ASHB

Association for Smarter Homes & Buildings

The Smart Home Data Compact

Navigating Privacy, Consumer Trust, and Value Creation

Exploring data privacy, evolving standards, and innovative business models in connected homes

Connect to what's next™

www.ashb.com

About Harbor Research

Firm History
Harbor Research was the first firm to focus on Smart Systems, Services and the Internet of Things (IoT) and first to publish groundbreaking research on new business models in the Harvard Business Review in 2004 & 2005.

Clients and Engagements
For over 30 years we have focused on identifying, analyzing and helping clients to develop or adopt emergent technologies. Every relationship we develop is enhanced by the range and depth of these experiences.

Technology Developers & Suppliers

100+ clients   **400+** engagements

OEMs and Service Providers

150+ clients   **600+** engagements

Offices
Denver, Colorado - USA   Berlin, Germany - Europe

Overview of Harbor's Services
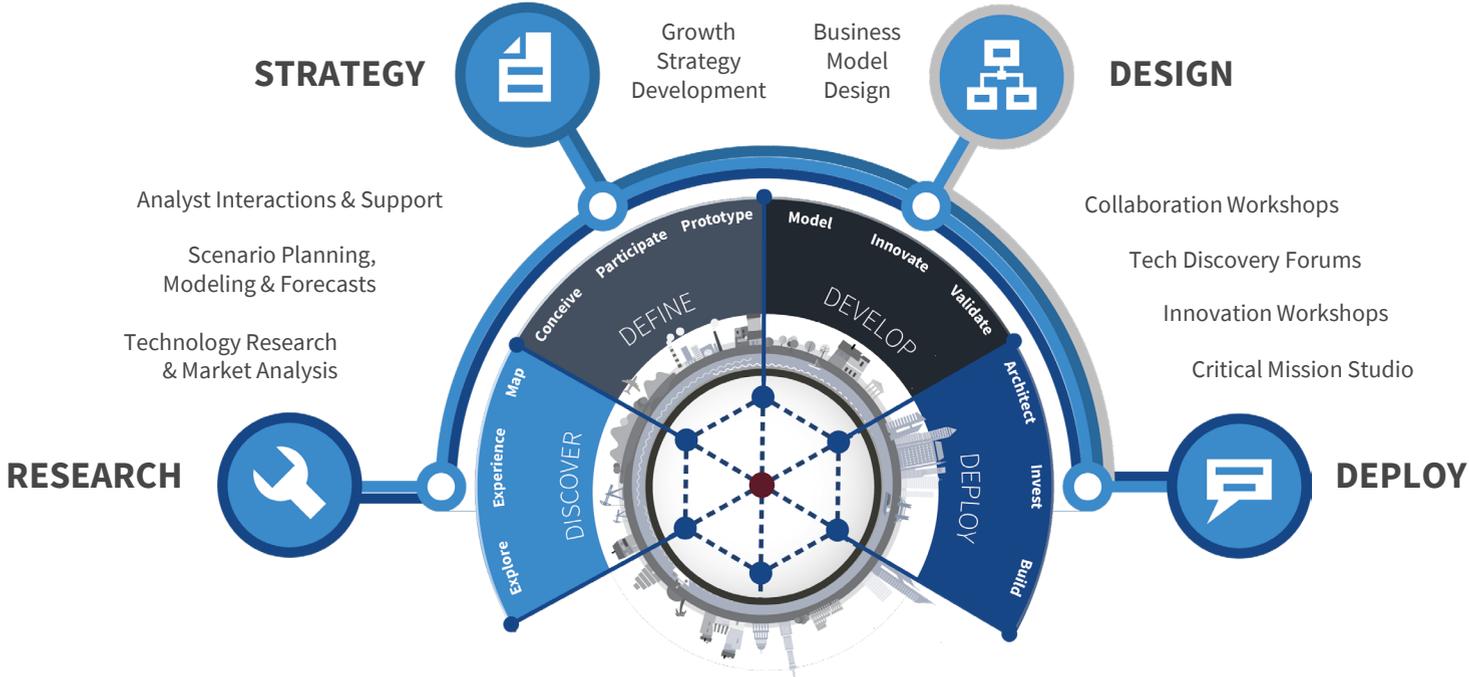
Opportunity Identification
Research, market intelligence and Smart Systems market sizing and forecast model to ID tech-driven growth opportunities

Growth Strategy Development
Business model development & growth strategy consulting services

Venture Advisory
Venture development studio and advisory for mission-critical industries and tech

We work and facilitate strategy across corporate functions

Corporate Development   Business Development   Market Intelligence   Strategic Marketing   New Growth   Research & Development

Introduction & Session Goals

Understanding the Smart Home Data Compact to Drive Privacy, Trust, and Innovation

Definition of the Smart Home Data Compact

- Framework for stakeholder collaboration
- Focus on privacy, trust, and data value
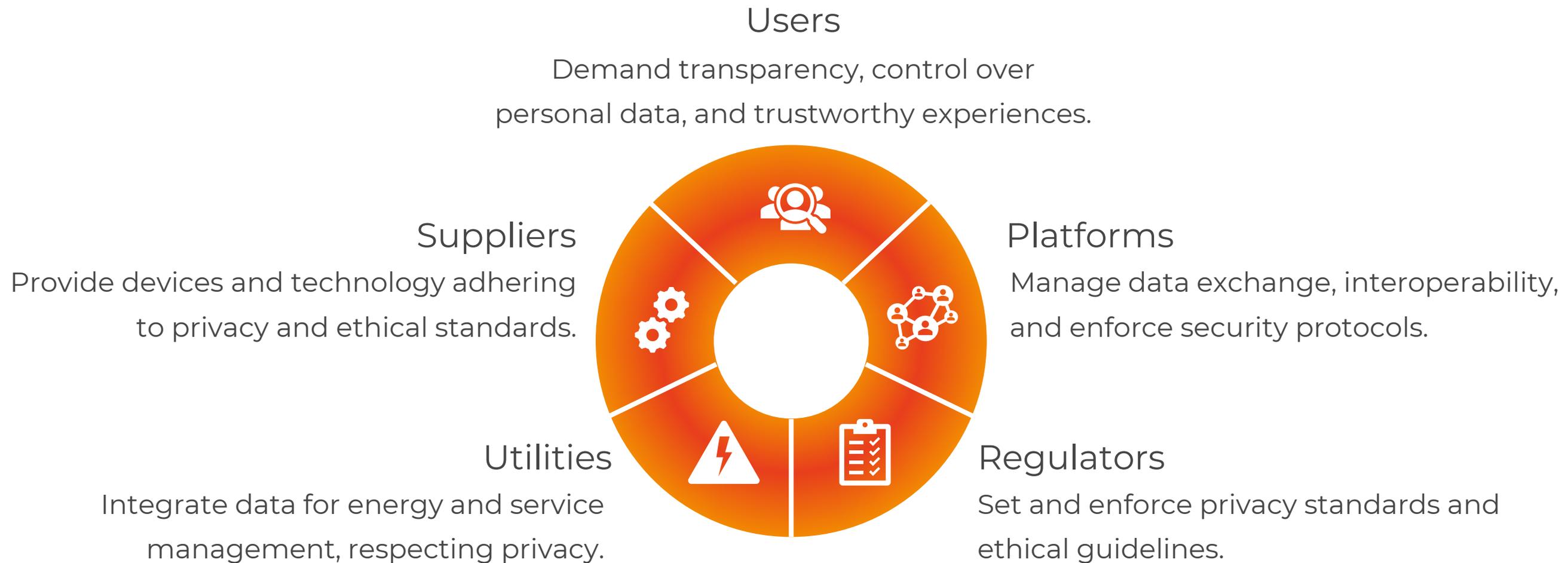- Shared principles for responsible data governance

Session Goals

- Align industry on privacy principles
- Identify insights to build consumer trust
- Balance privacy and innovation in business models
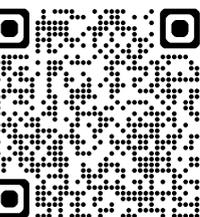- Develop solutions for better consumer experiences
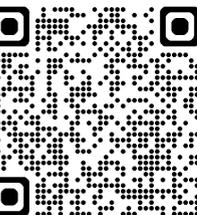
Aligning Stakeholders for Smart Home Data Governance

Establishing a unified compact to ensure privacy, trust, and innovation

Users
Demand transparency, control over personal data, and trustworthy experiences.

Suppliers
Provide devices and technology adhering to privacy and ethical standards.

