

# Trends in Smart Home Data Security and Privacy

<https://marketpublishers.com/r/TD700A38A34CEN.html>

Date: October 2019

Pages: 82

Price: US\$ 3,500.00 (Single User License)

ID: TD700A38A34CEN

## Abstracts

Connectivity in the home and the addition of connected devices continue to expand year-over-year, with consumers now owning an average of more than eight connected CE products in their home. The increasing levels of connectivity in consumers' lives provide easy targets for hackers and present security and privacy concerns for consumers. This report examines the challenges in securing the smart home and new opportunities for security solution providers. The report also assesses common and potential attacks in the connected landscape as new connected solutions, such as 5G technologies, are implemented. It profiles companies offering data security solutions for the connected home and product and service providers who are leading the way on securing the smart home.

## Contents

### RESEARCH OBJECTIVES

Research Approach  
Companies Interviewed or Researched

### EXECUTIVE SUMMARY

Industry Insight  
Data Security & Privacy Trends - User Experiences  
Data Security & Privacy Trends - Technologies  
Data Security & Privacy Trends – Marketing & Sales Channels  
Connected Home Data Security and Privacy Ecosystem  
Key Findings and Recommendations

### DEFINING DATA SECURITY AND PRIVACY

Data Security vs. Data Privacy  
Trade-offs for Consumers  
Classification of Data Security and Privacy Attacks  
Targets and Objectives of Data Security/Privacy Attacks  
Direct and Indirect Attacks  
Privacy Vulnerabilities

### CONSUMER INSIGHTS

Security/Privacy Concern and Problems (Q4/18)  
Consumer Concerns on Security/Privacy Issues (Q4/18)  
Actions Taken to Prevent Unauthorized Access to Devices (Q4/18)  
Smart Home Devices: Purchase Inhibitors (Q4/18)  
Appeal of Cybersecurity Services (Q4/18)  
Appeal of Cybersecurity Services by Introduction Text (Q4/18)  
Desirability of Cybersecurity Services (Q4/18)  
Preferred Provider of Cybersecurity Services (Q4/18)

### DATA BREACH INCIDENTS AND VULNERABILITIES

Status of Data Breaches in Connected Homes

The 2016 Mirai Attack by Exploiting Default Username/Password  
The 2017 Fish Tank Attack Showed Much Bigger Lateral Damages  
The 2019 Nest Cam Hacking due to Credit Stuffing Attacks  
Supporting Consumers: An Academic Study on Privacy Vulnerabilities in Smart Home  
Turning Data Attacks into Physical Attacks  
Data Privacy/Security Ecosystem Opportunities for Action

## **REGULATORY ANALYSIS ON DATA SECURITY AND PRIVACY**

Legislations on Smart Home Data Security and Privacy  
Leading Legislation: The EU General Data Protection Regulation (GDPR)  
GDPR: The Smart Home Manufacturers Respond  
Data Protection Laws in the US  
Passed and Pending US Regulations and Standards  
Federal Standards: Defining Cybersecurity and Privacy Risks for Organizations  
Federal Standards: IoT Device Manufacturers  
Pending Federal Legislation: IoT Device Manufacturers Selling to Government  
State Legislation: California SB-327 Information Privacy: Connected Devices 2018  
State Legislation: CCPA Affects Businesses Using Consumer Data  
CCPA vs. GDPR - Summary  
CCPA vs. GDPR - Details  
Cybersecurity Impacts: Brand Perception and Fines

## **BUSINESS MODELS AND SERVICES**

Business Models in Smart Home Data Security and Privacy  
Interest in Security/Privacy Services (Q4/18)  
A Taxonomy of Cybersecurity Solutions  
B2C Business Model by Smart Home Service Provider  
B2C Business Model by Broadband Service Provider  
B2B Business Models  
B2C and B2B Example: F-Secure  
Business Models: B2B + B2B2C  
CUJO AI Security Profile  
CUJO AI: Unique Advantages  
The Public/Private Partnership Model

## **TECHNOLOGY OPPORTUNITIES**

Technologies to Protect Data Security and Privacy in Smart Home  
Tradeoff between Security and Convenience: TFA and MFA  
Privacy Enhancing Technologies (PET)  
Typical Privacy Enhancing Technologies  
AI and ML Become Essential for Cybersecurity  
Where and How to Apply AI/ML in Cybersecurity  
Example: Cybersecurity AI Platform  
Privacy by Design (PbD)  
Impact of 5G to Smart Home Data Security and Privacy

## **APPENDIX**

Glossary of Security Threats  
Definition of Adversary/Threat Model  
Capability Levels of Adversary & Threat Models

## I would like to order

Product name: Trends in Smart Home Data Security and Privacy

Product link: <https://marketpublishers.com/r/TD700A38A34CEN.html>

Price: US\$ 3,500.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/TD700A38A34CEN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:  
Last name:  
Email:  
Company:  
Address:  
City:  
Zip code:  
Country:  
Tel:  
Fax:  
Your message:

**\*\*All fields are required**

Customer signature \_\_\_\_\_

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970