

# Feeling Safe in the Home of the Future

A product life-cycle approach  
to improve the trustworthiness  
of smart home products  
and services

BRIEFING PAPER

AUGUST 2020



Cover: R Classen Layouts/Getty Images

Inside: Hispanolistic/Getty Images, Marvin Samuel Tolentino Pineda/Getty Images, Eye Crave/Getty Images, Onfokus/Getty Images, Glenn Carstens-Peters/Unsplash

# Contents

3	Foreword
4	1 Introduction
7	2 Pre-Market
9	3 Sales and Setup
11	4 After-Market
13	5 Conclusion
14	Contributors
15	Endnotes

© 2020 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.



# Foreword

Smart home technologies are changing the way we live. It is time to change the way we design and manage these technologies.



**Burak Demirtas**  
Koç Holding Fellow,  
Centre for the Fourth  
Industrial Revolution,  
World Economic Forum



**Jeff Merritt**  
Head of Internet of  
Things, Robotics and  
Smart Cities, Member of  
Executive Committee,  
World Economic Forum

For many children and young adults growing up around the world today, voice assistants such as Alexa, Siri or Google Assistant have become almost like another member of the family. They provide advice on the weather when you cannot decide what to wear, they answer your questions when you are having trouble remembering a fact or are just feeling curious, they can tell you a joke or play your favourite songs if you are feeling down, and they may even help turn off the lights for you when it is time for bed.

Whereas voice assistants and smart speakers are still relatively new – Amazon Alexa and Echo were

first introduced in 2014 – the ease and speed in which consumers have adopted these and other smart home technologies has been dramatic. Meanwhile, many details about these technologies – from their business models to their product features and maintenance plans – remain ill-defined or shrouded in mystery. It is time for the smart home ecosystem to grow up.

This paper is intended to spur collective thinking and action among business, government and civil society. We invite you to join us as we work to shape the development, use and impact of these technologies for the benefit of society.

1

# Introduction

To realize the true promise of the smart home, trust must be baked into each phase of the product life cycle.

A home is more than a building or a place of shelter. It is where we take care of the people and things that mean the most to us. Turning a physical structure into a place of comfort, safety and sanctuary is hard work, but what if the home itself could help?

This is the promise of the smart home, a house equipped with internet-connected devices for controlling, automating and optimizing functions such as temperature, lighting, security or entertainment, either remotely or through a system within the house. Incorporating these Internet of Things (IoT) devices into a home can help a homeowner increase the safety of their loved ones and valuables, save money on energy bills, improve their wellness and save time.

Technological advancements can also come with unintended impacts for society. The appliance boom brought forward by the Second Industrial Revolution, for example, not only made it easier to do laundry, it ultimately opened the door for more women to enter the workforce.<sup>1</sup> The introduction and expansion of processed foods and microwave ovens made mealtime easier at home, but also contributed to higher rates of obesity.<sup>2</sup> As the smart home environment continues to evolve, the full range of new opportunities – as well as potential challenges – continue to emerge.

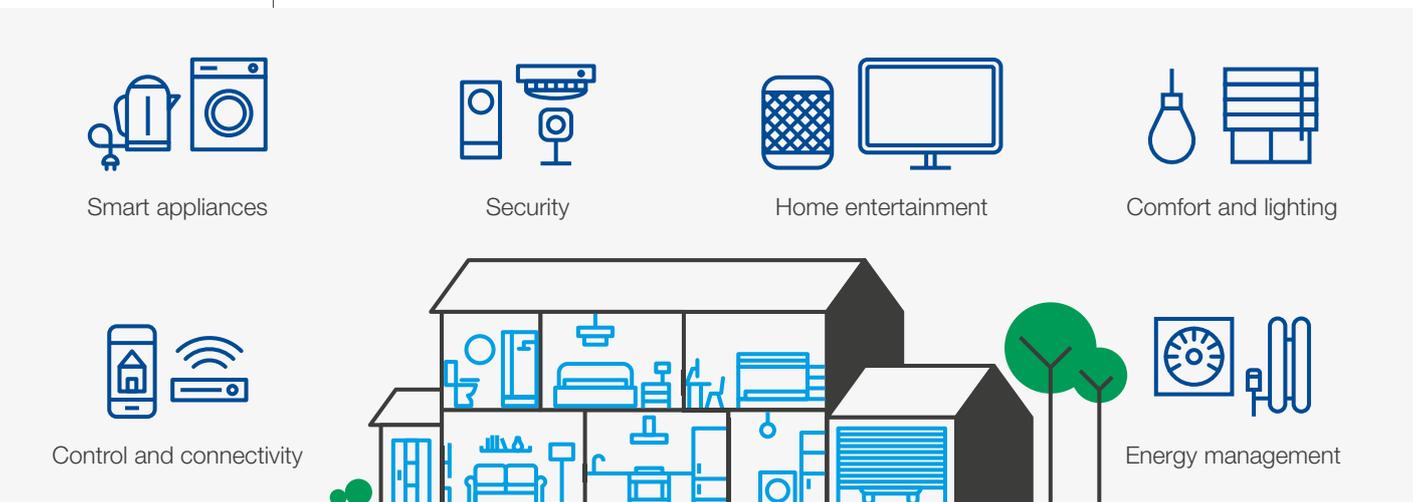
The COVID-19 pandemic is shining a spotlight on the potential impact of smart home devices

in our daily lives, businesses and society. Most notably, COVID-19 has dramatically increased the amount of time people are spending at home. According to data from Google’s COVID-19 Community Mobility Report, the global average of time spent at home increased 35% in March 2020 as a wide range of shelter-at-home orders were put in place.<sup>3</sup> In this context, research from ABI Research suggests that smart home devices, such as touchless doors, cameras and smart speakers, have an important role to play in enabling safe social distancing. The need for contactless ordering and delivery of goods, for example, is expected to increase global sales of voice-controlled devices and cameras.<sup>4</sup>

