Apple Vision Pro Privacy Overview

Learn how Apple Vision Pro and visionOS protect your data

February 2024

Contents

Introducing Apple Vision Pro

Apple's privacy principles

Data minimization
We use innovative technologies and techniques to minimize the personal data that we, or anyone else, can access.

On-device processing
We minimize data collection by processing as much of your data on your device as we can, rather than sending it to a server.

Transparency & control
We help you better understand the data being collected so that you can make your own choices over who you share that data with and how it's used.

Security
Security protections, such as Data Protection, are the foundation of privacy.

At Apple, we believe privacy is a fundamental human right. Like all our products, Apple Vision Pro and visionOS were built with privacy and security in mind from the beginning. Apple Vision Pro tightly integrates hardware and software to help you simultaneously feel present in the world around you and seamlessly interact with digital content in your physical space. For our first spatial computer, we had to innovate across every facet of the hardware and software, including how to build great features that don't come at the expense of privacy.

Spatial computing brings digital content closer to your world than ever before - which makes it an incredibly personal device. Apple Vision Pro packs multiple depth sensors, cameras, microphones, and gyroscopes generating a wealth of realtime data to drive a rich immersive spatial experience. It was at the forefront of our design for that data to enable an amazing user experience and not be collected and used for other purposes by Apple, apps, or anyone else.

We built visionOS from the ground up to protect your privacy and the privacy of people around you. Apple Vision Pro is the first Apple product that uses advanced always-on camera streams of your eyes and the world around you to enable spatial experiences. And where you look can reveal what you are thinking, such as links you almost clicked or apps you thought about downloading. To keep your thought process private, where you look before you interact with content is not shared with Apple or the apps you are using, and does not leave your device. Similarly, because Apple Vision Pro blends digital content with your physical space on-device, the apps you use cannot access information about your surroundings by default. This paper details how each feature designed for spatial computing was built to provide a powerful user experience while protecting the privacy of both the person wearing the device and those nearby.

Privacy by design

Privacy features brought to Apple Vision Pro

1. Advanced Data Protection
2. App Tracking Transparency
3. Data Access prompts
4. Data Protection classes
5. Hide My Email
6. iMessage encryption
7. iCloud Private Relay
8. Location Services
9. Privacy indicators
10. Private Network Address
11. Safari Private Browsing

And many more!

We've been building privacy features and protections into our products for years. Safari Private Browsing, App Tracking Transparency, Privacy Nutrition Labels, and Advanced Data Protection are part of the privacy foundation of many of our products including Apple Vision Pro. As a result, Apple Vision Pro shares the same strong privacy and security foundation in all our platforms.

In some cases, we expanded these features on visionOS to meet the unique needs of Apple Vision Pro. For example, we added three new data types that apps can add to their Privacy Nutrition Label on the App Store: information about head movement, hand movement, and your surroundings.

We integrated hardware and software on Apple Vision Pro to protect your information in light of the unique privacy challenges posed by spatial computing. Apple Vision Pro features, from using it with your eyes and hands to showing digital content in your physical space, also have privacy built in. There are four privacy principles that inform everything we do at Apple, including all the new features on Apple Vision Pro. These four principles are: data minimization, on-device processing, transparency and control, and security.

Data minimization
Apple Vision Pro and visionOS minimize how much information developers, including Apple, can collect by only using the data necessary to support seamless spatial experiences. visionOS includes powerful on-device technologies to support realistic lighting and audio, so developers do not need to access information about your surroundings.

On-device processing
visionOS processes data on-device where possible instead of sharing it with Apple or other developers. To protect where you look, the hover effects that are shown when you look at content are rendered on-device by visionOS and are not shared with the app you are using. visionOS also maps your surroundings on-device in order to realistically render virtual objects in your physical space. Additionally, your Persona is generated entirely on-device with photos you take of yourself using your Apple Vision Pro.

Transparency and control
visionOS helps you understand how your data is being used, and gives you control over when it's shared. In addition to offering the existing data privacy permissions from our other platforms, visionOS includes control over sharing hand movement and surroundings data with apps. Additionally, the Guest User feature gives you control over what content friends and family members are able to see when they use your Apple Vision Pro.

