PARKS ASSOCIATES

Face Recognition and the Smart Home: Applications, Demand, and Innovation

IN PARTNERSHIP WITH: Xailient

Introduction

New, advanced tech is accelerating growth in the video device market, especially in access control for residential, SMBs, and commercial/enterprise businesses. Customer demand for features such as keyless entry, reduced false alarms, and smarter alerts such as package theft detection is driving manufacturers and OEMS to embed artificial intelligence (AI) and video analytics into products. Residential front door or entryway applications, including video doorbells, smart video door locks, and smart garage doors, are leading other sectors in smart camera adoption.

AI, including face recognition, can enhance the value propositions and be a key differentiator for smart home providers, but raises concerns over privacy and data security.

> 86% of consumers reported at least one AI feature† as important to their purchase decision, but 26% said that data concerns could be an impediment to their adoption.

Consumers are concerned not only about unauthorized access by hackers and bad actors, but many are concerned about how the product and service companies are storing and using their data.

Only 37% of consumers trust the companies that have access to their personal data.

This white paper addresses the role of face recognition technology for security and personalization, how AI and face recognition can enhance convenience and peace of mind for consumers, and how advanced tech solutions on the edge can reduce vulnerabilities and allay the privacy and security concerns surrounding these solutions within the connected home. Security and privacy concerns impact brand loyalty and trust, a critical factor for the growth of any product.

† AI features include ability to detect strangers and distinguish people from objects. Top scoring features listed on Page 5.

AI and Face Recognition Grows Across the Connected Home

Players across the connected home ecosystem are increasingly implementing AI in video devices. In security monitoring, AI helps users reduce notification fatigue by decreasing useless alerts, while also enabling a personalized experience.

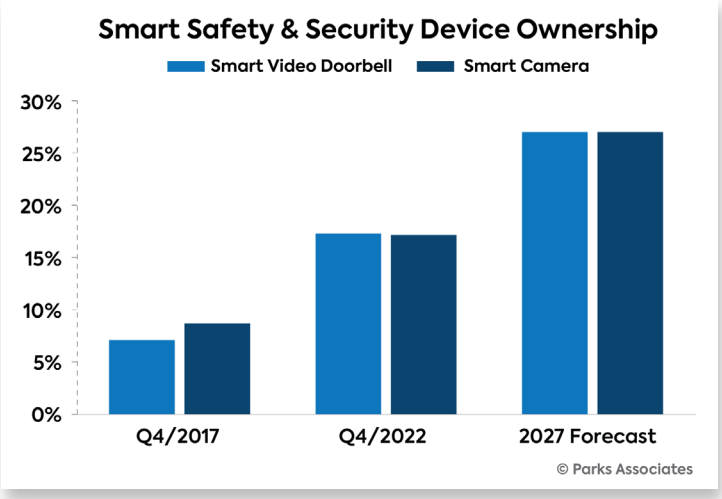
- Determining friend from foe: AI can determine who is on camera at the user's property and notify the user if a package is being delivered or stolen. AI can even predict a break-in.
- Assessing threats: smoke alarms with AI identify the actual cause of the smoke and assess the threat level.
- Granting access: smart door locks or smart video door locks can use AI by reading biometric data (face recognition, fingerprints, etc.) to allow temporary access to guests or delivery services.

Face recognition is a type of AI technology that is used to identify or verify a person from a digital image or a video frame. It works by analyzing and comparing patterns in a person's facial features, such as the distance between the eyes, nose, and mouth, to a database of known faces.

Security and Safety Devices in the Home

Consumers are embracing smart home devices – **41% of US internet households report owning at least one and 28% own three or more.**