Platforms
Manage data exchange, interoperability, and enforce security protocols.

Utilities
Integrate data for energy and service management, respecting privacy.

Regulators
Set and enforce privacy standards and ethical guidelines.

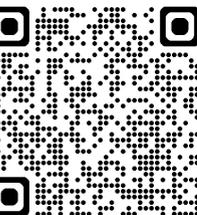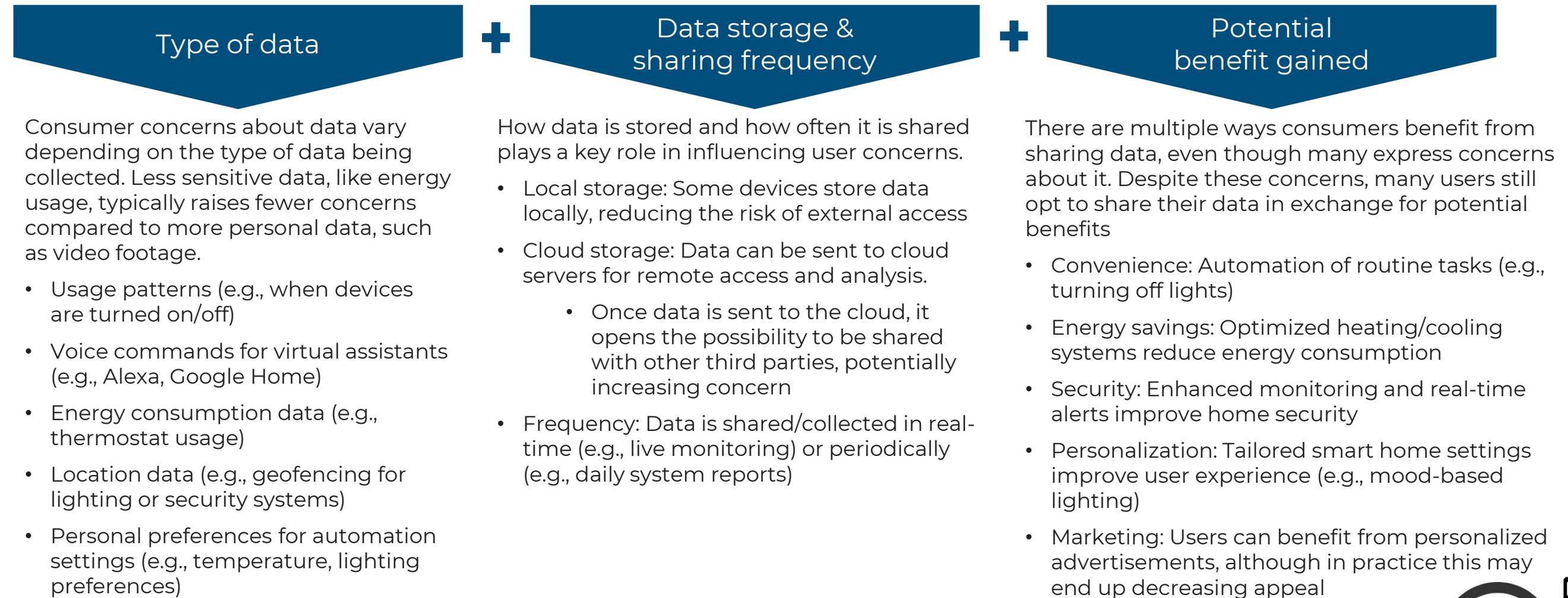*Collaborative frameworks balance innovation with consumer protection and trust building. Visualizing roles clarifies responsibilities and promotes unified ecosystem solutions.*

Consumers Behave Under a Privacy Paradox- Despite Voicing Concerns, Many Still Share Data

Although consumers generally report data privacy concerns, their behaviors tend to follow a more complicated cost-benefit analysis based on the above factors

Data Sharing Considerations

| Type of data | + | Data storage & sharing frequency | + | Potential benefit gained |

Type of data

Consumer concerns about data vary depending on the type of data being collected. Less sensitive data, like energy usage, typically raises fewer concerns compared to more personal data, such as video footage.

- Usage patterns (e.g., when devices are turned on/off)
- Voice commands for virtual assistants (e.g., Alexa, Google Home)
- Energy consumption data (e.g., thermostat usage)
- Location data (e.g., geofencing for lighting or security systems)
- Personal preferences for automation settings (e.g., temperature, lighting preferences)

Data storage & sharing frequency

How data is stored and how often it is shared plays a key role in influencing user concerns.

- Local storage: Some devices store data locally, reducing the risk of external access
- Cloud storage: Data can be sent to cloud servers for remote access and analysis.
  - Once data is sent to the cloud, it opens the possibility to be shared with other third parties, potentially increasing concern
- Frequency: Data is shared/collected in real-time (e.g., live monitoring) or periodically (e.g., daily system reports)

Potential benefit gained

There are multiple ways consumers benefit from sharing data, even though many express concerns about it. Despite these concerns, many users still opt to share their data in exchange for potential benefits

- Convenience: Automation of routine tasks (e.g., turning off lights)
- Energy savings: Optimized heating/cooling systems reduce energy consumption
- Security: Enhanced monitoring and real-time alerts improve home security
- Personalization: Tailored smart home settings improve user experience (e.g., mood-based lighting)
- Marketing: Users can benefit from personalized advertisements, although in practice this may end up decreasing appeal

Consumer Trust Varies by Data and Company Type

Utilities, telecom, and security companies are uniquely positioned to build data applications, with smart device companies enjoying a relatively advantageous position
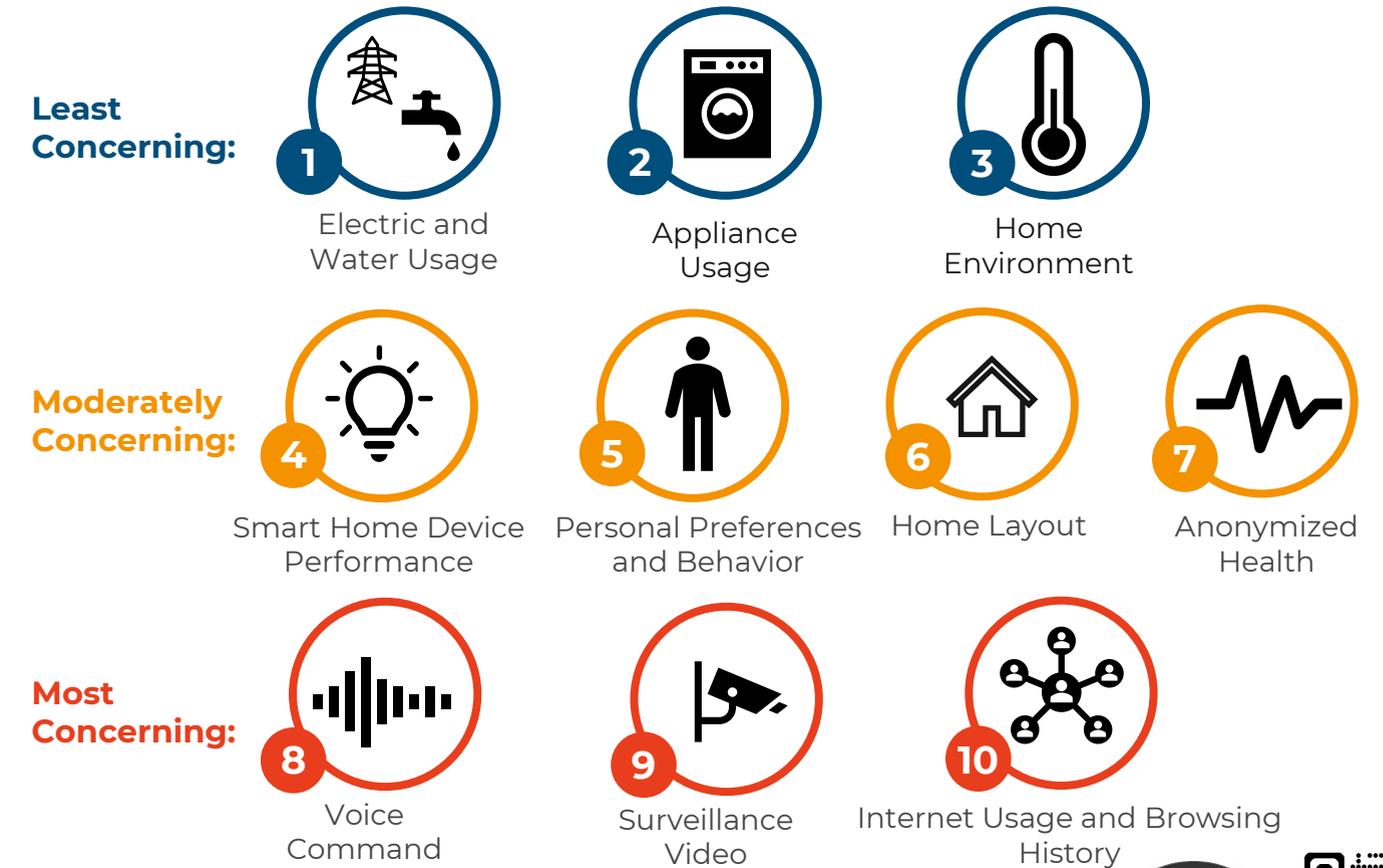
Most Trusted Company Types