Smart home IoT devices can also take care of the world outside of the home. By enabling a more efficient use of energy, devices such as smart thermostats, smart lights and smart refrigerators hold the potential to decrease a home’s impact on the environment. If half of homes globally transitioned to using smart thermostats by 2050, it is estimated that 2.6 gigatons of carbon dioxide emissions would be eliminated, roughly equal to 8% of global CO<sub>2</sub> emission in 2019.<sup>5</sup>

The concept of a smart home is not a recent creation; it has featured in laboratories and popular culture since the early 1900s. Yet, with recent advances in wireless technology and mobile platforms, smart home devices have become

FIGURE 1 Smart home devices by segment



affordable, viable and in demand. Smart home devices typically fall into one of six verticals: energy management, comfort and lighting, home entertainment, security, smart appliances, control and connectivity.<sup>6</sup> According to the International

Data Corporation (IDC) Worldwide Quarterly Smart Home Device Tracker, the smart home market is forecast to grow at a compound annual growth rate of 17% from 2019-2023 with nearly 1.6 billion devices shipped in 2023.

## A crisis of trust

To harness these benefits for consumers and the planet and drive economic value, smart home devices must have trust built in so that consumers feel they are fair and safe to use. Incorporating trust across the life cycle of a device is essential for a thriving smart home ecosystem. Whereas individual consumers may place different value on the product features that they feel are important when purchasing devices, consumers come with preexisting expectations regarding the privacy, security, reliability, usability and resilience of their devices. Each one of these aspects effect consumers' perception on the trustworthiness on the product and the manufacturer.

There are a number of important questions on consumers' minds as they consider purchasing smart home devices:

- Could someone hack into my security camera without my knowledge?
- Do companies sell my information to other companies for extra revenue?
- Is my voice assistance listening to my conversations? Can I delete my data?
- Could law enforcement get access to my data?

Recent research conducted by Consumers International and the Internet Society found:<sup>7</sup>

- 75% of respondents distrust the way data is shared
- 50% of respondents do not know how to disable a data collection feature

- 28% of respondents do not want to buy a smart device due to cybersecurity concerns
- 88% of respondents think that manufacturers should have to comply with legal privacy and security standards

These findings clearly articulate the connection between consumer trust and the privacy and security of IoT devices. Moreover, they show that consumers expect policy-makers to play an active role in creating a trustworthy environment by enacting regulations and guidelines for privacy and security. As such, this paper will mainly focus on the privacy and security aspects of the smart home ecosystem to improve trust.

Contrary to common public perception, smart home device manufacturers have been heavily investing in new innovations to build more trustworthy devices. This includes technical solutions like encrypting communication between devices and storing personal data in secured cloud platforms. Many of consumer concerns stem from the fact that neither these technical implementations nor the data sharing protocols between companies are transparent or easy to understand.

Additionally, sources such as the Internet Society's report *The economics of the security of consumer-grade IoT products and services*,<sup>8</sup> identify misaligned incentives on cost of security risks and missing responsibility on attacks to external entities by these IoT devices as critical factors for lack of trust. Taken together, the transparency issues related to technical complexities and the economic considerations related to cost of risks demonstrate an obvious gap between stakeholders' perceptions of trustworthiness in smart home devices.

## A path forward

Effectively building consumer trust will require collective action by all stakeholders in the smart home ecosystem. This includes, but is not limited to, device manufacturers, standard development organizations, retailers, government and civil society organizations. Among these stakeholders, policy-makers have an important role to play in establishing a level of consumer

protections that reflect common duty of care and establishing the respective responsibilities of the business community and consumers or end users of technology.

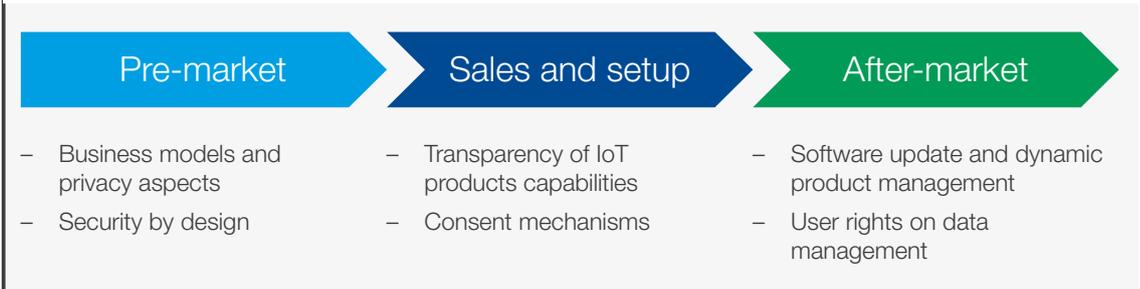
While regulations and standards are critical in creating a trustworthy smart home environment, crafting them is no easy feat. Things like software

updates, data collection and internet connectivity require frameworks to consider not only design phase implementations and processes, but also after sales implementations and processes too.<sup>9</sup> To develop proper policies that take these features into account, it is important to consider all the processes related to product life cycle; from design to business model, to manufacturing, marketing and even aftersales of a smart home device.

These elements of the product life cycle can be grouped into three phases. The first phase is

called the pre-market phase and it encompasses activities handled prior to launch: design, business development and manufacturing. The second phase is called sales and setup, and it includes activities related to product marketing, educating consumers about product capabilities and providing consent mechanisms during product setup. The final phase, called after-market, focuses on software feature updates and user rights on data-related processes. Although there are some common themes in all these phases, each offers unique opportunities for building consumer trust.

FIGURE 2 Product life-cycle phases and trust-related topics



The sections that follow are structured to map against the three phases of the smart home product life cycle. Section one on the pre-market phase focuses on the impact of business models on privacy and security by design principles. Section two addresses the sales and setup phase and elaborates on topics related to product feature transparency and consent mechanisms. Finally,

the section on the after-market phase is dedicated to software updates and user rights on data management of devices. Through each of these sections, this paper intends to help policy-makers and other key stakeholders understand, consider and incorporate the phases of the smart home product life cycle as they define collective actions and guidelines for privacy and security.