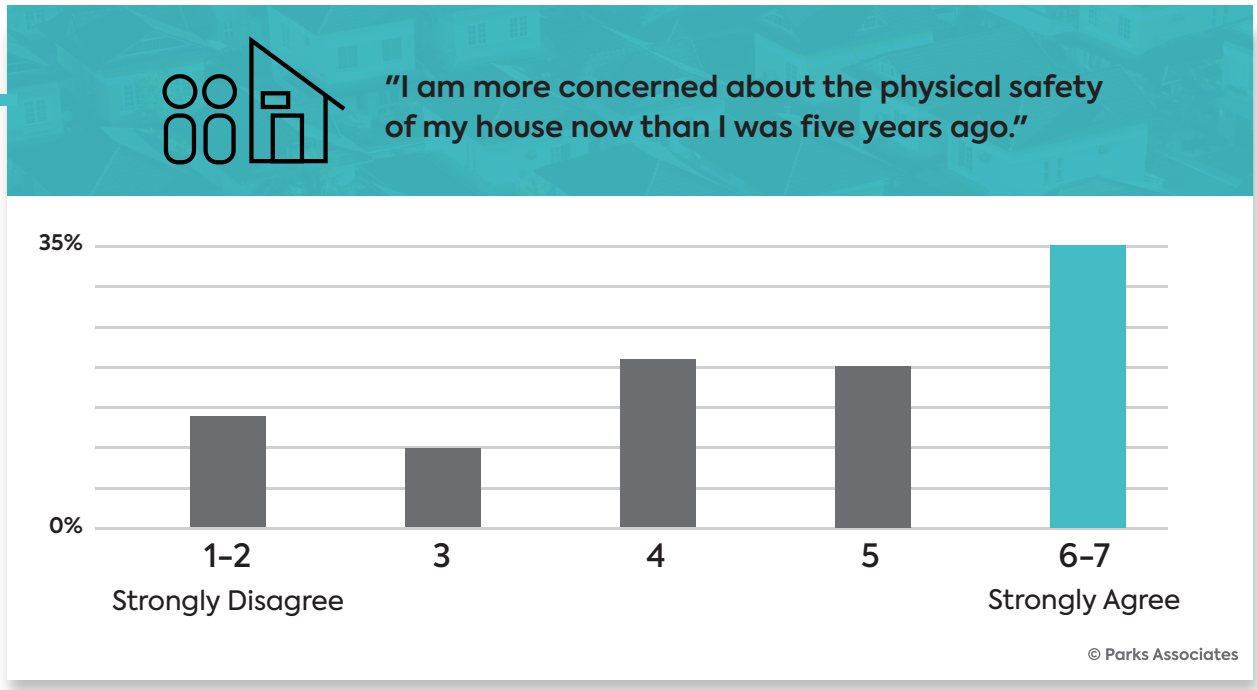
Currently, indoor/outdoor smart cameras and floodlights are a popular security solution for consumers. In US internet households, 17% own a video doorbell, and an equal percentage own a networked camera. Announcements this year point to device makers continuing to improve existing features while also expanding their solutions to serve SMB, multifamily housing, and commercial markets. Parks Associates forecasts ownership in video doorbells and smart cameras will grow to more than 25% of US internet households for each category by 2027.



Smart Video Devices: Top Drivers and Barriers

Consumers' anxieties and the desire to protect their homes and loved ones have driven strong growth of video devices in recent years.

- 57% video doorbell owners report safety and security as a factor for purchasing the device
- 54% of consumers in US internet households report their home is their most significant investment and put effort into protecting it
- 35% report having far more concern about the physical safety of their home than five years ago, up from 27% in Q2 2021
- 9% of consumers in US internet households have experienced a vehicle break-in
- 12% have experienced package theft



The top barriers to adoption for video devices are consumers' concern for their data privacy and security, the cost of video devices, and ease of use and installation. The IoT space is unfortunately vulnerable to data and device hacks. Consumers are aware of these issues and have concerns about connected devices.

- 62% of consumers feel it is impossible to keep data completely private
- 55% of consumers are very concerned about their personal data security
- 49% of consumer report experiencing at least one data/security privacy problem

> 26% of consumers are hesitant to adopt technology because of data security concerns

In addition to the obstacles of data privacy and security concerns, consumers are reevaluating their spending.