Security
Security is the foundation of privacy. Optic ID data is encrypted and never leaves your device. Optic ID uses the Secure Enclave, a special subcomponent of the M2 chip, to store and protect your sensitive biometric data.

Surroundings

The places where you use Apple Vision Pro, like at home, often have detailed information about your personal life. From items on your desk to who is in the room with you, data about your surroundings is protected by visionOS. visionOS blends apps with your surroundings entirely on-device, so the apps you use do not need to access information about surroundings.

visionOS builds a three-dimensional model to map your surroundings on-device. Apple Vision Pro uses a combination of camera and LiDAR data to map the area around you and save that model on-device. The model enables visionOS to alert you about real-life obstacles, as well as appropriately reflect the lighting and shadows of your physical space. visionOS uses audio ray tracing to analyze your room's acoustic properties on-device to adapt and match sound to your space. The underlying scene mesh is stored on-device and encrypted with your passcode if one is set.

How content appears in your space

Windows
Content is shown as a two-dimensional plane in space, like an article you can scroll.

Volumes
3D content in an app, which is viewable from any angle, such as a 3D dinosaur in your room.

Shared Spaces
Apps are automatically shown side-by-side with other apps, similar to a Mac desktop.

Full Spaces
An immersive experience, where only one app appears. Apps can create windows, volumes, and unbounded content.

What surroundings data can be shared with apps with permission?

Plane estimation
Detecting flat surfaces nearby, where objects may be able to be placed.

Scene reconstruction
A polygonal mesh that represents the outline of objects within your physical space.

Image anchoring
Data representing persistent locations of specific objects as you move.

Object recognition
Identifying objects of interest in your space.

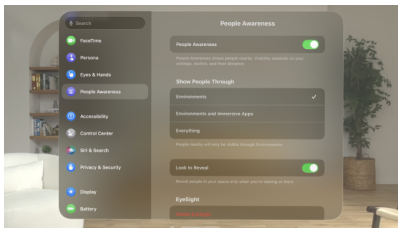
Sharing surroundings data with apps

Apps do not need access to information about your surroundings to build powerful experiences. To provide more immersive experiences, apps will ask your permission to access more information about your surroundings.

Types of apps that can access surroundings
Apps automatically launch into a Shared Space, where the app is shown side-by-side with other apps, similar to the desktop on a Mac. By default, apps cannot access any information about your surroundings. Apps can also open a Full Space for a more immersive experience, where content from other apps disappears and the app can create windows, volumes, and unbounded content. With your permission, apps in a Full Space can access surroundings data to support more immersive experiences.

Automatic: visionOS blends content into your surroundings
Apps in a Shared Space can not access your surroundings, and instead rely on visionOS to automatically blend digital content into your space. visionOS automatically adjusts the content to the physical lighting conditions and audio characteristics of your space without giving apps access to information about your surroundings. As your environment changes, like when you turn on the lights or the sun sets, visionOS continuously adjusts how apps are displayed to ensure content always matches the physical characteristics of your physical space.

With permission: apps can access surroundings data
You can choose to give Full Space apps access to your surroundings to further integrate digital experiences in your physical environment. For example, Encounter Dinosaurs requests access to your surroundings so the dinosaurs can burst through your physical space. By giving an app access to surroundings data, the app can map the world around you using a scene mesh, recognize objects in your surroundings, and determine the location of specific objects in your surroundings. The app will only get access to information about your surroundings within five meters of where you are.



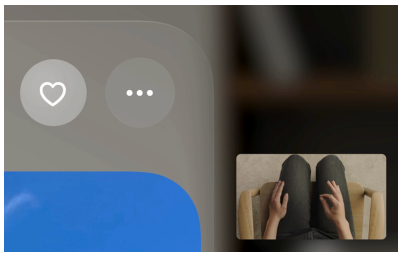
You can control how prominently people are shown to you on Apple Vision Pro in People Awareness Settings.