How comfortable are you with sharing personal data with different technology companies if it means improved performance and increased control over your smart home devices? (n=760)

Most Trusted:
1. Electric and Water Utilities
2. Telecom
3. Security Solution

Moderately Trusted:
4. Smart Device Suppliers
5. HVAC/Air Quality Equipment Vendors
6. Contractor, Electrician, Plumber, or Similar Service

Least Trusted:
7. Property Mgmt.
8. Cloud Services
9. Social Media & Streaming

Least Concerning Data Types

How comfortable would you be with sharing the following types of data? (n=760)

Least Concerning:
1. Electric and Water Usage
2. Appliance Usage
3. Home Environment

Moderately Concerning:
4. Smart Home Device Performance
5. Personal Preferences and Behavior
6. Home Layout
7. Anonymized Health

Most Concerning:
8. Voice Command
9. Surveillance Video
10. Internet Usage and Browsing History

Smart Home Data Sharing Use Cases

Smart homes currently have many potential applications that leverage data, but even the more innocuous seeming ones can leverage "sensitive" data

Integrated Light Control
Saves energy and adds convenience by automating lighting based on presence and schedules. It may use occupancy data, user preferences, and natural light levels to adjust lights accordingly.

- 1 — Electric and Water Usage
- 3 — Home Environment
- 4 — Smart Home Device Performance
- 5 — Personal Preferences and Behavior
- 6 — Home Layout
- 8 — Voice Command

PV / Solar Excess Optimizer
Optimizes solar energy use, reducing electricity costs and potentially selling excess energy. It may use solar production, energy use, and battery levels to decide when to store or feed energy back to the grid.

- 1 — Electric and Water Usage
- 5 — Personal Preferences and Behavior
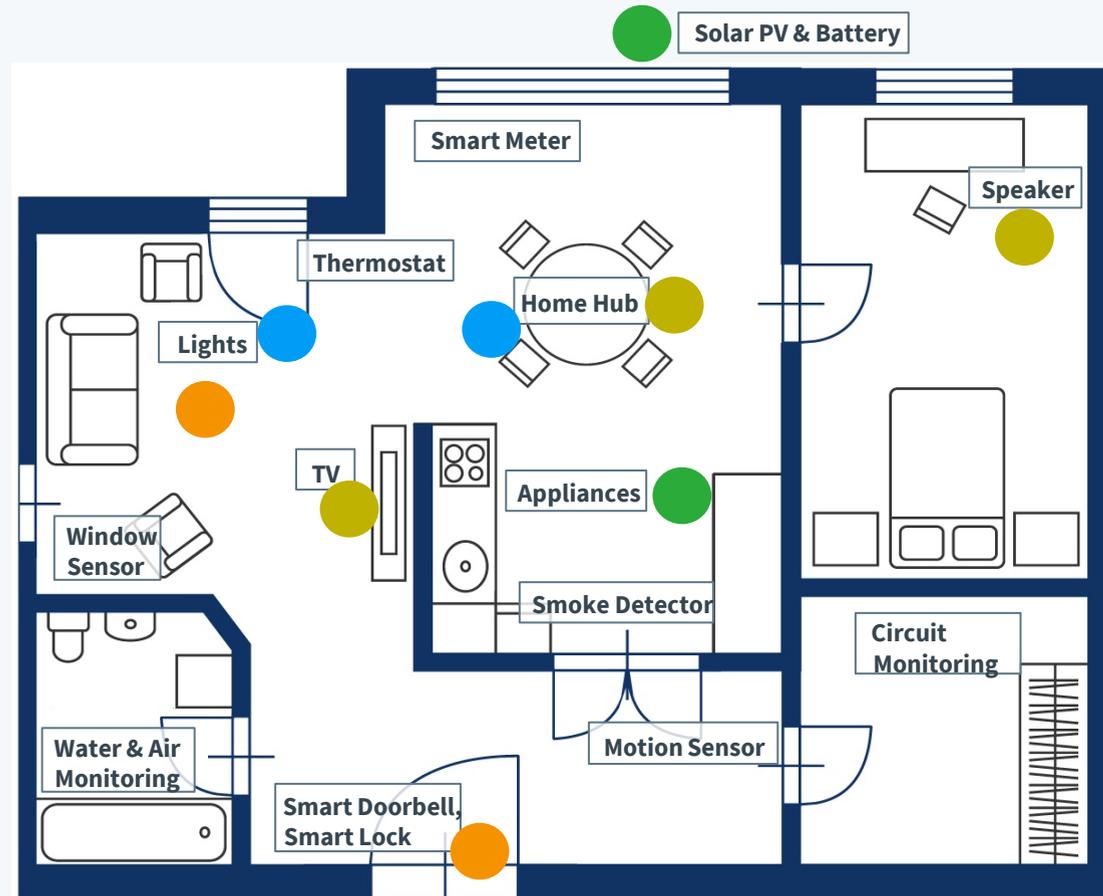
Smart Lock Integration
Enhances security by controlling and monitoring home access. It may use entry logs, user authentication, and access schedules to manage who enters and exits, integrating with cameras for extra security.

- 5 — Personal Preferences and Behavior
- 6 — Home Layout
- 8 — Voice Command
- 9 — Surveillance Video

Entertainment
Enhances user experience with personalized content and voice control. It may use data on viewing habits, preferences, and voice commands to tailor media suggestions and integrate with other smart devices.

- 5 — Personal Preferences and Behavior
- 8 — Voice Command
- 10 — Internet Usage and Browsing History

Floor plan labels
- Solar PV & Battery
- Smart Meter
- Speaker
- Thermostat
- Home Hub
- Lights
- TV
- Appliances
- Window Sensor
- Smoke Detector
- Circuit Monitoring
- Water & Air Monitoring
- Motion Sensor
- Smart Doorbell, Smart Lock

Polling Question

Polling Question
What most influences customers to share their data with smart home suppliers?
a. Clear explanation of the benefits they'll receive
b. Transparent privacy policies and controls
c. Trust in your brand reputation
d. Competitive pressure (seeing others do it)
e. Regulatory requirement or incentive
f. Other / Open Response

What most influences customers to share their data with smart home suppliers?
(n=11)