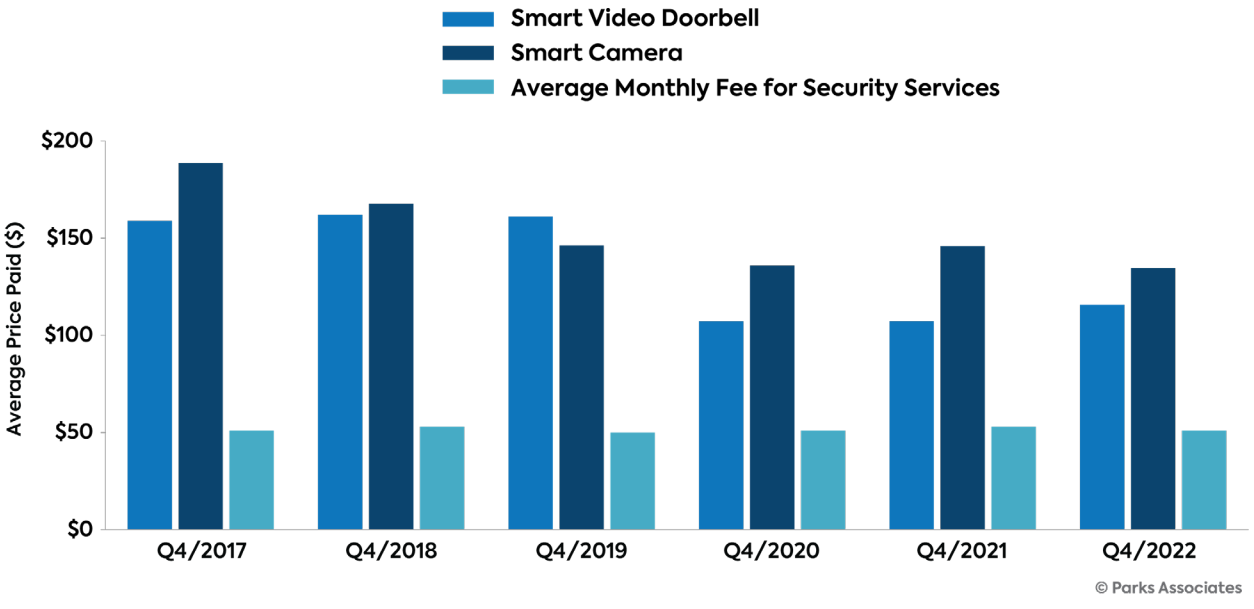
The ongoing supply chain issues and inflation have impacted companies, creating higher prices and increased material and labor costs.

Prices of video devices started to increase in Q4 2021 and were even higher in July 2022, not a typical trend of technology products, signaling macroeconomic trends are impacting manufacturers.

Consumers' Top Privacy Concerns

Identity theft	54%
Virus or spyware	41%
Hackers gaining device access	41%
Private information made public	39%
Companies selling personal data to other companies	33%
Data theft over the home network	28%
Companies tracking online activity for marketing purposes	27%
Data theft over public Wi-Fi	27%
Unwanted recording of voice, image, or activities by devices	22%

Average Consumer-Reported Selling Price: Smart Video Doorbell, Smart Camera, and Security Services