People Awareness

People Awareness helps you see and hear the people around you while you are using apps on Apple Vision Pro. In addition to helping you stay connected to people around you, People Awareness helps ensure you are not surprised by who can hear or see you.

visionOS does not share information about who may be physically nearby with the apps and websites that you use, or with Apple. Information about who may be physically nearby does not leave the device. And visionOS allows you to control how prominently people are shown to you while you use Apple Vision Pro. In Settings > People Awareness > Look to Reveal, you can choose how prominently people in physical proximity to you are surfaced through your digital content.

Input

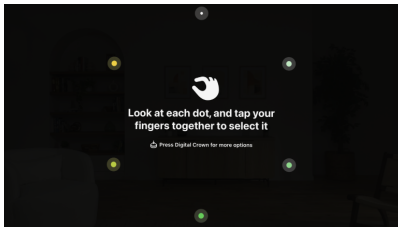


You can click on a button by looking at the button, and tapping your fingers together.

Apple Vision Pro allows you to seamlessly interact with content just by using your eyes, hands and voice. The content you look at, but don't interact with, can reveal information about your thought process. We carefully considered the best ways to build powerful experiences using cameras directed at your eyes without unnecessarily revealing information about you to apps and websites. As a result, visionOS does not share eye input with apps or websites, or even Apple. Additionally, apps and websites only know what you select, not what you are looking at when you browse.

Eyes

You navigate Apple Vision Pro with your eyes, and use your hands to select content you want to engage with.

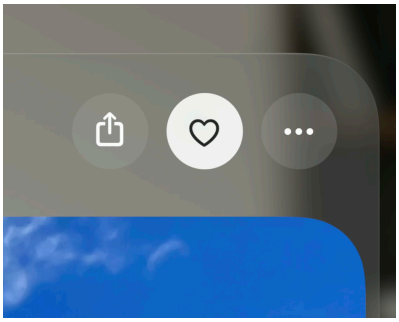


The first time you set up Apple Vision Pro, you will be asked to do Eye Setup.

Data used to calibrate your Apple Vision Pro to your eyes is protected on-device. Apple Vision Pro uses an advanced and interconnected system of LEDs and infrared cameras to project invisible light patterns onto each of your eyes. This system can determine precisely where you are looking while wearing Apple Vision Pro, enabling you to interact with apps and content just by looking at them. These sensors are calibrated to your eyes during Eye Setup, which happens when you first set up your Apple Vision Pro and can be reset in Settings > Eyes & Hands > Redo Eye Setup. Eye Setup results in a customized model of your individual eye geometry. This information does not leave your device, is encrypted, and is not shared with apps.

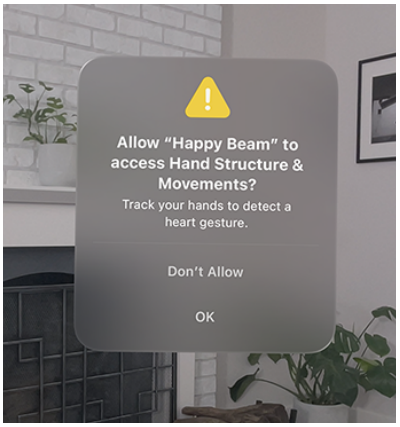
Where you look is not shared with apps because the content we look at, and how long we look at it, may reveal our thought process. visionOS processes eye movements at the system level, and doesn't share where you are looking, or your eye input, with apps or websites before you engage with content. As a result, apps and websites only know what content you select when you tap your fingers together, not what you look at but don't select.

At the same time, visionOS ensures you know what content is selected so you can easily interact with it. We designed on-device protections and an interaction system that enables realistic spatial experiences while protecting your privacy.

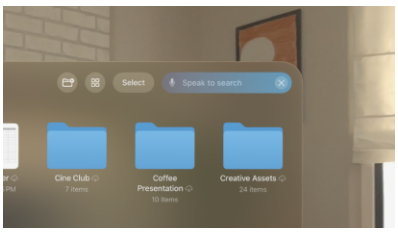


When you look at button, visionOS highlights that button without revealing to the app what you are looking at.

Custom gestures
With your permission, a mapping app can let you hold the globe using a custom gesture.