Category	Value
Trust in your brand reputation	64%
Clear explanation of benefits they'll receive	55%
Transparent privacy policies and controls	36%
Other/open response	18%
Regulatory requirement or incentive	9%
Competitive pressure (seeing others do it)	9%
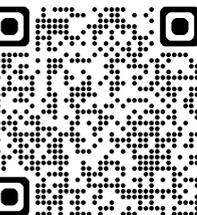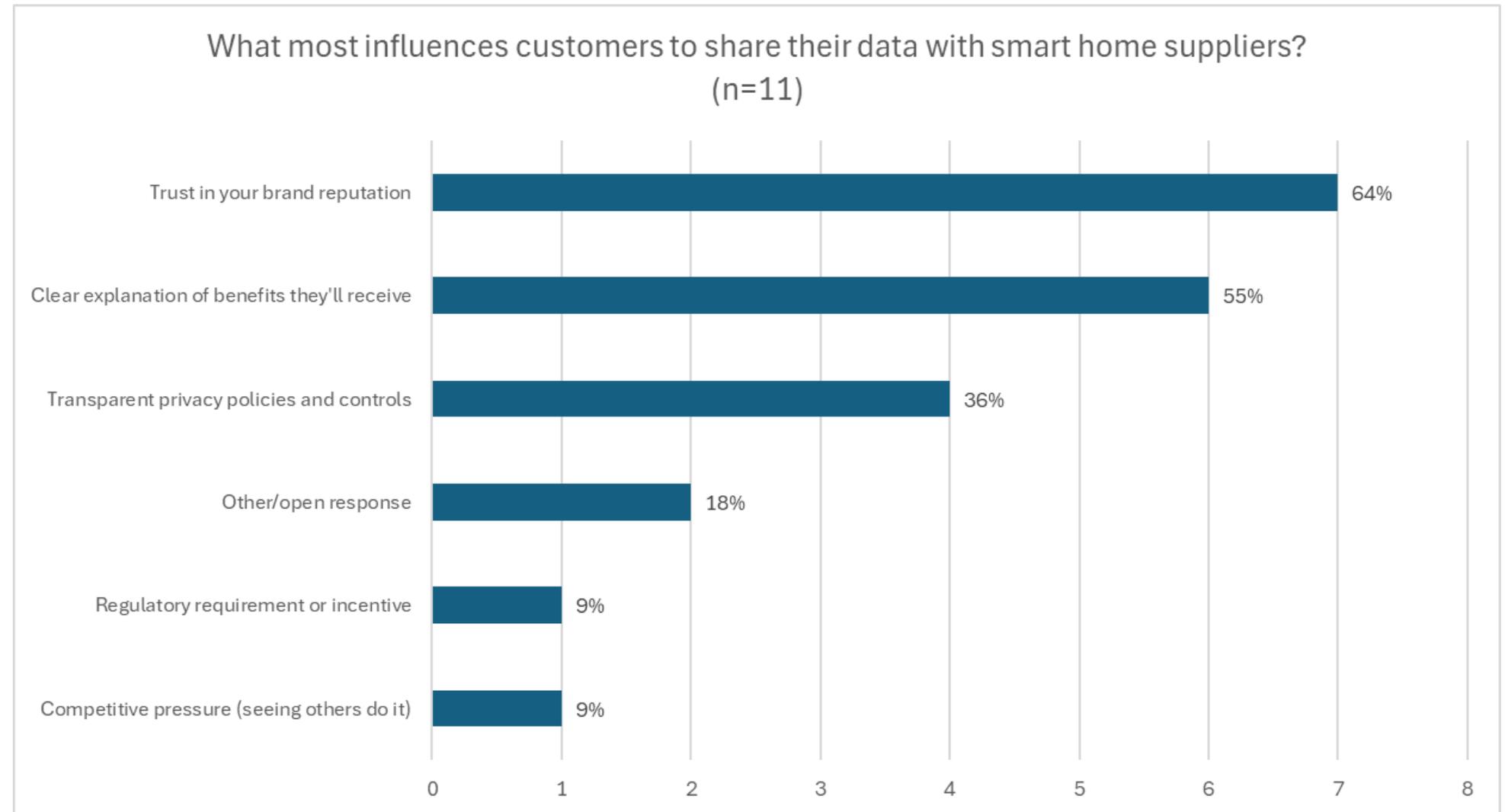
Interoperability & Standards: The Matter Protocol

Universal Connectivity Standard

- Designed to increase interoperability among smart home devices across multiple platforms

- Simplifies multi-vendor ecosystems by reducing fragmentation and compatibility issues

- Accelerates market adoption through seamless integration

Enhanced Privacy and Security

- Enforces consistent data handling and protection practices across devices

- Enables controlled sharing of user data to reinforce consumer trust

- Implements end-to-end encryption standards

Industry Alignment

- Represents a major step towards common technical standards in the smart home industry

- Positively influences consumer confidence in data privacy and device security

- Backed by leading tech companies and industry consortiums
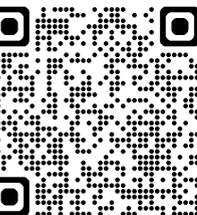
Interoperability & Standards: The Matter Protocol

Polling Question

What is your organization's current status regarding the Matter interoperability standard?

a. Fully adopted, certified products in the market
b. In development/testing phase
c. Evaluating/planning adoption
d. Not pursuing (using proprietary standards)
e. Waiting to see market adoption first
f. Other / Open Response

What is your organization's current status regarding the Matter interoperability standard? (n=7)

Category	Value
Not pursuing (using proprietary standards)	14%
Waiting to see market adoption first	14%
Evaluating/planning adoption	29%
Other/open response	43%
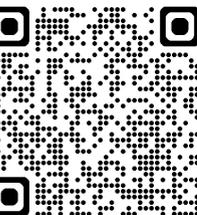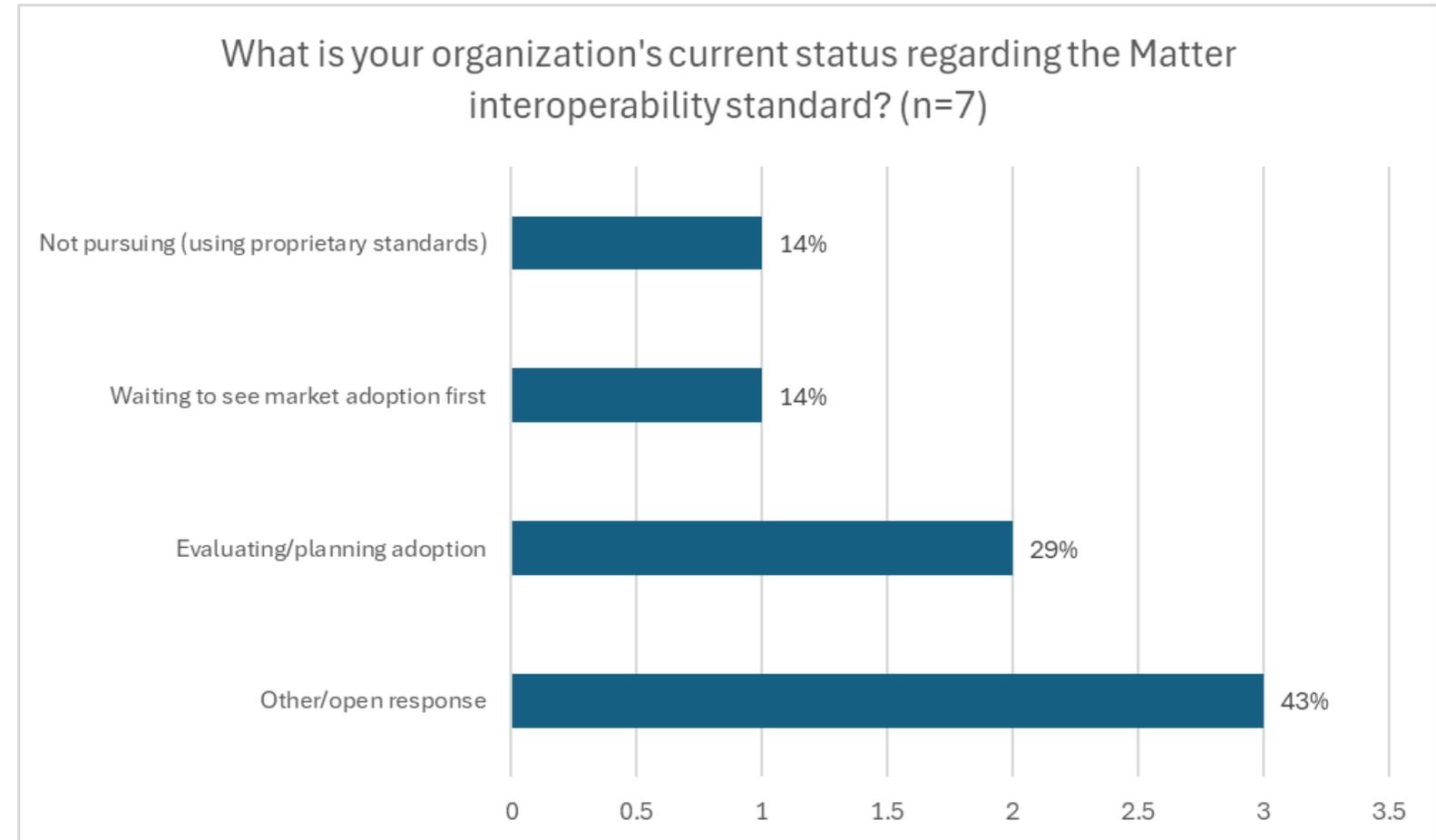
Evolving Privacy Regulations for Smart Homes

Key milestones shaping global and US data protection standards

1 2018 – GDPR Enforcement

European Union regulation establishing comprehensive consumer data protection and privacy transparency, setting global benchmark.