## 2

# Pre-Market

## Trustworthy products begin with good product design.

A smart home product or service is more than a physical device. In fact, there are three core components that are generally required for a smart home product to achieve “smart” functionality:

- A human-computer interface
- A data platform over cloud infrastructures
- An internet-enabled device

Oftentimes, there is an additional component layered on top to allow for data sharing or device interoperability. It is not uncommon for each of these components within a single smart home product to be developed or managed by a different party. This layered structure and complex business model creates an untamed information jungle with regard to technology stacks, business models and privacy, which creates distrust on the part of the consumer.

## Business models and their effect on privacy

One of the ways in which smart home products have enabled companies to improve their revenues is by selling software services with smart home products. Arlo, a smart camera product manufacturer, for example, released home security solutions by selling cameras as products and cloud-recording capabilities with a monthly subscription.<sup>10</sup> Moreover, smart home products enable new business models such as advertising, subscriptions, pay-per-use and maintenance contracts by leveraging connectivity and continuous data streams. For example, streaming service boxes like Roku and Amazon Fire TV work as platforms for television channels, but they also create contracts based on user subscription and advertisement revenue. In fact, the majority of revenue for these streaming box companies does not come from selling streaming devices, but rather through ads and subscriptions.<sup>11</sup>

Unbeknownst to consumers, these companies may also be generating revenue based on consumer data. According to research conducted by Princeton University and the University of Chicago, 89% of Amazon Fire TV channels and 69% of Roku channels include tracking software that collects information about viewing habits and preferences of the users.<sup>12</sup>

While the research on streaming devices show the hidden data collection mechanisms, Consumers International’s research reveals that 65% of consumers are concerned about data collection and data sharing through their smart home devices.

Clearly, one important factor in building trust is ensuring that device manufacturers store and

protect user data properly. Unfortunately, there are plenty of examples of irresponsible stewardship of personal data collected by smart home devices. Recently, the Electronic Frontier Foundation (EFF) conducted a test with Ring doorbell devices and discovered that the devices were sharing data with third-party companies, such as Facebook APIs.<sup>13</sup> Since data-sharing features are embedded into the software of the device, a user is not provided with the chance to learn what information is shared.

In recent years, regulators have spent a great amount of time deploying new privacy regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). However, it is still difficult for consumers to check if their devices, or the manufacturers of their devices, are compliant with these regulations. Transparency is essential to overcome this challenge, and there are models for how transparency helped consumers in other areas like OSHWA’s Open Source Hardware Certificate, Creative Commons’ content licensing, the FCC’s Broadband Nutrition Labels, Carnegie Mellon University’s Privacy Nutrition Labels, the iFixit Repairability Score, CE certification, the German Blue Angel environmental label, Fairtrade, energy star for home appliances and laundry labels.<sup>14</sup>

As listed above, there are many efforts either within the field or in different domains to enable transparency. It is crucial to merge the knowledge in these efforts with the needs of privacy in IoT and consumer education in technology. So, consumers become more informed within time to evaluate the products and services.

# Security by design

With every new connected device, the cybersecurity risk increases exponentially. Especially botnets, such as Kaiten, Qbot and Mirai, use IoT devices as the host for an attack to critical internet infrastructure.<sup>15</sup> Consider the Mirai botnet attack that caused many internet services to collapse in 2016. This attack originated in and spread through internet routers and security cameras that were using default passwords. This shows that designing the functionality of password management is necessary, but not enough for achieving security.

Another important feature that increases security and empowers consumers is two-factor authentication (2FA).<sup>16</sup> By implementing 2FA, companies enforce consumers to be a participant in the authentication process. As a result, this reduces the risk of hacking of the devices. Admin password change and 2FA are just two of the several concepts that manufacturers can embed to the smart home products to improve security by enabling consumer contribution.

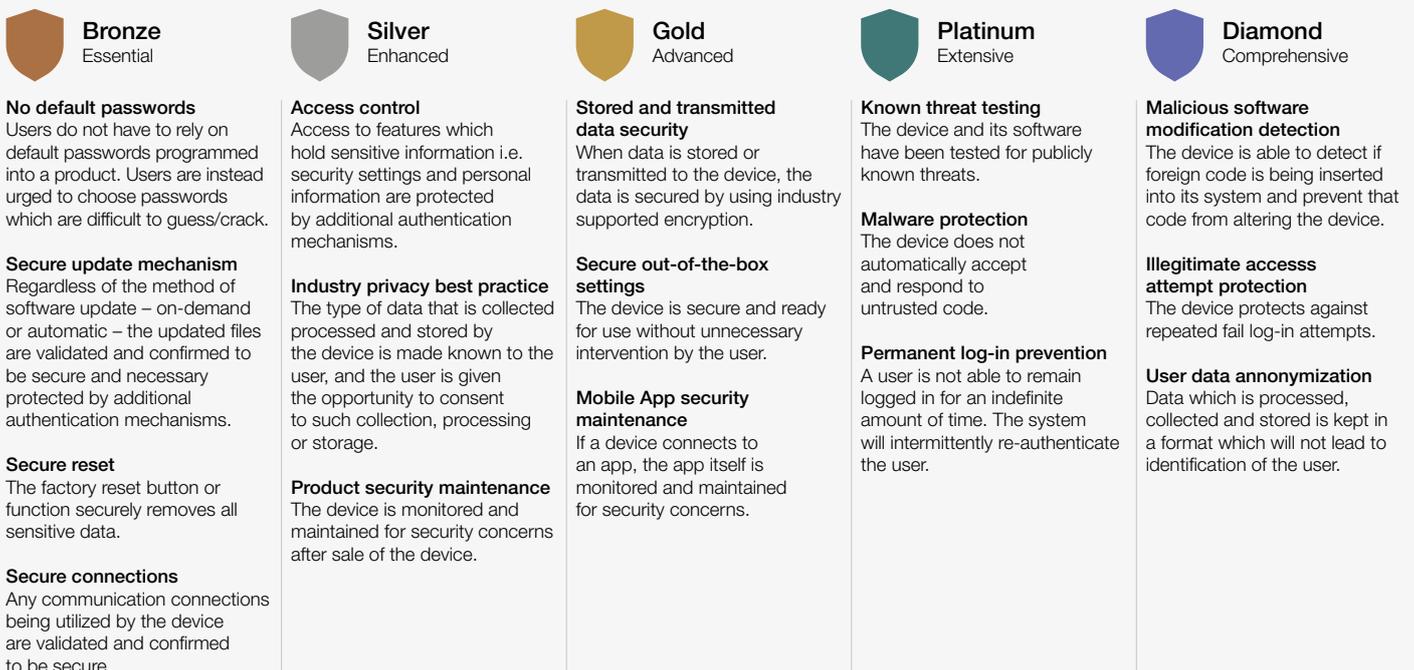
Another critical factor to consider when it comes to designing for security is the relationship to other devices. If there are several connected devices within the same network, the device with the weakest security precautions may cause other devices to be hacked. In 2017, hackers took over a casino's customer database through a fish tank's temperature adjustment system within the casino.<sup>17</sup> While it is not expected for a temperature sensor to have as high-level security as a camera, it should support a meaningful level of security by its design to reduce the risk to other devices.