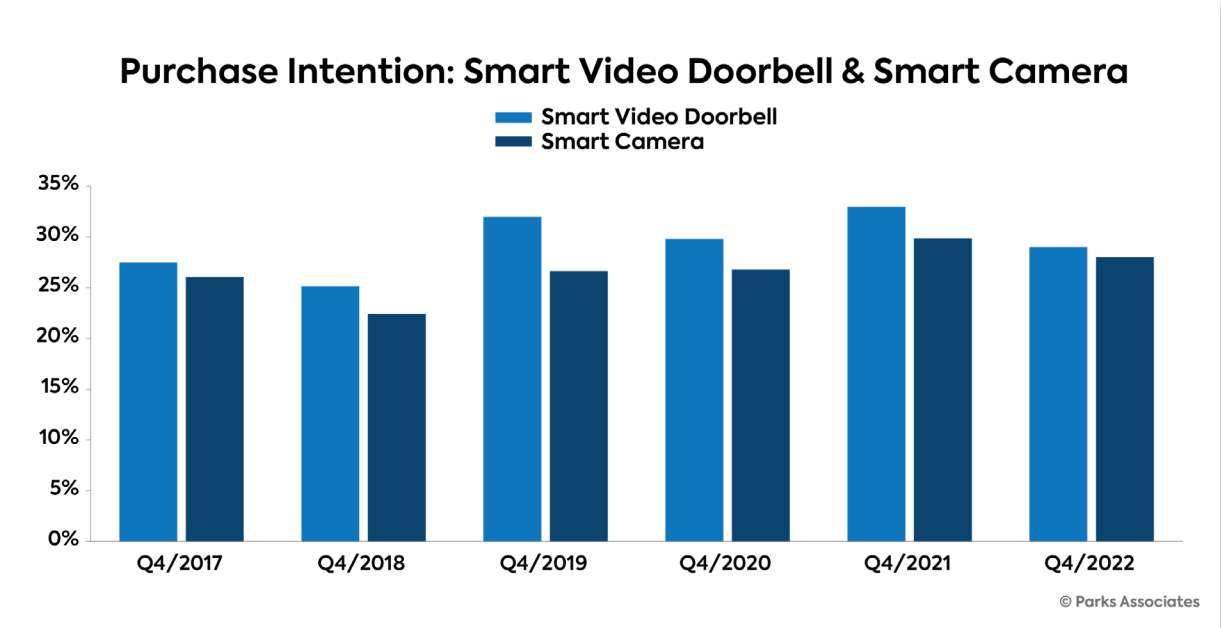


Purchase Intentions

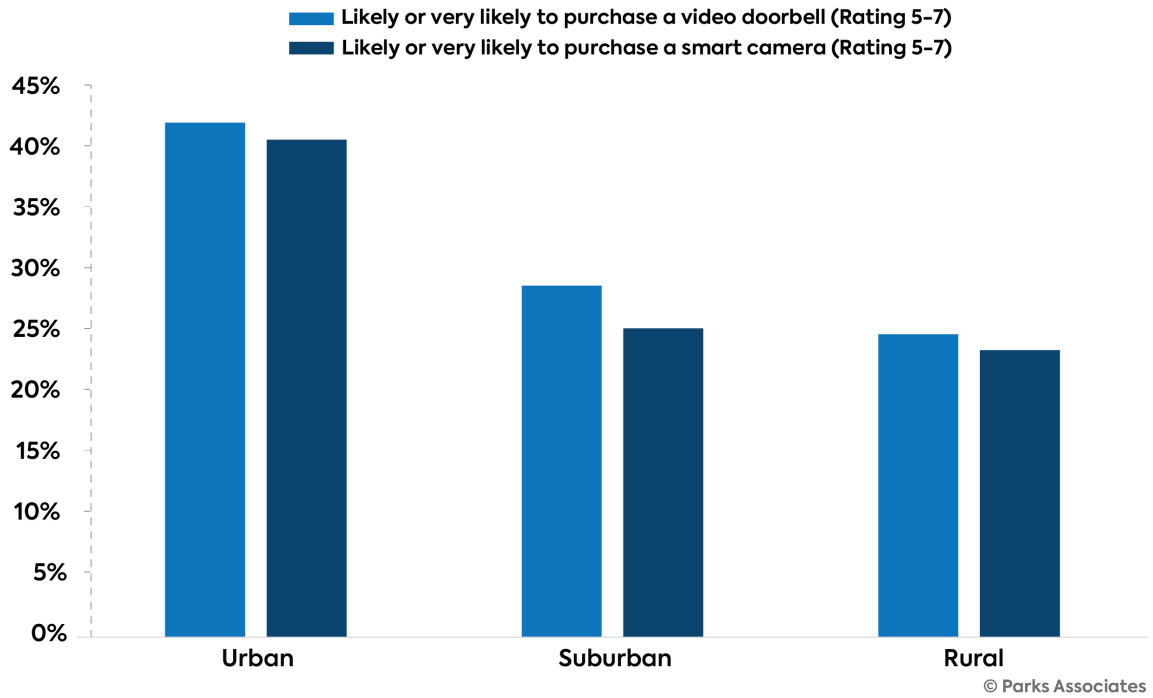
Around 30% of internet households report they are very likely to buy a video doorbell and/or smart camera within the next year. Their decision-making process includes consideration of advanced video features, such as ability to detect different objects and distinguish a known person from a stranger, making face recognition a key differentiator in the shopping experience.

Parks Associates research shows consumers have great interest in these applications and note a strong majority rate them as important features:

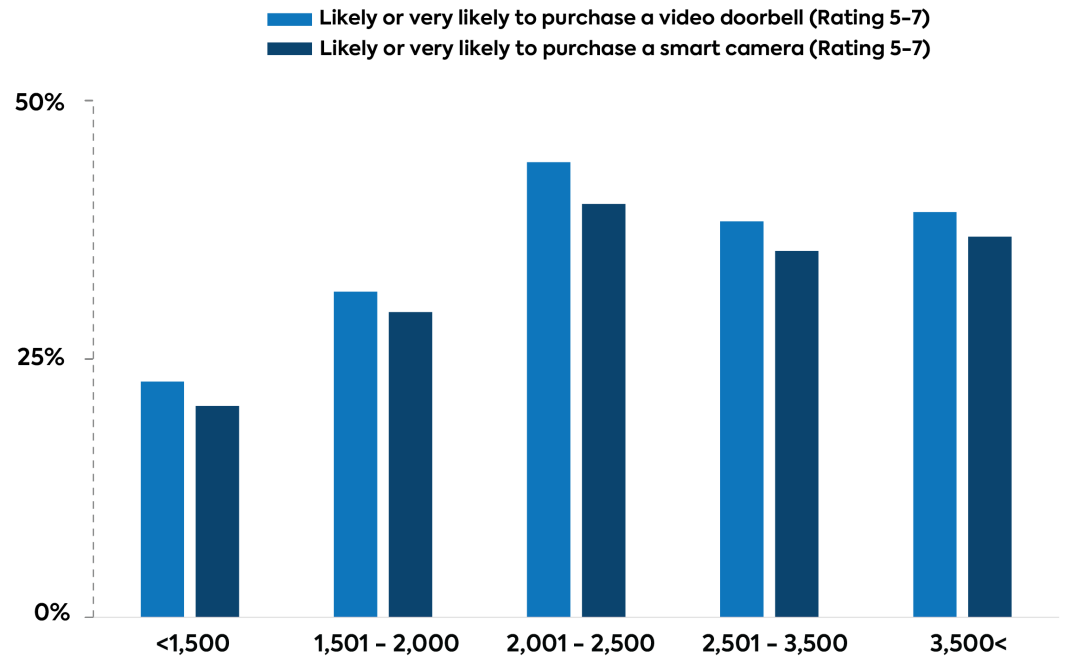
- Detection of a stranger near the home (86%)
- Distinguishing people from moving objects to reduce false alerts (84%)
- Identifying security and safety-related sounds (84%)
- Sending alerts when an object has been moved or removed from view (83%)
- The ability to identify types of objects, such as packages, plants, newspapers, etc. (78%)
- The ability to identify known persons from strangers (76%)