2 2018 – California Consumer Privacy Act

Introduced strong consumer data rights and privacy protections at state level, influencing nationwide approaches.

3 2020 – IoT Cybersecurity Improvement Act

Federal US law setting minimum security standards for Internet-connected devices in government procurement and operations.

4 2023 – Cyber Trust Mark Initiative

Emerging global program promoting trust via cybersecurity certification for IoT products, enhancing consumer confidence.
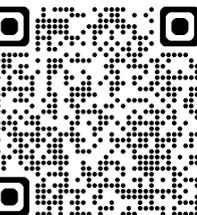
Vendors Can Improve Offerings With A Complete Product Life Cycle View

While consumers often associate data with advertising or sales, manufacturers can derive significant value by using customer data to enhance product design, functionality, and longevity, ultimately improving the customer experience.


Beginning of Life (BOL)

Design & Development

Middle of Life (MOL)

Manufacture

Sell

End of Life (EOL)

Operate

Maintain

Manufacturing Data

Sales Data

Performance and Usage Data

Support, Maintenance and Failure Data
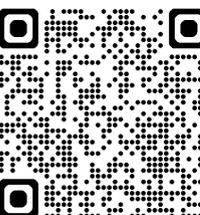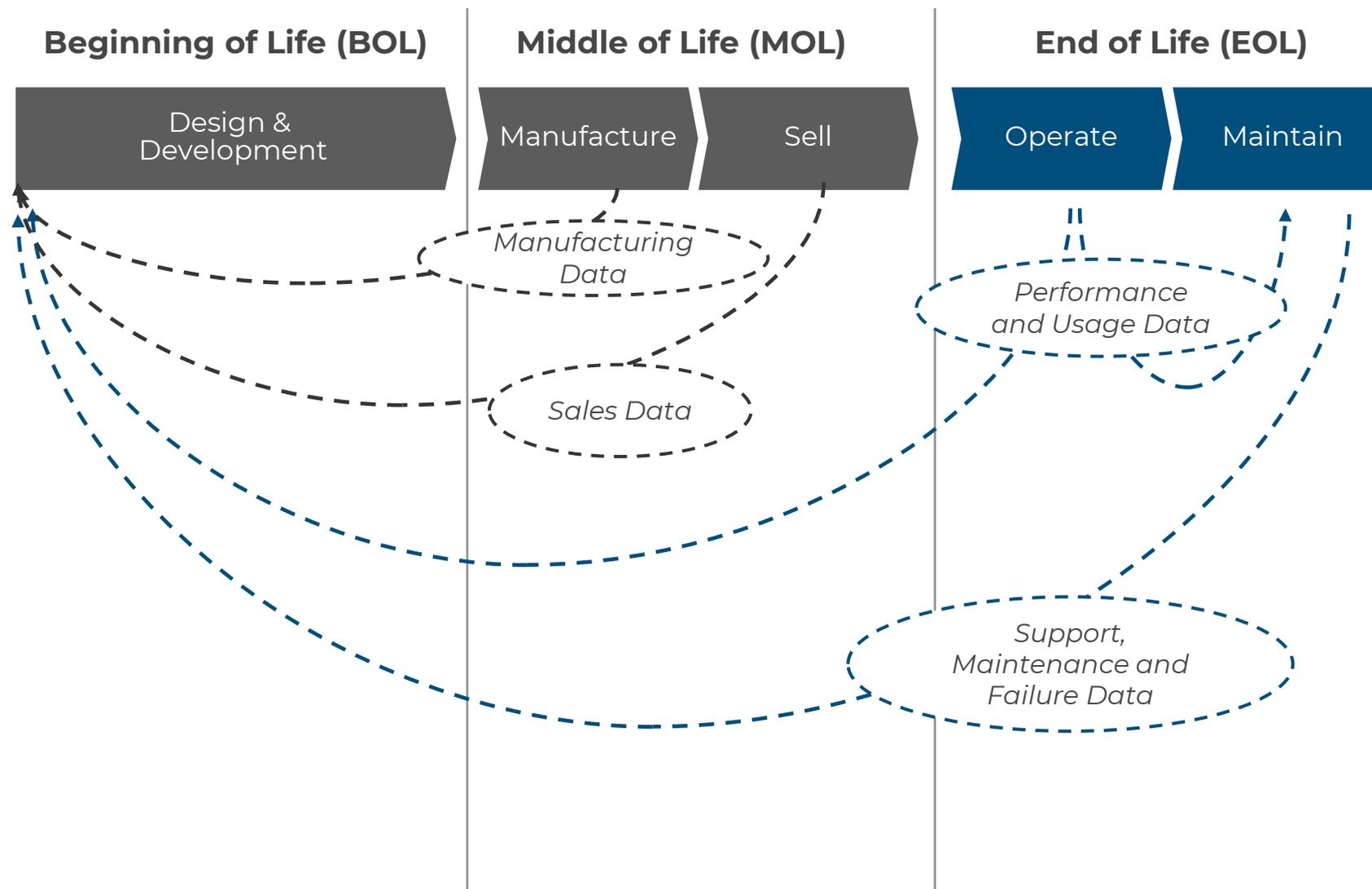
Vendors Can Improve Offerings With A Complete Product Life Cycle View

Polling Question

What is your PRIMARY business driver for collecting customer data?

a. Product improvement and R&D
b. Personalized customer experiences
c. Predictive maintenance and support
d. New revenue streams or business models
e. Required for basic functionality
f. Other / Open Response

What is your PRIMARY business driver for collecting customer data? (n=9)

Personalized customer experiences	56%
Product improvement and R&D	44%
Required for basic functionality	22%
Predictive maintenance and support	22%
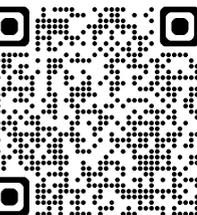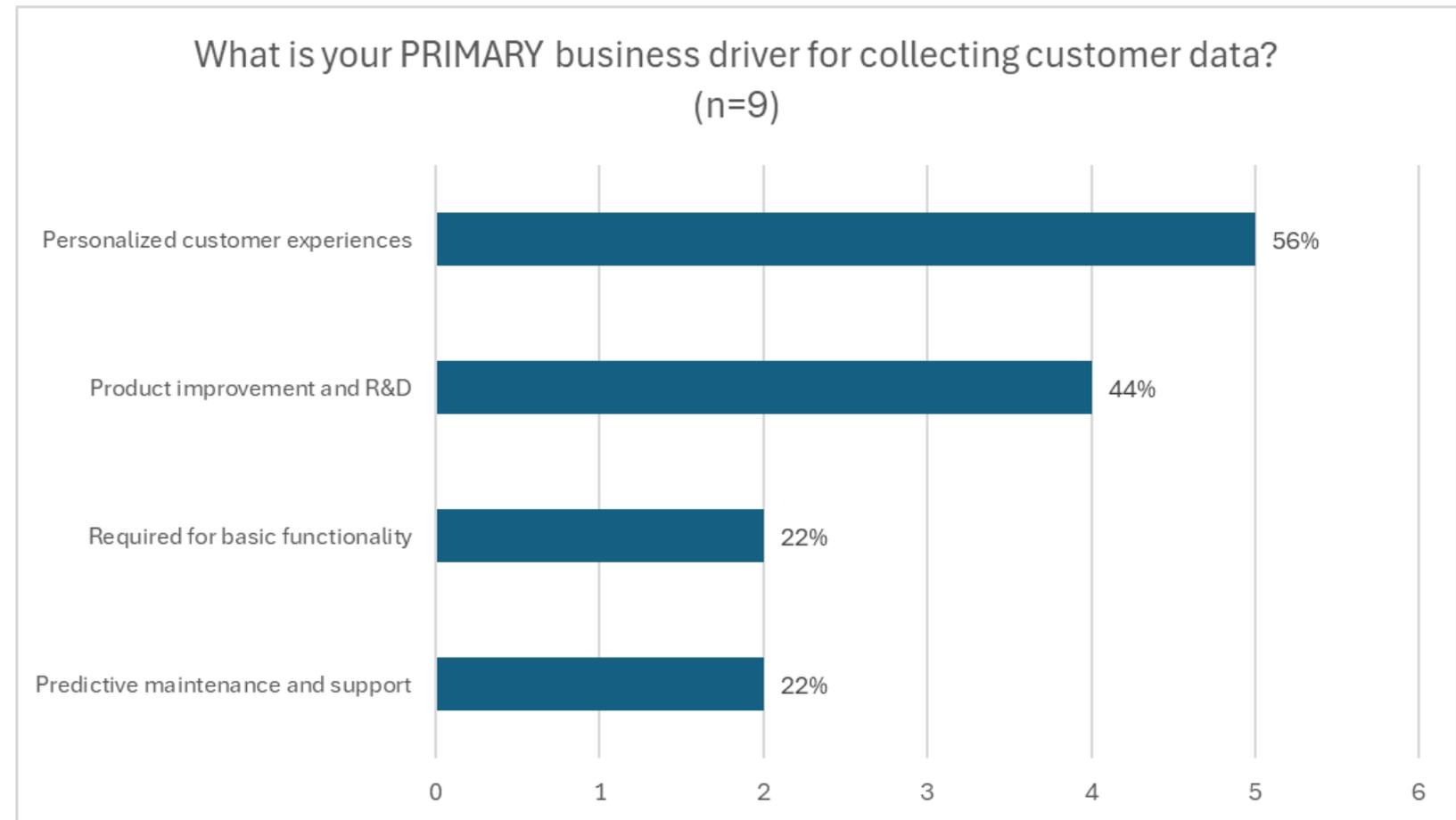
Staying Local Can Decrease Cybersecurity Risks