Finally, security by design should encompass the manufacturing processes of smart home products. In today's connected world, this means that the supply chain should be considered as critical as in-house design. For example, many of the smart home device manufacturers use microcontrollers that are designed and manufactured by third parties. Since consumers do not have insight into these relationships, it is the device manufacturer's responsibility to check all supply chain steps properly.

It is not feasible to expect a user to understand and manage all of these risks properly. On the one hand, a regulatory framework is needed to standardize device security schemes for smart home devices. On the other hand, due to differences in IoT products' capabilities, a one-size-fits-all approach may not work while developing policies.

While new regulations such as the EU cybersecurity Act, California Bill SB-327 and Oregon House Bill 2395 are being released, there are also many industrial initiatives attempting to standardize products. The Common Criteria (ISO 15408) framework,<sup>18</sup> Underwriters Laboratories' IoT Rating scheme<sup>19</sup> and Mozilla Foundation's Privacy Not Included Guide,<sup>20</sup> IoTSF Compliance Framework<sup>21</sup> and Online Trust Alliance's The OTA IoT Trust Framework<sup>22</sup> are some of the efforts that organizations are actively working on. But, none of them currently forces manufacturers to comply with them. As a result, products that do not have proper security precautions can compromise an entire smart home environment. Comprehensive standardization of security will improve the reliability of the overall smart home ecosystem.

FIGURE 3 Underwriters Laboratories' IoT Rating scheme



3

# Sales and Setup

Transparency is a critical first step to enable more informed and empowered consumers.

Smart home products have become so ubiquitous that consumers can do many daily tasks such as turning on and off devices and monitoring home security with the help of these devices easily. Voice assistants, smart thermostats, security cameras and others make daily life and home management easier and more efficient, but consumers have little knowledge about how the manufacturers of these devices collect and share personal data. Research from Consumers International shows that 77% of

consumers look for information available about the product’s privacy and security either on a website or in literature included with the product during their purchasing decision process. Moreover, only 50% of consumers know how to disable data collection features on these devices. This knowledge gap for privacy and security requires policy-makers to address transparency issues at two key moments in time: in the creation of marketing materials and at the initial at-home setup of products.

## Transparency of IoT product features

Providing real-time situational awareness that enables adaptability and efficiency is one of many important features of smart home devices. This situational awareness is powered by the continuous collection of data from the surrounding environment. While the purpose for providing situational awareness is the same for every device, the technical capabilities and execution may be different. Consider smart doorbell products; at their core, they are intended to let a homeowner know the person at the door by sharing the scene that it records. However, there are a variety of products on the market that offer different video-sharing features. For example, Eufy offers cameras with local storage, while Ring sells products with cloud storage service. Even though both doorbells let users see who is at the door, their data collection and sharing technology are different. Many smart home devices have these

technical differences that are not immediately clear to consumers. Even with technical explanations in online retail pages or product packages, it is hard to understand the implications of these specifications. To reduce this knowledge gap, critical features of the devices – such as purpose, wireless technology and data storage location – must be more accessible for consumers.

Several groups are working on labeling frameworks to tackle this problem for the smart home,<sup>23</sup> medical wearables<sup>24</sup> and public spaces,<sup>25</sup> but a formal policy has not been developed yet. Consequently, consumers try to learn not only the features of the product, but also how it operates too. If there can be a guideline created like Figure 4 below, then people will be able to match their need with the products more efficiently.