Purchase Intentions of Video Devices by Region



Purchase Intentions of Video Devices by Home's Square Footage



Regulations of Biometric Data: Impact on Industry

Over half of consumers are concerned about their personal data security, and over a quarter are reluctant to adopt technology based on data security concerns.

Consumers are justified in their concerns, as nearly half reported experiencing at least one data security or privacy problem. The implications of data security are even more critical when applied to biometric data (e.g., face recognition, fingerprints, and iris scans) because biometric data is unique and cannot be altered. Once biometric data has been compromised, it cannot simply be changed like a password, making the potential consequences much more significant.

Regulations play a crucial role in mitigating these risks and ensuring that individuals' biometric data is protected. Currently, there are no federal laws specifically governing the use of biometric technology in the United States, but multiple states and municipalities have enacted their own regulations for specific biometric technologies. For example, Texas and Illinois enacted biometric privacy laws that require companies to provide reasonable security measures to protect individuals' biometric data from unauthorized access or disclosure. They also require the company collecting biometric data to obtain informed consent from users. At the local level, municipalities such as San Francisco and Boston have enacted bans or restricted face recognition technology for government use.

In Illinois, several major lawsuits have occurred since the passing of its Biometric Information Privacy Act (BIPA), and with damages calculated at $1,000 for each violation (increasing to $5,000 if the violation is judged intentional or reckless), costs can increase quickly and exponentially. For example, a recent verdict penalized BNSF Railway Co. $228 million, while White Castle System could face a ruling of more than $17 billion in a lawsuit brought by a former employee alleging the company collected and disclosed her biometric data without consent. These potential losses have had a significant impact on the tech industry, setting a precedent for future BIPA cases and now the need to find solutions to not only receive consent from users when collecting biometric data but also how to prevent the data from being compromised.

In contrast, accusations of **Apple** violating BIPA were dismissed because customers voluntarily use the touch and face ID options to access their phones. Also, and just as important, their biometric data was stored locally on the device. As long as tech that is using the edge to process data complies with informed consent, data retention, and data destruction requirements, they are not in violation of biometric data laws such as BIPA.

In comparison, if the technology is processing and storing data on the cloud rather than the edge, the risk of being liable if the collected biometric data is compromised is greater because the data is stored centrally. This requires cloud providers to implement additional layers of security, increasing the complexity and cost of implementing a cloud computing solution. In addition, obtaining consent to collect biometric data through a cloud-based service is more challenging since it often involves third-party providers.

Overall, BIPA and other forms of regulation have the potential to impact the development and use of edge and cloud technology with biometric capabilities, as companies must ensure compliance with the law's requirements for biometric data collection, use, and storage. Currently, it is much simpler for edge technology to be compliant with biometric data laws versus cloud-based technology for a few reasons:

- Edge processes and stores data locally on the device itself, reducing the risk of unauthorized access
- Edge devices usually transmit data with encrypted protocols, reducing risks of data interception or tampering
- Jurisdictional issues can arise with cloud-based technology since the data is stored centrally. For example, biometric data collected from residents of different states must comply with the different laws of each state.

For these reasons, regulations may drive providers that manufacture technology that collects and stores biometric data to implement edge solutions.

Processing Power for Face Recognition

Video analytics applications employ AI to detect and identify persons, objects, animals, packages, license plates, and other subjects of interest visible in video camera feeds. Video analytics can also be fused with other contextual sensor data to validate the meaning and intent of the video subject, a critical issue in security use cases. Advances in enterprise video analytics are trickling down to consumer applications as chip, sensor, and cloud computing costs become more affordable.