Although there's multiple benefits to allowing external connections, once devices are made accessible to external networks, security vulnerabilities can increase

Sending data to the cloud inherently places trust in external service providers to securely manage said data

External server

Weakly-secured devices can provide hackers with entry points to all devices connected to the home network

Smart home inputs and data

Home network
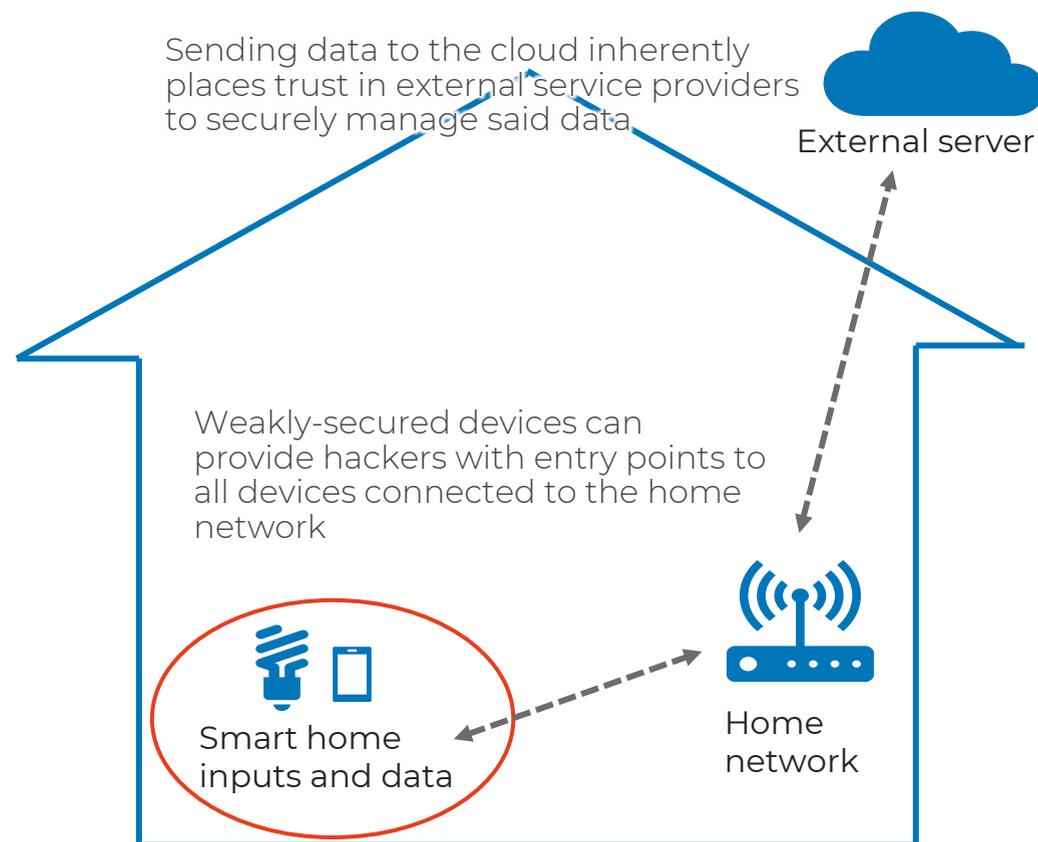
Especially as data sizes increase, cloud storage can prove beneficial for its flexibility and remote access features.

Smart home solutions, however, do not *have* to store everything in the cloud. For privacy-oriented consumers, local storage alternatives may provide peace of mind.
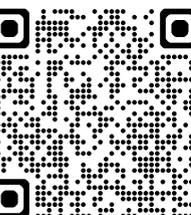
Value-Based Data Exchange

Driving mutual benefits through ethical smart home data sharing

Empowering data collaboration for mutual success.

→ **Consumer Benefits**

Consumers gain personalization through tailored services, improved energy efficiency, and ongoing innovation that enhances daily living.

→ **Supplier Benefits**

Suppliers access valuable insights to refine offerings, create new revenue streams, and achieve service differentiation in competitive markets.

These approaches build mutually beneficial relationships—customers keep control over their data while suppliers enhance value with ethical data use.

Model	Data Ownership	Privacy & Control	Value Distribution	Collaboration Scope	Example Use Case
Data Marketplace Transparent exchange platforms	Shared / tradeable	Variable, negotiable	Explicit (sales/tokens)	Multi-party, commercial	Selling energy usage data
Personal Data Store User-controlled repositories	Individual-owned	High, granular	User-centric	Limited (user chooses)	Home health tracking
Federated Learning Privacy-preserving analytics	Decentralized	Strong, by design	Algorithmic/collective	Collaborative, anonymized	AI security camera analytics
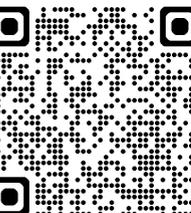
Overcoming Key Business Barriers

Identifying top challenges to accelerate privacy innovation

Regulatory Complexity
Complex regulatory compliance creates uncertainty and slows adoption across diverse jurisdictions.

Integration Challenges
Technological integration challenges hinder seamless deployment across diverse device ecosystems.
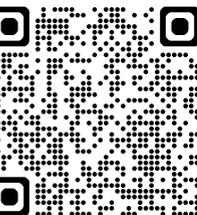
Education Gaps
Consumer education gaps limit understanding and trust, reducing engagement with privacy features.

Cost Barriers
High associated costs restrict investment and scalability for privacy solutions.

Overcoming Key Business Barriers

Polling Question

What is the BIGGEST barrier to achieving better data privacy in smart homes?

a. Regulatory complexity or inconsistency
b. Consumer education/awareness gap
c. Technology limitations/costs
d. Business model dependency on data
e. Lack of industry coordination
f. Other / Open Response

What is the BIGGEST barrier to achieving better data privacy in smart homes? (n=9)

