



Position paper, October 2025

Privacy in the smart home

Personal privacy in the smart home requires data autonomy. This means smart home data should be local first, user owned and controlled, and legally protected. In addition, the privacy implications of any smart home device or service should be easily understood thanks to simple labeling.

Introduction

Privacy in the smart home is a topic of great importance. But it exists in a regulatory desert. While landmark legislation, such as the EU General Data Protection Regulation (GDPR) of 2018, has strengthened rights at the intersection of privacy and personal data online, legislation explicitly protecting the privacy and data autonomy of people who live in smart homes is still largely missing. As the leading non-profit foundation fighting for privacy, choice, and sustainability for smart homes and every person who lives in one, the Open Home Foundation calls for smart home data that is local first, user owned and controlled, and legally protected. We also call for the creation of a labeling system to help consumers easily understand the privacy implications of smart home devices and services at the point of purchase.

Central concepts

Privacy is a human right.

The right to privacy grants each of us the agency to decide what information we share about ourselves, and with whom we share it. Privacy is therefore central to our identities as human beings. After all, generous control of one's privacy—to the extent that it is balanced with and does not unjustly infringe on the rights of others—helps ensure we each have the opportunity to express ourselves, understand and interact with the world on our own terms, and thrive as free individuals.

The flipside is that gratuitous, involuntary loss of privacy constrains individual expression and can lead to widespread suppression or self-limitation of personal freedoms. Nobody should have to modify their behavior because of an algorithm. After all, you might think twice about the brands you purchase, or programs you watch, when such behaviors are used to categorize you as uninsurable, restrict your ability to travel, or mark you as undesirable to your employer

or society. In the worst case, losing control over your privacy can lead to physical and mental harms—and in some situations even death.

Privacy in the smart home poses its own challenges related to mountains of personal data.

The devices in and around your home—from smart light bulbs, speakers, and washing machines, to presence and air quality sensors, to vehicles and energy systems and beyond—gather vast quantities of personal data. This information is of tremendous value. And poses new and tremendous risks.

Unique to this context, a smart home system combines data from broadly different areas of life that might otherwise be kept apart.

This, along with the advent of functional AI, means powerful insights can be drawn from smart home data in a way never before imaginable.

It is therefore reasonable to maintain complete control over access to such insights even when they are accurate. But what about when they are based on biased training data—or are simply incorrect? What about when there are no real mechanisms in place to investigate false conclusions or reverse their consequences? Then the risks are even greater.

Smart home privacy requires data autonomy.

Privacy based on data autonomy means having control over your own personal data. You decide what to share on your own terms. You choose whether to analyze personal data on your own hardware and software at home, or grant access to a third party to analyze it for you. Or store it for future use. Or revoke access and delete it forever.

Achieving data autonomy greatly strengthens—but does not ensure—your ability to maintain privacy while still benefiting from the wealth of personal data produced in a smart home. It likewise hands you the keys to share nothing at all.

Recommendations

With exceptions for legal restrictions and where it infringes on the rights of others, the Open Home Foundation holds the following positions:

Smart home data should default to a user-controlled, local-first approach.

The data produced by a smart home should depend on solutions, storage, and processing within the smart home itself wherever feasible. Functionality that requires data to leave the home, for instance to transit the cloud, is acceptable when it offers convenience, security, or is not yet feasible locally—but must be opt-in. We consider the following requirements central to a user-controlled, local-first approach:

- **Fully functional, user-accessible, local APIs:** An API, or application programming interface, is a technical solution that allows computers, devices, and services to communicate between one another. Being local means communication takes place entirely within your smart home, on hardware you own, rather than being sent over the internet. An example would be turning on your lights, or changing the volume on your smart speaker, without needing to route control signals or data outside your home's local area network via a company's servers. Being user accessible means local APIs are open for a user to interact with and control via third-party software (including the user's own), and largely documented. It is important that such local APIs allow for a device's or service's full functionality wherever feasible.
- **Local data storage, retrieval, backup, deletion, and processing:** The data produced by a smart home should be stored and processed, as well as retrievable and able to be deleted, without transiting the internet or external systems wherever possible. For instance, if your smart home has a digital shopping list, its data, including its history, should be stored entirely within your home. You should be able to easily access this data for any purpose, whether to analyze your buying habits, share your history with a friend or third party, or to delete the record (or any part of it) permanently.
- **Cloud-optional:** Any functionality that requires data or control signals to leave your home must be transparently explained, opt-in by default via a simple workflow, and

revocable at any time on a feature-by-feature basis. An example is a smart light with a fully functional, user-accessible, local API, and local data storage and processing. The light's vendor might want to let users securely control that light while away from home via the vendor's own mobile app—requiring data and signals to transit the cloud. To enable this functionality, the vendor's app must clearly explain what data is needed and why, ask permission from the user before this functionality can be turned on, and provide an easy way to toggle this cloud-based functionality as desired without limiting other features.

If a person or household purchases or pays for a system, device, or service, that person or household should own and control all the data it generates in their smart home. Vendors shouldn't arbitrarily withhold functionality in exchange for data access, nor charge users to access their own data.