Video processing can occur on an edge device or on-premises server, in the cloud, or a hybrid combination.

Available processing power in the edge device is a critical requirement for the level of data analytics complexity that can be delivered in real-time. For instance, intelligent motion detection is the simplest application of video analytics and requires far less processing power than face recognition. Intelligent motion detection reduces false alerts common to traditional passive infrared sensors (PIR) by filtering out everything (leaves, cars, animals, swaying bushes) other than what the user wants to know about (people or dogs). Some of these systems can also divide the visual field into zones with customized sensitivity settings.

As advancements have occurred, the pendulum of processing data at the edge or at the cloud has swung back and forth among smart home device makers. Both approaches have benefits and challenges associated with them, and some device makers are now taking a hybrid approach.

Edge vs. Cloud Computing Comparison

Processing	Edge	Cloud
Data	Private	Unlimited Storage
Analytics	Fast	Complex
Cost	One-time Upfront	Recurring
Reliability	Stable	Flexible

Edge Computing Strengths and Weaknesses

Strengths	Weaknesses
• Low latency gives a speed advantage • Enhanced privacy as data is kept local with less vulnerability to bad actors • Some essential functions can work without Wi-Fi • No recurring costs	• More expensive upfront for device OEM, but prices are decreasing over time • Expensive to upgrade • Limited storage capacity • Device failures = loss of data • Data security must be where the data is stored, so data in an edge device that is also a connected device would need high standards of security

Cloud computing and storage refer to a type of computing where computing processes, data storage, and applications are performed on a centralized server over the internet. A device collects data, sends it to the cloud, and receives analysis via an internet connection. This allows users to access and use computing resources without having to manage and maintain physical hardware. The cloud can perform large-scale analytics and the ability to fuse data from other cloud sources while incorporating AI and machine learning. This allows for flexibility and scalability that edge does not provide.

However, due to the centralization of the data on the cloud, transferring large data streams or data files from the edge network to the cloud at high speed is difficult. Providers typically send video to the cloud for analysis only when a secondary sensor detects some anomaly, such as motion. Providers may also limit the resolution (size of the image) and framerate (number of images per second or per minute) to fit within bandwidth and cost constraints.

Cloud Computing Strengths and Weaknesses

Strengths	Weaknesses
• Essentially unlimited storage capacity • Potential for dynamic analytics • Potentially less expensive devices • Data security can be managed by cloud-provider	• Loss of connectivity = loss of functionality • Latency • Recurring costs • Capacity for redundancy and backup • Privacy/security concerns (real or perceived) as data is moved to and from the cloud

Security vs. Flexibility

Edge computing and cloud computing both have their own unique security and flexibility features. In terms of privacy and security, edge computing offers stronger security because data is processed closer to the source and does not need to be transmitted to other device or to the cloud. This reduces the risk of data breaches and hacking. Additionally, edge computing devices can be physically secured and are less likely to be targeted by hackers compared to centralized cloud servers. However, security in edge computing also depends on the implementation and the devices used to deploy it.

There are instances where edge analytics is best, and other circumstances where large-scale cloud-based data analysis is better applied. For real-time data analysis with real-time applications, companies often employ a hybrid approach, where edge is utilized as an extension of the cloud. This can be done by separating computing of the data that needs to be analyzed quickly on the edge while supporting data (such as product information and software updates) is sent to the cloud. Data can be processed in progressive stages, allowing the edge AI to filter data before it is transmitted to the cloud, reducing the bandwidth and expense of pure-cloud solutions. In this way, a hybrid device can benefit from the edge's ability to process and analyze and the cloud's ability to maximize efficiency and functionality.

As a result of the efficiency edge AI provides for data processing, edge AI is being applied to a growing number of smart home and security devices as the cost to implement edge in products decreases. As AI features necessitate more resources – be it edge or cloud – product makers will be facing the challenge of educating consumers on why their approach matters, especially regarding processing speeds and privacy.

Face Recognition Capabilities and Use Cases

Advanced AI with face recognition can enhance the user experience of products in the home:

- Smart door locks
- Smart indoor and outdoor cameras
- Video doorbells
- Smart fridges
- Smart ovens
- Smart garage door openers
- Floodlights
- Assisted driving for vehicles

The more objects and faces the system is exposed to, the better it gets in recognizing the differentiating features that expedite accurate identification. Machine learning (ML) applied to time-series data—a form of data critical to understanding changes in user behavior and the state of a home over time—requires algorithms and database architectures different from those used in object identification. Time-series data can inform behavioral pattern recognition, detect behavioral and mechanical anomalies, and predict events based on IoT sensor data. The value of AI-powered video analytics in the consumer space is largely in providing a better user experience with more intelligent alerts.