With your permission, immersive apps can use information about the size and shape of your hands to create custom gestures in their app.



Look to Dictate makes it easier to quickly search for content in apps.

How apps respond to where you look
We know that it’s important for you to be aware of content you’re about to tap on before you tap. As a result, you can tell what you’re about to select on Apple Vision Pro without sharing where you are looking with apps.

visionOS automatically highlights buttons that you look at, without app developers needing to know where you look. For example, if you are looking at a button in an app, visionOS may provide some visual indication like making the button glow. Only when you select the button, by both looking at it and tapping your fingers together, does where you are looking get communicated to the app. Visuals effects that respond to where you look, like a glowing button, are rendered out of process from the app. As a result, the apps you are using are not rendering the effects you see when you look at content — visionOS renders these animations because the apps you use do not know what you are looking at until you make a selection.

Hands

The first time you set up Apple Vision Pro, you will be asked to set up your hands. During enrollment, Apple Vision Pro measures and stores information on-device about the size and shape of your hands and finger joints to make it easier for you to interact with content.

Sharing hands data with apps
Apps do not need access to your hands set up information in order to help you interact with content. For apps that are windowed and not immersive, visionOS will communicate the content you interact with to apps, so that apps don’t need to access your hands set up information.

With your permission, immersive apps can access hands structure and movements to help you interact with content using custom gestures. For example, a developer could create a hand gesture that recognizes when the user forms a heart with their hands, and has an associated behavior. Hand input information includes real-time movement of your finger joints, wrists and elbows. For apps you grant permission to access hand structure and movements, developers can create custom gestures based on hand movements in their app.

Head

Apps do not need to access information about the orientation of your head in order to show realistic three-dimensional content. Apps in a Shared Space cannot access information about the orientation of your head. Full Space apps can use the location of your head to render realistic spatial experiences, and maintain stable perspectives of immersive content as you physically move. Apps use your head position in realtime to prevent any disorientation that may result from content that appears locked to your perspective.

Look to Dictate

Look to Dictate makes it easy to quickly search for content in apps without using your hands. For example, when you look at the microphone icon in a search field in Finder, the microphone will animate if you continue to look at the icon. When

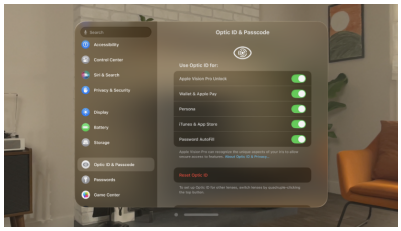
the animation completes, Dictation will automatically begin. As you begin to say what you are searching for, your search query will populate in the search field. The content in your search query is not shared with the app until you finish speaking. If you look away from the search field while speaking, the Dictation will end. This allows visionOS to confirm your intent to dictate without requiring you to click on a text field or unnecessarily revealing information to the app you are searching in.

Virtual Keyboard

The virtual keyboard cannot be accessed or controlled by the apps you are using.

You can use a virtual keyboard to type on Apple Vision Pro or dictate text. When you start typing or dictating, typing suggestions will be shown to you at the top of the virtual keyboard. These suggestions are personalized on-device using your previous typing patterns, and can also include other information like your usernames and passwords. The keyboard is displayed by visionOS and not visible to the app, so the apps you use can only see the text you type or dictate and cannot access the suggestions, including passwords that are suggested. Additionally, only you can access and control the virtual keyboard, not the apps you are using.

Optic ID

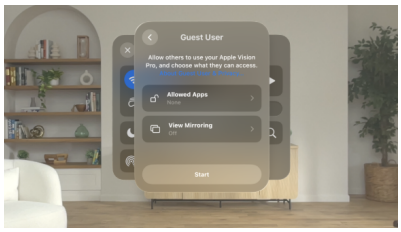


You can choose to turn Optic ID on or off in Privacy & Security settings.

Optic ID lets you securely unlock your Apple Vision Pro, authenticate purchases, sign in to apps, and more. Optic ID uses an advanced system of LEDs and infrared cameras inside the enclosure and machine learning to create a mathematical representation of your iris. Optic ID data — including mathematical representations of your iris — is encrypted and protected by the Secure Enclave. Optic ID data does not leave your device, and is never backed up to iCloud.