Smart home data ownership and control must reside with the people who purchase or pay for the devices, services, or systems that produce the data, or who live in homes where the data is generated. We consider the following requirements critical to user ownership and control of smart home data:

- **Data ownership:** Data produced by devices, services, and systems within your smart home should belong and be fully accessible to you.
- **Transparency:** It should be clear to the user what data or control signals are shared with a third party, or leave their smart home's local area network, and why. This information should be documented online, appear in printed materials, or be easily accessible via vendor apps.
- **Access control:** The person or household that purchases or pays for a smart home device, service, or system must have fully granular control over the sharing, revocation of access to, deletion, and licensing of data produced by it. This is particularly important for granting temporary access to data for troubleshooting purposes.
- **Withholding of functionality:** Vendors cannot arbitrarily withhold functionality in exchange for data access.

Data generated by smart homes should be legally regulated and protected.

It's not enough to call for privacy best practices. Some aspects of privacy in the smart home must be legally regulated and protected. We consider legal requirements particularly important for the following subjects:

- **Data ownership:** Data ownership is too important to be left up to vendors and end-user agreements. Data ownership residing with the person who purchases a smart home device, service, or system, or who lives in a smart home that produces data, must be a legal requirement.
- **Data location:** Data and control signals must remain within a smart home's local area network by default ("local by default"). Therefore, sharing data with third parties must be turned off by default. Changing these defaults must require granular, opt-in agreement accompanied by clear explanations about what data is shared, for what purposes, with whom, and for how long.
- **Data deletion:** Whether data is shared with a third party or stored locally, users must be provided with a simple, non-technical method to permanently delete personal data in a timely manner.
- **Side-channel access:** An overlooked area that requires legal scrutiny is side-channel access of data between devices, services, and systems on home networks. There are dozens of technologies involved, such as UPnP and mDNS, that are currently unregulated. For instance, while a user may have declined internet access to a baby video monitor, a third-party device on the network may be able to discover the monitor or access sensors, media streams, saved files, or metadata, circumventing the first-party app's permissions. While side-channel access requires legal attention, it is important that regulations are not used to justify the arbitrary locking-down of a device or local data access, for instance via a cloud-authorization requirement.
- **Transfer to third parties:** Any data sharing with third parties must be disclosed and transparently described to the user, including disclosure of data the third party shares with other parties. Sharing that is revoked, or data that is requested to be deleted, must occur along the entire chain of transmission—with each third party at risk of financial penalties if it cannot reasonably show it has deleted data it stores, as well as forwarded revocation and deletion requests to entities with whom it has shared data.
- **Data security and encryption:** Personal data must be secured. This includes end-to-end encryption when personal data is transmitted beyond a smart home's local area

network, and encryption-by-default when personal data is stored outside a smart home. In addition, cloud-based storage must adhere to data minimization principles.

The privacy implications of any smart home device or service should be easily understood at the point of purchase due to simple labeling.*

An easy-to-understand, consistent, and visually accessible labeling system is needed so that consumers can comprehend the basic privacy implications of smart home devices and services when shopping online or in person. Because additional research, design, and debate on such a system is required in order to ensure it is both accurate and usable, we call for the following:

- The system should provide a visually accessible label (with colors or numbers as adjuncts) so consumers who have done no previous research can easily determine if what they are about to purchase is consistent with their personal privacy preferences. This will likely include coverage of local vs. cloud functionality, data storage and security, and requirements regarding the creation of third-party accounts, among other topics.
- Such a system will have an online component, searchable via QR code or similar, so consumers can quickly check for additional details and up-to-date information (for instance, changes due to firmware updates).
- Those working to design such a system should consider both what has and has not worked with similar systems, such as the EU Nutri-score or Energy Label, or various nutrition information requirements that appear on food items and meals in different legal jurisdictions.
- When designing or updating such a system, research related to efficacy should take precedence over speculation. A “good” idea that results in worse outcomes than the current status quo should be rejected.
- Vendors, regulators, and other organizations should aim to adopt the labeling system that best balances widespread use with high efficacy. The only thing worse than no labeling system, or a single bad one, is so many labeling systems that consumers lose trust in the concept altogether.

*The Open Home Foundation is exploring the development of its own labeling system.

Conclusion

Personal privacy in the smart home is an important topic that impacts us all at a fundamental level—and must be addressed by a broad range of stakeholders. It is also one of the Open Home Foundation’s central principles.

To that end, this paper represents our current positions related to privacy in the smart home, while acknowledging the evolving nature of technology and society, and the dynamic and diverse experiences of people who live in smart homes.

We call on all relevant stakeholders to take action. And above all, we call on legislators to move forward drafting regulatory frameworks and laws to enshrine the right to personal privacy in the smart home. The Open Home Foundation stands ready to join you to ensure that smart home data is local first, user owned and controlled, and legally protected.



About the Open Home Foundation

The Open Home Foundation fights for the fundamental principles of privacy, choice, and sustainability for smart homes. And for every person who lives in one. It does this by supporting the development of open source projects, and open connectivity and communication standards. These projects include Home Assistant, ESPHome, and Music Assistant, which are used by millions of households around the world.