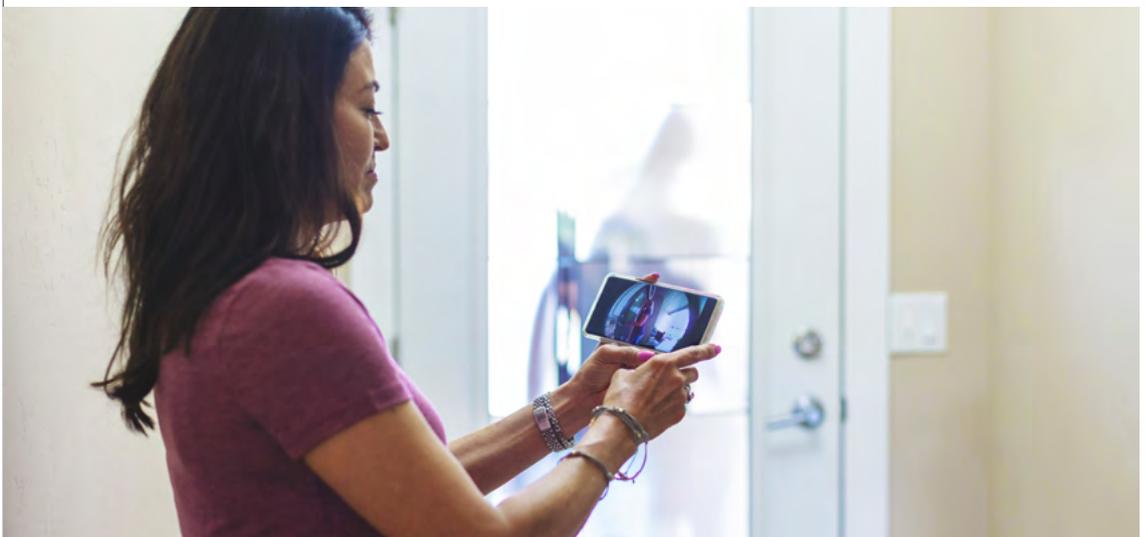


FIGURE 4 | An example IoT device label developed at Carnegie Mellon University

## Security & Privacy Overview

**Smart Security Camera NS200**  
 Firmware version: 2.5.1 - updated on: 6/15/2019  
 The device was manufactured in: United States

Casa

---

  
**Security Mechanisms**

<b>Security updates</b>	Automatic - Available until at least 1/1/2022
<b>Access control</b>	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed

---

  
**Data Practices**

<b>Sensor data collection</b>	 <b>Visual</b>	 <b>Audio</b>	 <b>Physiological</b>	 <b>Location</b>
<b>Sensor type</b>	Camera	Microphone		
<b>Purpose</b>	Providing device functions, Research	Providing device functions, Research		
<b>Data stored on device</b>	Identified	Identified		
<b>Data stored on cloud</b>	Identified - Option to delete	Identified - Option to delete		
<b>Shared with</b>	Manufacturer, Third parties	Manufacturer, Third parties		
<b>Sold to</b>	Not sold	Not sold		
<b>Other collected data</b>	Movement, Account info, Payment info, Device setup info, Device tech info, Device usage info			
<b>Privacy policy</b>	<a href="http://www.NS200.example.com/policy">www.NS200.example.com/policy</a>			

---

  
**More Information**

**Detailed Security & Privacy Label:**  
[www.iotsecurityprivacy.org/labels](http://www.iotsecurityprivacy.org/labels)



## Consent mechanisms at initial setup

After purchasing a smart home product, a consumer must sign up to an IoT platform, usually through a smartphone application, in order to use the product. Oftentimes, this sign up requires a consumer to share personal information such as an email or telephone number and accept a terms of service document. Terms of service documents are the main contract between a consumer and a manufacturer. They are also considered to reflect a consumer's consent to the services that the smart home product offers.

Typically, terms of service documents are long and laden with legalese. This tends to lead consumers to skip over the terms and accept them blindly. Research from York University and Michigan State University shows that 75% of users "ACCEPTS" terms of service without reading the

text.<sup>26</sup> The 25% that try to read the text only spend on average one minute checking the text, which has several thousand words.

By updating the terms of service process and the text within these documents, the IoT ecosystem can increase the awareness of consumers, create consumer agency and improve trust. For example, one initiative called "Terms of Service; Didn't Read" examines the text of ToS and grades them according to their attitude about data collection, sharing and managing user privacy.<sup>27</sup> Besides the declaration, the initiative also shares the insights openly online. While it is tricky to balance user consent and legal responsibilities of manufacturers, it is important for policy-makers to consider a clearer terms of service process to improve consumers' trust.

# 4

## After-Market

Software updates can enable new and improved services; they can also erode trust if not properly managed.

Because smart home products are internet connected, they require software updates and data collection features that conventional products do not need. Autonomous vehicles provide analogous insights into the way connected products can incorporate software and hardware updates to maintain and enhance the value of a connected product. This is perhaps best evidenced in the way Tesla releases software updates to improve the autopilot capabilities of its cars. Within these software updates, Tesla includes features like active safety and advanced driver assistance. Through these features and the associated data collection mechanisms, insurance companies are able to offer new insurance services based on safe driving patterns.<sup>28</sup>

As Tesla created new business value out of software updates, smart home product manufacturers also could begin offering new services that consumers pay extra money too. While the potential for innovation is massive, update and data management infrastructures require regulation and standardization in order to maintain the trustworthiness of these products. Because manufacturers sell their products not only with features existing today, but the promises they give for the features that are going to be available in the future with the help of software update and data management infrastructure. Regulation and standardization mechanisms will ensure these platforms to operate with high availability and securely to deliver their promises to all their customers.