Personalizing the Home Security Services

Smart home security systems equipped with face recognition technology can seamlessly arm and disarm when a household member arrives or leaves a property and can alert a household member when an unauthorized individual is present on the property. This system can also identify familiar or friendly faces and let the user know if someone they know is on the property or at the door. The system can also ignore known people in the home so that owners are not inundated with useless alerts when family members come and go. All family members can have a better, more convenient experience with the system as well, as face recognition software allows for easier access control by unlocking doors or opening garages when detecting approved faces.

The benefits of face recognition extend to security providers. Face recognition creates operational savings for monitoring stations by reducing the time to validate the security event and provides verification data to first responders to reduce response times and fines for false alerts. Face recognition technology will expand beyond home security and will also cater to user convenience and comfort in other verticals.

Additional Personalization Functions

Face recognition technology can customize a user's experience with smart home devices by identifying the user and automatically adjusting settings based on that person's preferences helping make the home more safe and secure:

- Adjusting the temperature or lighting to a specific user when they enter the room
- Auto-unlock doors as users approach
- Seamlessly set a detected user's preferred audio and visual entertainment settings
- Auto-login into their profiles on streaming accounts
- Remind specific users of calendar events
- Identify and allow access to authorized individuals while denying access to others
- Identify familiar guests from strangers on a user's property
- Monitor the safety and well-being of home members, such as older adults, children, or disabled individuals, by detecting falls or other accidents and alerting caregivers or emergency services

Outlook

Face recognition technology will be pervasive in video devices in the years to come.

If face recognition features follow the same path as prior video analytics innovations, these solutions will be in most new video devices by 2025.

Consumers, business, and law enforcement will rely on this advanced technology to understand the environment for protection and safety. New use cases are emerging in the financial, security, human resources, law enforcement, healthcare, robotics, and advertising sectors. In the future, the technology will be used to validate financial transactions, prevent trespassing, time-track employees, identify suspects in a crime, help detect symptoms of certain diseases, and provide more targeted ads to consumers.

> By 2025, video doorbells and smart cameras will sell a combined 27.6 million units in the United States, with a 8% and 10% CAGR, respectively.

Like video storage, face recognition technology can be provided as a subscription service, where a customer pays a recurring fee to access the technology on an ongoing basis. This can be beneficial for businesses that only need to use the technology occasionally, as they can avoid the upfront cost of licensing the software. With a licensing model, the customer would pay a one-time fee to use the software and would own it outright. This can be cost effective for businesses that need to use the technology frequently.

In the security and smart home space, consumers will value face recognition technology for the peace of mind and convenience it can deliver, provided their privacy and personal data are secured. As with many emerging technologies, face recognition technology brings privacy and security concerns that the industry needs to address, but these challenges can be overcome. Companies can take the necessary steps to ensure user data is respected and protected while delivering the full value of these solutions to consumers.

Ultimately, the ability of face recognition to meet growing market demand will depend on the capacity of technology to satisfy the privacy and security requirements of regulatory bodies.

About Parks Associates

www.parksassociates.com
info@parksassociates.com
972.490.1113

Parks Associates, a woman-founded and certified business, is an internationally recognized market research and consulting company specializing in emerging consumer technology products and services. Founded in 1986, Parks Associates creates research capital for companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, workshops, executive conferences, and annual service subscriptions.

The company's expertise includes new media, digital entertainment and gaming, home networks, internet and television services, digital health, mobile applications and services, consumer apps, advanced advertising, consumer electronics, energy management, and home control systems and security.

About Xailient

Xailient's computer vision AI for Edge devices enables innovators to bring their visions to life.

Our software solutions allow companies to deploy Face Recognition and detection features for continuous monitoring and updating while always ensuring privacy-safe data collection.

Xailient's software products run on exceptionally low power and make embedded Edge Computer Vision accurate, real-time, and cost-effective, solving the most difficult problems in the Enterprise CV lifecycle.

About the Author

Chris White, Research Director, **Parks Associates**

Chris is a research director with Parks Associates, covering the smart home and smart energy markets. He was previously a Director of Insights at PeopleMetrics in Philadelphia and the Data Manager of a youth-serving collaborative in New Orleans. He leverages this background in marketing research and data gathering to contribute to the design of Parks Associates consumer surveys.

Chris earned his BBA in Marketing from the College of William & Mary and his MBA in Marketing and Finance from American University.