Barrier	Percentage
Lack of industry coordination	56%
Regulatory complexity or inconsistency	33%
Business model dependency on data	33%
Consumer education/awareness gap	33%
Technology limitations/costs	11%
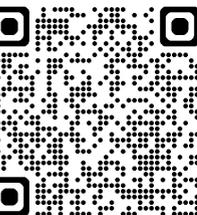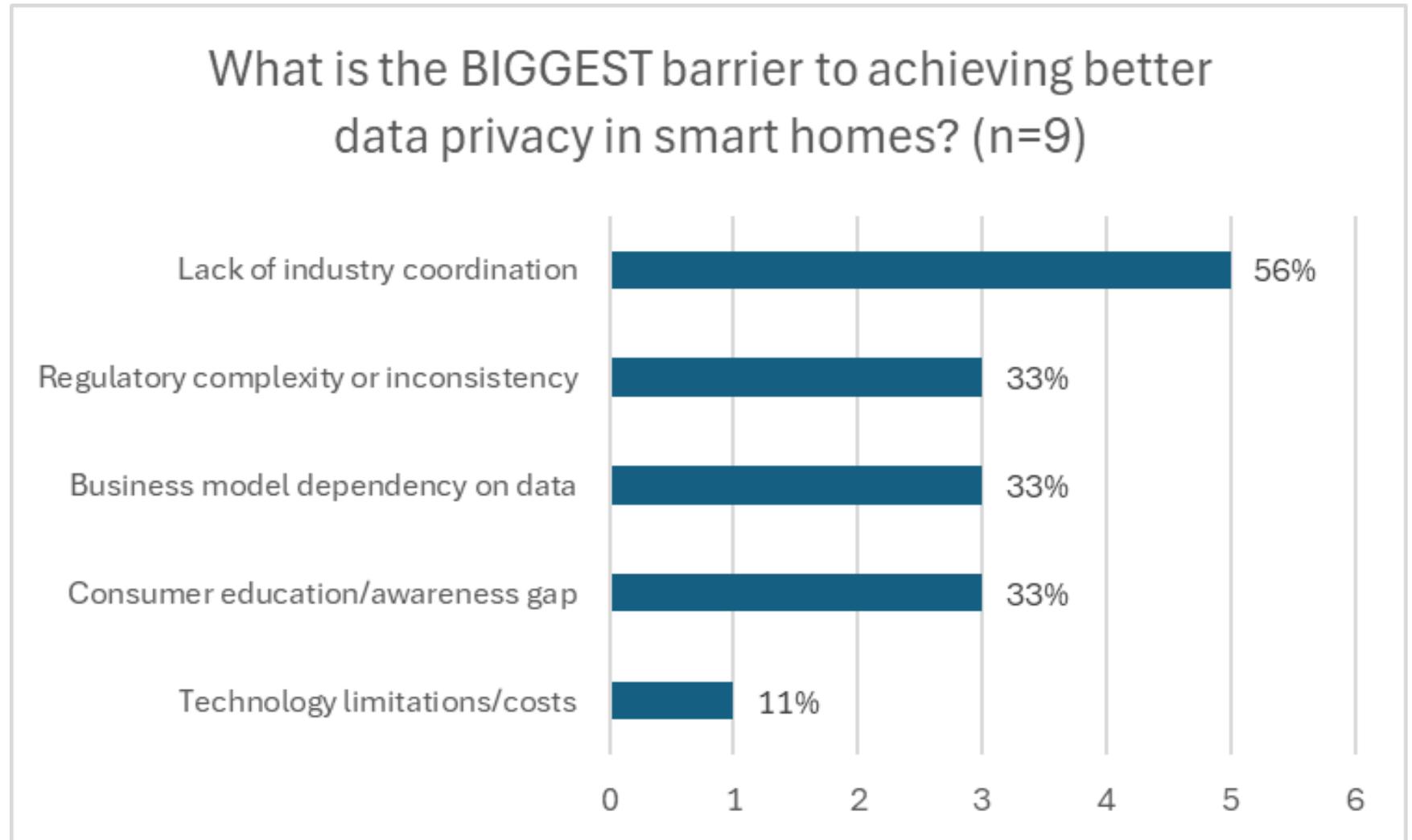
Supplier Differentiation & Best Practices

Building trust and compliance through strategic privacy measures

01

Privacy-by-Design

Embed data protection from the start of product development, not as an afterthought.

02

Transparent User Controls

Enable clear management of data preferences through intuitive interfaces and dashboards.

03

Local Data Storage

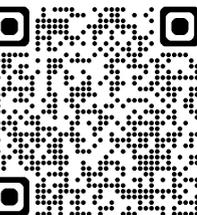Minimize external exposure of sensitive information and enhance data sovereignty.

04

Security Certifications

Pursue recognized certifications to validate security posture and build consumer confidence.

05

Competitive Advantage

Promote responsible data stewardship as a key market differentiator within smart home ecosystems.

Polling Questions

Which privacy/security feature would you prioritize investing in next?

a. Local/on-device processing capabilities
b. Enhanced user privacy dashboard/controls
c. Third-party security certification
d. Privacy-preserving AI technologies
e. Transparent data marketplace/sharing options
f. Other / Open Response

Which privacy/security feature would you prioritize investing in next? (n=10)

Feature	Percentage
Enhanced user privacy dashboard/controls	50%
Privacy-preserving AI technologies	30%
Local/on-device processing capabilities	30%
Other/open response	20%
Third-party security certification	20%
Transparent data marketplace/sharing options	10%
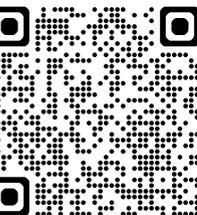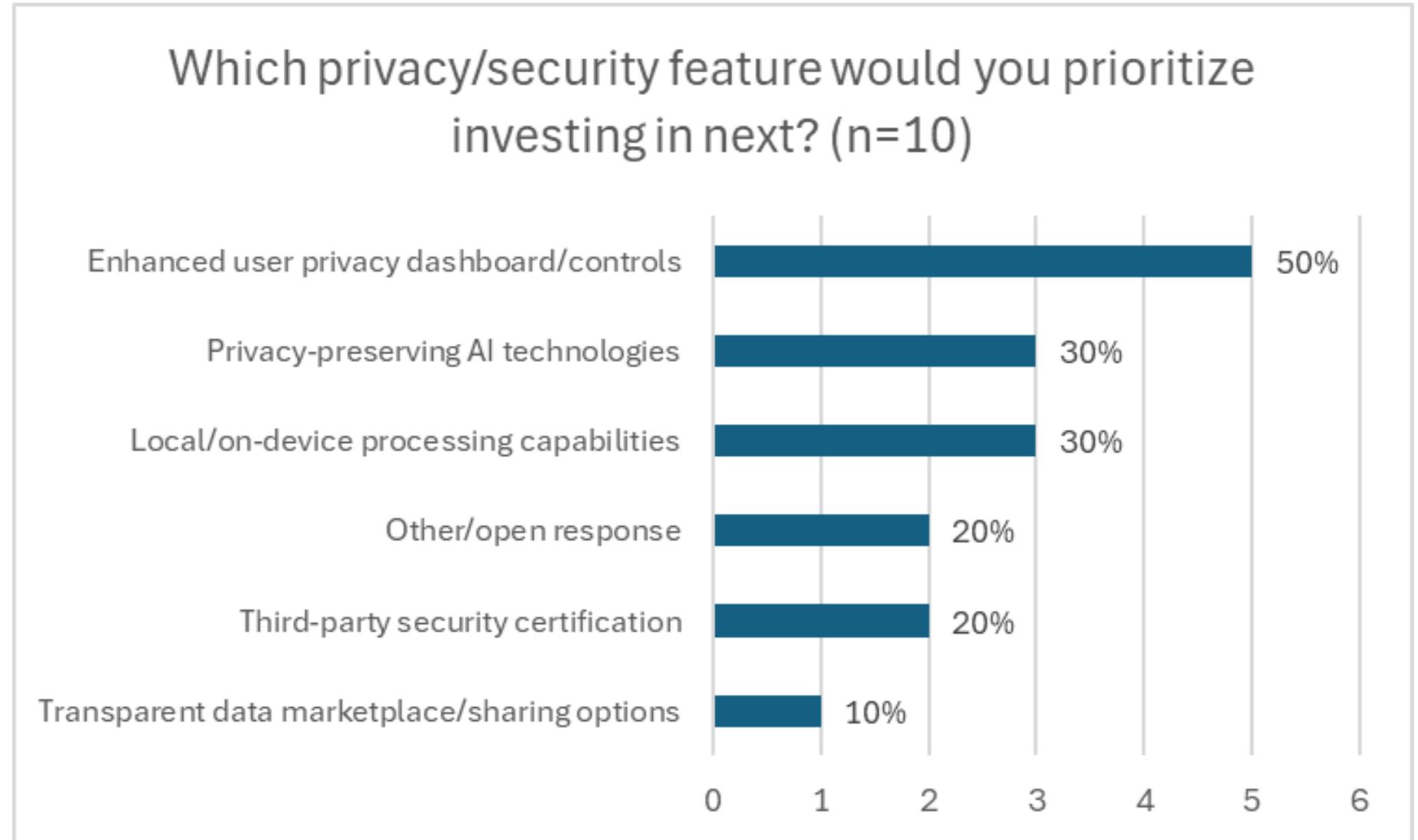
Polling Questions

Which cross-stakeholder collaboration would most benefit the industry?
a. Manufacturers + Platform owners (standardization)
b. Suppliers + Utilities (value-based programs)
c. Industry + Policymakers (sensible regulation)
d. Companies + Consumer groups (trust building)
e. Integrated approach (all of the above)
f. Other / Open Response

Which cross-stakeholder collaboration would most benefit the industry? (n=10)

