recognition. Once enabled, a user can disable the use of face images for quality assurance and feature improvement at any time, while continuing to use the Face Recognition service, within the Consent Settings.

4 How is the Data Shared?

All matching occurs on the user's device and faceprints are never shared with any third party off the user's device. However, copies of images captured by the doorbell and metadata, such as the doorbell's unique ID number, are shared to the cloud and with service providers to enable the feature to function, and for quality assurance and feature improvement purposes.

Consumer-Facing Terms of Use

In certain jurisdictions, the law requires users to obtain the consent of individuals whose biometric information is processed by the system.

Consider adding language to your user agreement (e.g., Terms of Use) to make clear that the user is responsible for their own use of the service, including for obtaining any required consents.

The following language provides a sample of the provisions described above that Customer may include in its user agreement:

> [Customer] product is intended for personal and household use. When you enable [Face Recognition], the system will generate a faceprint of any third parties you identify using the system. The faceprint will be stored exclusively on your device and will not be shared with [Customer] or its service providers. This faceprint may be considered “biometric information” under applicable laws.
>
> You are responsible for making sure that your collection of faceprints from other third parties who you identify using the system complies with applicable laws. This means that you should make sure you have consent from all third parties before you identify them using the system.

Be compliant.

Reach out to Xailient today! →

Xailient

See what matters