If you choose to enroll in Optic ID, you can disable it at any time in Settings > Optic ID & Passcode. If you disable Optic ID, all Optic ID data including mathematical representations of your iris will be removed from your device. Apps can choose to use Optic ID to securely authenticate content in their apps. Just as with Face ID and Touch ID, apps only receive information about whether the attempted authentication was successful, and do not get access to the underlying Optic ID data or any data associated with the enrollment.

Guest User



You can choose whether a Guest User has access to all apps and data, or just the apps that are open.

Guest User sessions let you share your Apple Vision Pro with friends and family members. Unlike an iPhone or iPad that you and a friend can look at together, Apple Vision Pro requires unique eye and hand set up to use and the content is only visible to the person wearing the device. We addressed this challenge with Guest User sessions, which give you peace of mind that guests are not seeing content you did not intend. Guest User sessions also allow you to view what content the guest is looking at on your device using View Mirroring. If you enable View Mirroring, you can choose a supported device to view what a guest sees on your Apple Vision Pro.

You can limit what apps and data someone can access on your Apple Vision Pro by starting a Guest User session in Control Center. You can configure a Guest User session to allow access to all apps and data on your device, or limit the apps they can interact with to just those currently visible. This enables you to share experiences, like showing a friend a spatial photo you took of them, without giving them unrestricted access to your entire device. Even if you choose to give a guest access to all apps and data, guests will not be able to access the following sections in the Settings app: Apple ID, Persona, and Wallet & Apple Pay. Once you start a Guest User session, you will have 5 minutes to give your device to your guest before the device locks itself. You can also use View Mirroring to see what your guest is seeing in real-time, empowering you to help guide them and confirm they are looking at expected content.

When a guest puts on Apple Vision Pro, they will be asked to go through eye and hand set up so that guest can navigate accurately. When your guest takes off your Apple Vision Pro and the Guest User session ends, their eye and hand setup information will be promptly deleted on-device.

Persona

Persona is a digital representation of you that reflects your movements in realtime.

Persona is a digital representation of you, allowing other people to see you while you're using Apple Vision Pro during FaceTime and video calls. Your Persona will reflect your facial expressions and movements in real-time. Persona is available in beta.

Persona is generated entirely on-device using an advanced neural network. The data used to build your Persona, including the photos taken while capturing your Persona, are stored encrypted on your device. You can choose to transmit your Persona in experiences like FaceTime, or if you explicitly choose to provide Persona feedback to Apple.

In order to protect your digital representation, Apple Vision Pro has protections designed to help ensure only you are using your Persona. If a passcode is not set on your device, you will not be able to enroll a Persona. Your Persona is not accessible while in a Guest User session is in progress. Additionally, if the Persona is protected by Optic ID, any change to Optic ID settings deletes the Persona.

If your Persona is protected by Optic ID, your Persona has additional protections. If you have an Optic ID enrollment, using Persona requires a successful Optic ID authentication by default and does not fallback to the passcode. As a result, in the event that a family member or friend is using your Apple Vision Pro and knows your passcode, they cannot access your Persona with just the passcode if you have enrolled in Optic ID.

Persona and FaceTime end-to-end encryption

Your Persona will be used to represent your expressions in realtime for FaceTime calls you join from your Apple Vision Pro. Persona in FaceTime is underpinned by protections designed to ensure that only you and the people you call can see your Persona. And this works no matter what devices other people on your

What is end-to-end encryption?

End-to-end encrypted data can only be accessed on your trusted devices where you're signed in with your Apple ID. No one, not even Apple, can access your end-to-end encrypted data unless you choose to share it. If you lose access to your account, only you can recover this data, using your device passcode or password, Recovery Contact, or Recovery Key.

FaceTime call are using! Your Persona is sent securely to the other people on the call using end-to-end encryption. To make it quick and easy for others to see your Persona, your Persona is stored in iCloud using end-to-end encryption. Only you and people you call can access Persona in FaceTime, not Apple or anyone else.