### Software updates and dynamic product management

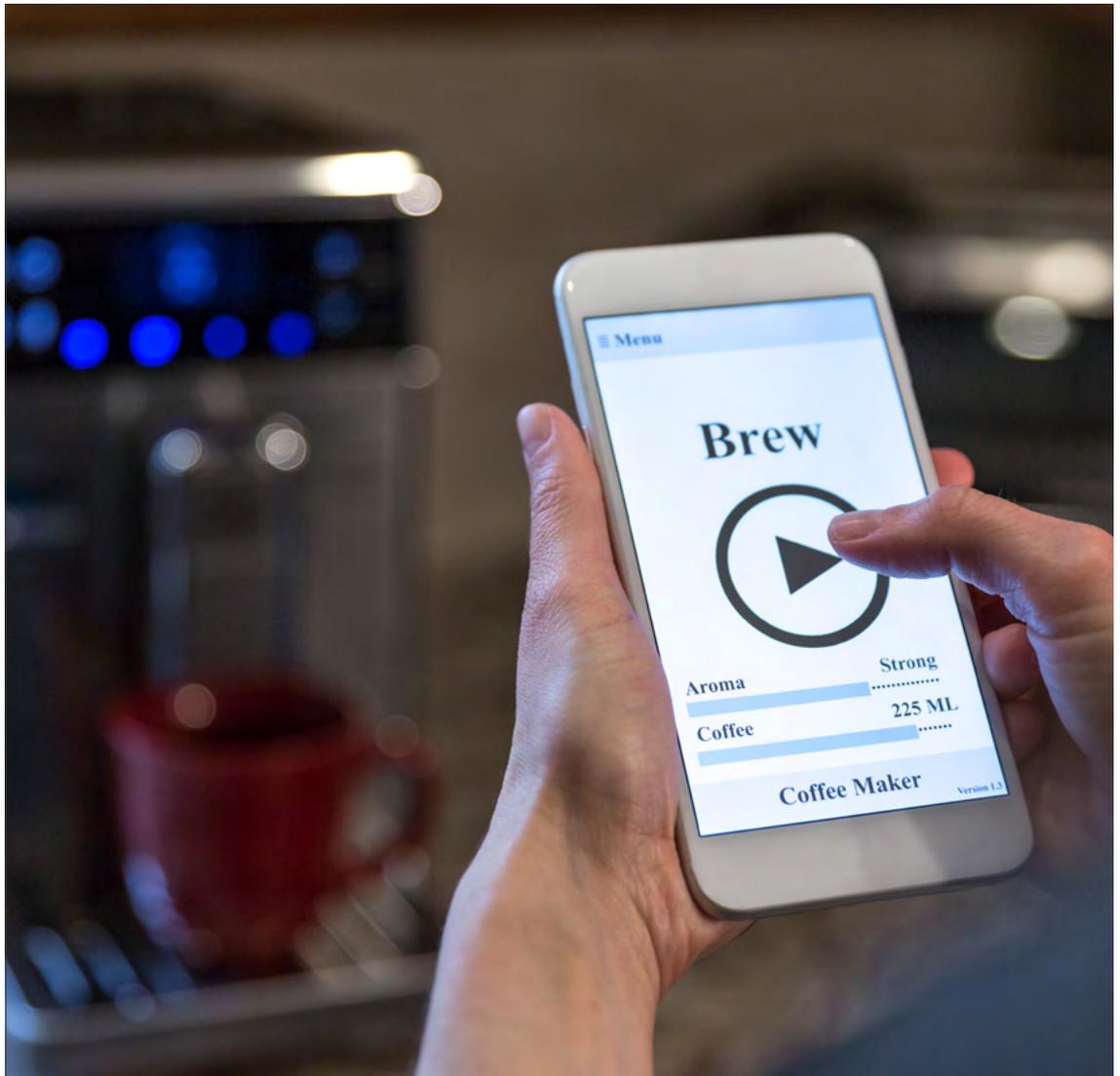
One of the most exciting capabilities of smart home products is the way they enable new feature introduction through software updates. For example, a young couple might purchase a washing machine, and then have the ability to upgrade it and include a “baby clothing” programme upon having their first child.<sup>29</sup> But, if the feature update and maintenance processes are not designed properly, customers will become upset and companies will lose credibility. Consider Sonos's recent announcement that it would stop releasing software updates for some of its products.<sup>30</sup> This created a customer backlash and degraded the value of Sonos products as people feared that their product might soon become obsolete. Eventually, the company's CEO was forced to walk back his decision and pledge to continue to provide software updates for security purposes.

This example highlights another value driver of software update for connected products: device cybersecurity. In 2016, the Mirai botnet attacked such connected devices as IP cameras and home routers, allowing it to enter and crash internet services around the world. A recent threat analysis conducted by Palo Alto Networks' Unit 42 revealed that a new version of the Mirai botnet is targeting

smart TVs.<sup>31</sup> Since cyberthreats are evolving day by day, IoT device manufacturers should have infrastructure and processes in place to protect and update devices against cyberattacks.

While the introduction of software updates enables new and improved services, it also has the potential to decrease consumer awareness, bypass meaningful consent and ultimately erode trust. Currently, there is no regulation holding smart home manufacturers accountable to a standard. This has implications for operational continuity, raising questions. How will the warranty of this IoT product be affected if the user does not download the software update? How can the user be sure that this device is updated for newly detected viruses? It is important for policy-makers to fill this gap by enacting proper guidelines to enforce industry for applying or developing proper standards for software update infrastructure.

The information technology industry has been working on these issues for some time and has developed and implemented a group of standards like ISO 27001<sup>32</sup> (Information Security Management System) and 22301<sup>33</sup> (Business Continuity Management). According to these standards,



companies must meet several requirements related to continuous operation of their IT systems throughout their operational period. By modelling this approach and defining standards

for continuous operation and cyberthreat management, policy-makers in the smart home domain can begin to build toward a more trustworthy smart home environment.

## User rights on data management

Like the Tesla insurance example, companies are spinning up new business models based on device usage data. This is usually driven by data processing within the company or by sharing data with third parties. In both cases, consumers can only participate in the process during the consent approval stage. As discussed, consent mechanisms enable a legal framework for businesses to operate, but they do not engender consumer trust. It is critical to enable some level of consumer agency over usage of data to enhance trust. For example, voice assistants have been listening to us for some time and it was not an easy task for a regular consumer to delete personal data from the platforms. In 2019, Amazon released a new software for Echo devices, and enabled consumers to delete their voice recordings

dynamically by voice commands whenever they want.<sup>34</sup> Although this implementation is a helpful improvement within the domain, there are many devices that do not allow users to delete their data immediately even if requested.

Regulations such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) mandate manufacturers to delete all data related to consumers whenever they request, but it is not easy for consumers to find an interface to request deletion. To empower consumers to manage their data, there should be standards or regulations to check the effectiveness of the consumer data rights portals of consumer IoT device manufacturers.