Jennifer Kent, Vice President, Research, **Parks Associates**

Jennifer manages the research department and Parks Associates' process for producing high-quality, relevant, and meaningful research. Jennifer also leads and advises on syndicated and custom research projects across all connected consumer verticals and guides questionnaire development for Parks Associates' extensive consumer analytics survey program. Jennifer is a certified focus group moderator, with training from the Burke Institute.

Jennifer earned her PhD in religion, politics, and society and an MA in church-state studies from Baylor University. She earned her BA in politics from the Catholic University of America in Washington, DC.

PARKS ASSOCIATES
International Research Firm

RESEARCH & ANALYSIS

for Emerging Consumer Technologies

With over 35 years of experience, Parks Associates is committed to helping our clients with reliable and insightful consumer and industry research.

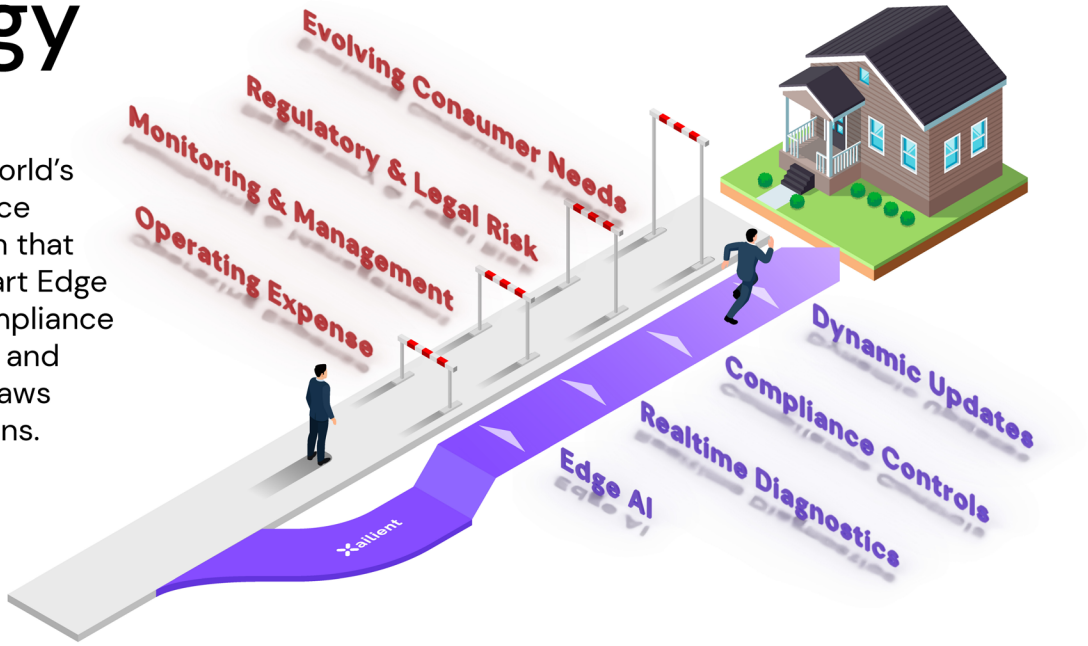
- Smart Home Devices and Platforms
- Digital Media and Platforms
- Home Networks
- Digital Health
- Support Services
- Entertainment & Video Services
- Consumer Electronics
- Energy Management
- Home Control Systems
- Home Security

www.parksassociates.com

Xailient

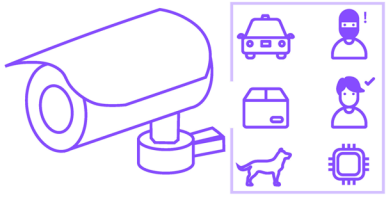
Accelerate your Smart Camera Strategy

Orchestrait is the world's first privacy safe Face Recognition solution that uses state-of-the-art Edge AI to ensure full compliance with biometric data and privacy protection laws across all jurisdictions.



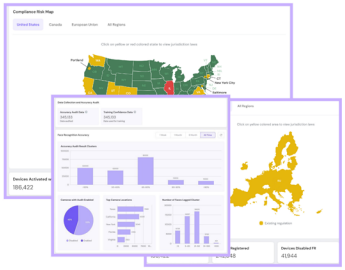
Learn how Xailient helps you simplify compliance with BIPA, CCPA, GDPR and other privacy regulations at xailient.com/parks

Cost Savings



Realtime Monitoring

Regulatory Compliance



Available now on all market leading camera chipsets for the smart home

君正 Ingenic · REALTEK · SigmaStar · SONY · ANALOG DEVICES · intel · arm

See What Matters
xailient.com