Persona for apps

If you allow apps to access your Persona, the app will receive a video feed of your Persona, including your realtime movements. Apps will not have access to the underlying camera data of your movements or information used to generate your Persona.

EyeSight

EyeSight reveals your eyes and lets people nearby know when you're using apps or fully immersed.

Apple Vision Pro helps you stay connected to people around you. EyeSight shows a digital representation of your eyes and lets those nearby know when you're using apps or fully immersed in an experience. When someone approaches, Apple Vision Pro simultaneously lets you see the person and reveals your eyes to them. EyeSight shows an indicator when you're capturing a spatial photo or video, to provide important cues to people around you.

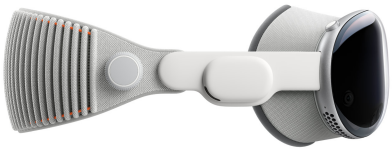
visionOS uses information from your Persona capture to create a personalized EyeSight on-device, which is used to show a digital representation of your own eyes on the outside of Apple Vision Pro. EyeSight also lets others nearby know if you're using apps or in an experience by showing a shimmer on top of your eyes. The enrollment information for your personalized EyeSight is stored on-device, and is not shared with Apple or anyone else.

Personalized EyeSight can be deleted at anytime in Settings > People Awareness > EyeSight > Delete EyeSight. If you delete personalized EyeSight, EyeSight will continue to match your skin tone, and will not have personalized eye color or face and eye shape.

Transparency for capture

EyeSight gently pulses with white light to let others around you know that you are capturing photos or video.

Apple Vision Pro enables you to capture memories using Apple's first three-dimensional camera, allowing you to transport yourself back into that moment in time with spatial photos and video combined with Spatial Audio. Additionally, Apple Vision Pro will capture your surroundings when you take a screenshot or screen recording that includes your physical space, or choose to share your view in FaceTime. Given Apple Vision Pro relies on ongoing usage of cameras to anchor content to your surroundings, we wanted to ensure that people in physical proximity understand when you are recording what's around you. When you capture photos or video including what's around you, EyeSight will show a pulsing white light to indicate that you are recording or using sharing your view in FaceTime. When you stop recording a spatial photo or video, the recording indication will stop. This indicator does not impact the quality of the content you are capturing.



In-store demo and purchase

Privacy underpins the entire Apple Vision Pro experience, and that includes the demo and fitting experience in your local Apple Store.

Getting a demo of Apple Vision Pro

When you come into an Apple Store for your demo of Apple Vision Pro, you will get fitted for a Light Seal and head band. An Apple Specialist will provide you with an iPhone with the Apple Vision Pro Fit App that you will use to scan your face. Any photos taken, or underlying representation of the geometry of your face, is immediately wiped from the iPhone upon completion and is only used to identify the correct Light Seal and head band size.

For those who choose to demo Apple Vision Pro in the retail store, the Specialist will take your glasses and utilize a lensometer to identify which demo optical inserts are needed. Then, the lensometer will output an encrypted QR code. As soon as the demo optical inserts are identified the data is purged from our systems.

Purchasing an Apple Vision Pro

When you purchase your ZEISS Optical Inserts for Apple Vision Pro, Apple does not see your glasses prescription values. At checkout, you will securely upload your prescription and it is shared with ZEISS. Your Optical Inserts are shipped directly to you from ZEISS. Your glasses prescription for your Optical Inserts cannot be accessed by Apple, or anyone else, as part of your purchase of Apple Vision Pro. Apple will store information about the Light Seal and head band size to facilitate future transactions, replacements, or returns.

Apple’s commitment to privacy

Privacy is more than a design principle, it is who we are. As you have seen, spatial computing is incredibly personal. Apple Vision Pro, powered by visionOS, features groundbreaking privacy protections to make it possible for you to have peace of mind while seamlessly interacting with digital content. From protecting where you look to storing Optic ID data on-device, Apple Vision Pro protects your information. As we continue to explore what’s possible with spatial computing, our work to bring privacy to life is not and never will be finished.