# Conclusion

Regulations and governance models do not need to be reinvented; the building blocks for a more trustworthy smart home exist today.

Trust is essential to realize the full potential of smart home technologies. Despite efforts by product manufacturers to build more trustworthy and secure platforms, consumer concerns persist with three-quarters of consumers expressing distrust over how their data is being shared and 28% of consumers saying they will not purchase smart devices due to security risks. To overcome these concerns, increased transparency and consumer awareness – particularly with regards to complex business models and technical solutions – is essential. New regulations, standards and governance models will need to build in trust at every stage of the product life cycle including during the design and pre-market phase, during sales and setup, and after-market.

In pre-market phases, privacy by design and security by design principles should be controlled by either certification schemes or labeling mechanisms. Moreover, the effect of business models on privacy needs to be considered in detail. Second, product marketing materials and product packages should contain information about the device's capabilities in a simpler way so that consumers can understand better. Since users need to accept a terms of service agreement before using smart home devices, consumers should be well-informed about what they are accepting during this process. Finally, maintenance of smart home products requires some extra effort to keep the device up to date and keep secure against cyberattacks. In addition, consumers

have rights to manage their personal data. Thus, device manufacturers should be able to answer users' requests like deletion or correction of data immediately via a simple and easy to use interface. All these measures seem very complex, but they are all important building blocks for a trustworthy smart home environment.

Regulations and governance related to each phase do not need to be reinvented or managed in separate frameworks. Rather, there are important efforts that has been in progress for some time like the European Telecommunications Standards Institute's ETSI 303 645,<sup>35</sup> Code of Practice for Consumer IoT Security<sup>36</sup> in the United Kingdom and National Institute of Standards and Technology's NISTIR 8259<sup>37</sup> in the United States. Second, different industries like payment or IT systems have deployed policies according to their needs too. Finally, there are also relevant academic studies like Carnegie Mellon University's labeling effort and Dartmouth College's project on security and privacy of IoT products.<sup>38</sup> All these efforts can be utilized as a baseline for a more robust and reliable smart home ecosystem for consumers to stay at home safely.

Now is the time for business, government and civil society to come together, to align their efforts and ensure that everyone can feel safe in the home of the future.



# Contributors

## Lead author

### **Burak Demirtas**

Koç Holding Fellow, Centre for the Fourth Industrial Revolution, World Economic Forum

## Acknowledgments

This white paper benefitted from the input of experts and diverse stakeholders, including, but not limited to, the following.

### **Rashid Alahmedi**

Chief Operating Officer, Dubai Electricity and Water Authority, United Arab Emirates

### **Kimmy Bettinger**

Specialist, Internet of Things, Robotics and Smart Cities, World Economic Forum

### **Tim Danks**

Vice-President, Risk Management & Partner Relations, Huawei Technologies, USA

### **William Dixon**

Head of Future Networks and Technology, Centre for Cybersecurity, World Economic Forum

### **David Kotz**

Pat and John Rosenwald Professor, Department of Computer Science, Dartmouth College, USA

### **Helena Leurent**

Director-General, Consumers International, United Kingdom

### **Katerina Megas**

Commercial Adoption Lead, Trusted Identities Group and Program Manager, Cybersecurity for Internet of Things (IoT) Program, National Institute of Standards and Technology (NIST), USA