Category	Percentage
Integrated approach (all of the above)	70%
Industry + Policymakers (sensible regulation)	20%
Companies + Consumer groups (trust building)	20%
Manufacturers + Platform owners (standardization)	20%
Suppliers + Utilities (value-based programs)	10%
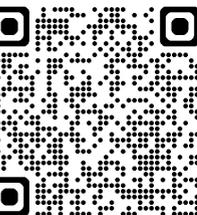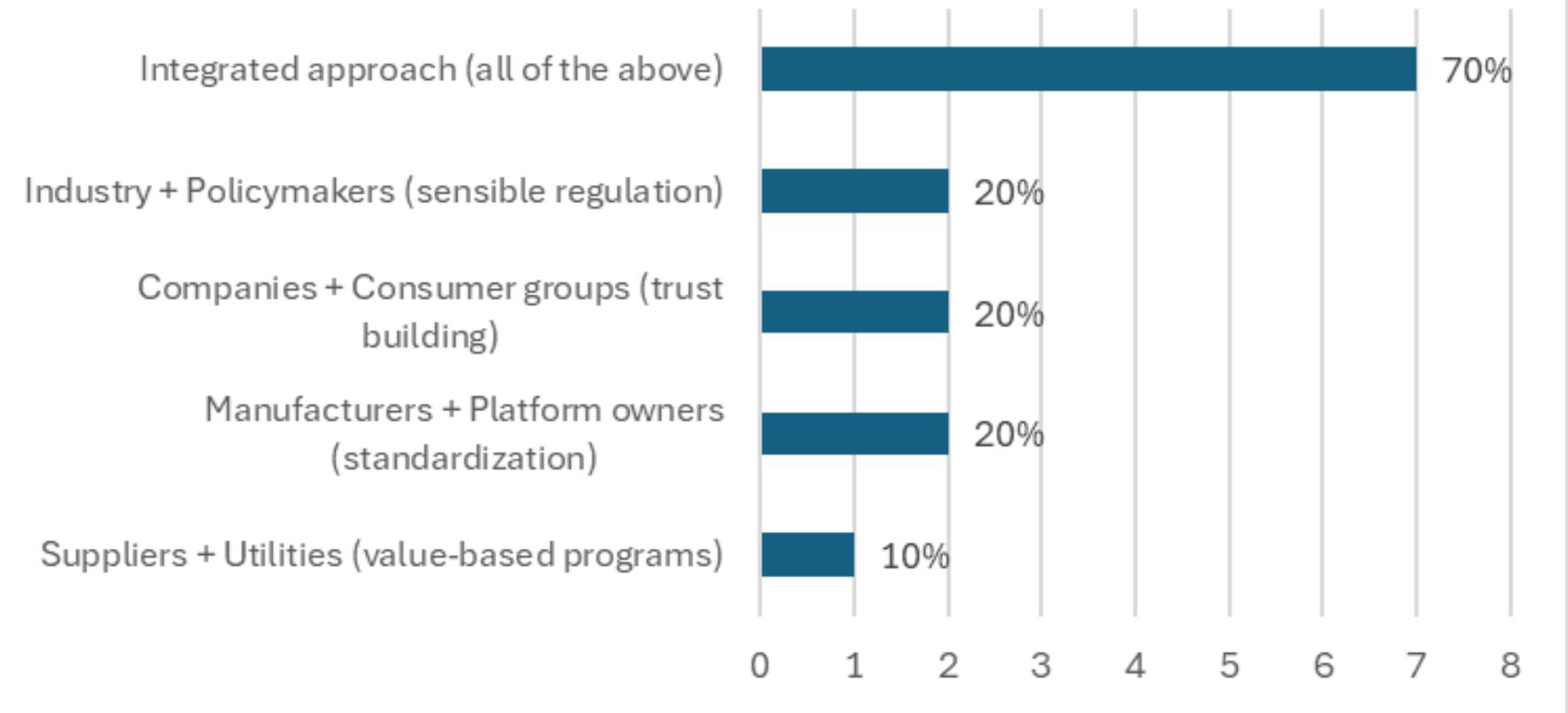
Next Steps: Empowering a Privacy-First Smart Home Future

To navigate the evolving smart home landscape successfully, suppliers must act decisively across immediate, medium-term, and long-term horizons.

Immediate Actions

- Conduct a comprehensive audit of current data practices against privacy-by-design principles.
- Enhance transparency in data collection and processing policies.
- Implement clear, informed consent mechanisms for all data types.
- Begin evaluating the Matter protocol for seamless device integration.
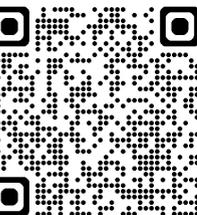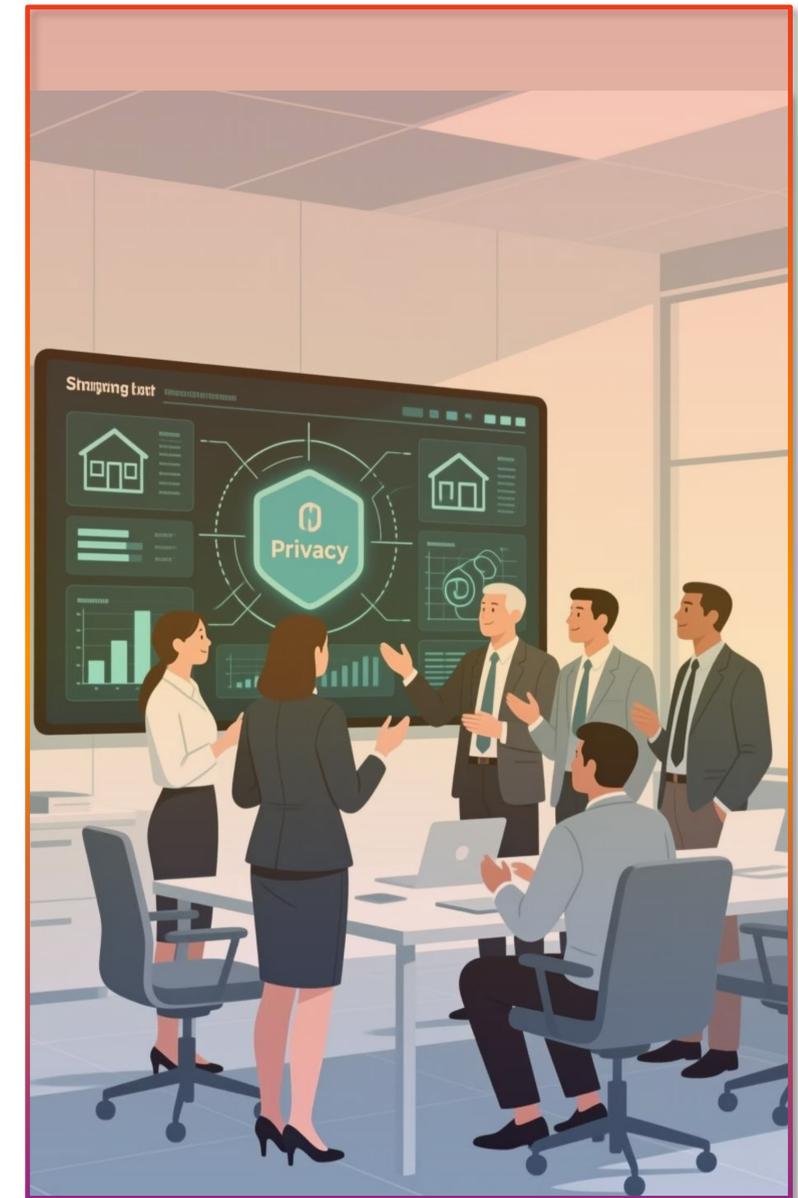
Medium-Term Strategies

- Develop robust user dashboards for granular data control and preferences.
- Pursue industry-recognized security and privacy certifications.
- Pilot Matter-enabled devices to test interoperability and security benefits.
- Explore models for value-based data exchange, such as data marketplaces.

Long-Term Goals

- Establish privacy as a core brand differentiator and competitive advantage.
- Proactively engage with regulatory bodies to shape future privacy standards.
- Invest in research and development for privacy-enhancing technologies like federated learning.
- Lead the smart home ecosystem in ethical data stewardship and consumer trust.

By committing to these strategic steps, suppliers can build a more secure, trustworthy, and ultimately successful smart home ecosystem.

Questions?

ASHB
Association for Smarter Homes & Buildings