### **Jeff Merritt**

Head of Internet of Things, Robotics and Smart Cities, World Economic Forum

### **Robert Morcos**

Founder and Chief Executive Officer, Social Mobile, USA

### **Hitomi Sano**

Associate Director, Corporate Strategy, Eisai, Japan

### **Geoff Wylde**

Lead, Internet of Things, Robotics and Smart Cities, World Economic Forum

# Endnotes

- 1 Michele W. Berger, "How the appliance boom moved more women into the workforce", PennToday, 30 January 2019, <https://penntoday.upenn.edu/news/how-appliance-boom-moved-more-women-workforce>.
- 2 Ultra-Processed Diets Cause Excess Calorie Intake and Weight Gain: An Inpatient Randomized Controlled Trial of *Ad Libitum* Food Intake. Hall KD, Ayuketah A, Brychta R, Cai H, Cassimatis T, Chen KY, Chung ST, Costa E, Courville A, Darcey V, Fletcher LA, Forde CG, Gharib AM, Guo J, Howard R, Joseph PV, McGehee S, Ouwkerk R, Raisingier K, Rozga I, Stagliano M, Walter M, Walter PJ, Yang S, Zhou M. *Cell Metabolism*. 2019 May 10. pii: S1550-4131(19)30248-7. doi: 10.1016/j.cmet.2019.05.008. PMID: 31105044. <https://www.ncbi.nlm.nih.gov/pubmed/31105044>.
- 3 Mohammed Haddad, "Coronavirus: How much more time are people spending at home?", Aljazeera, 12 April 2020, <https://www.aljazeera.com/news/2020/04/coronavirus-world-staying-home-200406122943899.html>.
- 4 Philip Prado, "Smart home tech sales could jump 30% as consumers combat the coronavirus", androidauthority.com, 1 April 2020, <https://www.androidauthority.com/coronavirus-smart-home-1101558>.
- 5 Paul Hawken, "Drawdown: The Most Comprehensive Plan Ever Proposed to Reverse Global Warming, 2017", <https://www.amazon.com/dp/B01KGZVNT0/ref=dp-kindle-redirect?encoding=UTF8&btcr=1>.
- 6 Christoph Blumtritt, "Statista Digital Market Outlook, Smart Home Report 2019", Statista.com, 1 September 2019, <https://www.statista.com/study/42112/smart-home-report>.
- 7 Consumers International, Internet Society, "The Trust Opportunity : Exploring Consumers' Attitudes To the Internet of Things", 1 May 2019, Consumers International & Internet Society, <https://www.consumersinternational.org/media/261950/thetrustopportunity-jointresearch.pdf>.
- 8 Mark McFadden, Sam Wood, Robindhra Mangtani, Grant Forsyth, "The Economics of the security of consumer-grade IoT products and services", 1 April 2019, Internet Society, [https://www.internetsociety.org/wp-content/uploads/2019/04/The\\_Economics\\_of\\_Consumer\\_IoT\\_Security.pdf](https://www.internetsociety.org/wp-content/uploads/2019/04/The_Economics_of_Consumer_IoT_Security.pdf).
- 9 Kevin Guerin, "A life cycle approach to IoT security", <https://www.riskinsight-wavestone.com/en/2019/09/life-cycle-iot-security/>, 17 September 2019.
- 10 Vigderman, Aliza, "Arlo Camera System", security.org, 6 July 2020, <https://www.security.org/security-cameras/arlo>.
- 11 Binder, Matt, "Netflix is paying to advertise on your Roku remote and you don't even know it", Mashable, 12 December 2019, <https://mashable.com/article/roku-button-home-screen-advertising>.
- 12 Hooman Mohajeri Moghaddam, Gunes Acar, Ben Burgess, Arunesh Mathur, Danny Yuxing Huang, Nick Fearnster, Edward W. Felten, Prateek Mittal, Arvind Narayanan, November 2019, Princeton.edu, <https://www.princeton.edu/~pmittal/publications/tv-tracking-ccs19.pdf>.
- 13 Bill Budington, "Ring Doorbell App Packed With Third-Party Trackers", 27 January 2020, Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers>.
- 14 Peter Bihl, "A trustmark for IoT", Thingscon, 13 September 2017, <https://thingscon.org/publications/report-a-trustmark-for-iot>.
- 15 Trend Micro, "Caught in the Crossfire: Defending Devices From Battling Botnets", 15 July 2020, <https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/caught-in-the-crossfire-defending-devices-from-battling-botnets>.
- 16 Fruhlinger, Josh, "2fa explained: How to enable it and how it works", 10 September 2019, CSOnline, <https://www.csoonline.com/article/3239144/2fa-explained-how-to-enable-it-and-how-it-works.html>.
- 17 Alex Schiffer, "How a fish tank helped hack a casino", 21 July 2017, Washington Post, <https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino>.
- 18 Common Criteria Organisation, <https://www.commoncriteriaportal.org>.
- 19 Underwriters Laboratories, <https://ims.ul.com/IoT-security-rating>.
- 20 Mozilla Foundation, <https://foundation.mozilla.org/en/privacynotincluded/about>.
- 21 IoT Security Foundation, <https://www.iotsecurityfoundation.org/iotsf-issues-update-to-popular-iot-security-compliance-framework>.
- 22 Internet Society, <https://www.internetsociety.org/resources/doc/2018/iot-trust-by-design>, 22 May 2018.
- 23 Lily Hay Newman, "IoT Security Is a Mass. Privacy 'Nutrition' Labels Could Help", 9 June 2020, Wired, <https://www.wired.com/story/iot-security-privacy-labels>.
- 24 Andrea Coravos, Megan Doerr, Jennifer Goldsack, Chirstine Manta, Mark Shervey, Beau Woods, William A Wood, 2 April 2020, Nature.com, <https://www.nature.com/articles/s41746-020-0237-3#Fig2>.
- 25 Sidewalk Labs, 19 April 2019, Sidewalks Labs GitHub Repository, [https://github.com/sidewalklabs/dtpr/blob/master/dtpr\\_designguide/DTPR\\_Design\\_Guide.pdf](https://github.com/sidewalklabs/dtpr/blob/master/dtpr_designguide/DTPR_Design_Guide.pdf).
- 26 Jonathan A. Obar, Anne Oeldorf-Hirsch, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services", 18 August 2018, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2757465](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465).
- 27 Terms and Service Didn't Read, <https://tosdr.org/index.html>.

- 28 Tesla, <https://www.tesla.com/support/insurance>.
- 29 LG, <https://www.youtube.com/watch?v=AYVWqfJaR3o>.
- 30 SONOS, <https://blog.sonos.com/en/end-of-software-updates-for-legacy-products>.
- 31 Ruchna Nigam, 18 March 2019, "New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems", Palo Alto Networks, <https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems>.
- 32 International Organization for Standardization, <https://www.iso.org/isoiec-27001-information-security.html>.
- 33 International Organization for Standardization, <https://www.iso.org/standard/50038.html>.
- 34 Jason Cipriani, 29 May 2019, "Amazon Echo stores your voice commands. Here's how Alexa can delete them", C|net, <https://www.cnet.com/how-to/amazon-echo-stores-your-voice-commands-heres-how-alexa-can-delete-them>.
- 35 European Telecommunications Standardization Institute, [https://www.etsi.org/deliver/etsi\\_en/303600\\_303699/303645/02.00.00\\_20/en\\_303645v020000a.pdf](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf).
- 36 Department for Digital, Culture, Media & Sport, "Code of Practice for Consumer IoT Security", October 2018, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/773867/Code\\_of\\_Practice\\_for\\_Consumer\\_IoT\\_Security\\_October\\_2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf).
- 37 Michael Fagan, Katerina N. Megas, Karen Scarfone, Mathew Smith, "Foundational Cybersecurity activities for IoT device manufacturers", National Institute of Standards and Technology, 1 May 2020 <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf>.
- 38 Security and Privacy in the Lifecycle of IoT for Consumer Environments (SPLICE), <https://splice-project.org>.



---

COMMITTED TO  
IMPROVING THE STATE  
OF THE WORLD

---

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

---

**World Economic Forum**  
91–93 route de la Capite  
CH-1223 Cologny/Geneva  
Switzerland

Tel.: +41 (0) 22 869 1212  
Fax: +41 (0) 22 786 2744  
contact@weforum.org  
www.weforum.org