“Nobody’s Happy”: Design Insights from Privacy-Conscious Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control

Sunyup Park*, Anna Lenhart*, Michael Zimmer**, Jessica Vitak*
*University of Maryland, College Park
**Marquette University

SOUPS presentation on August 8, 2023

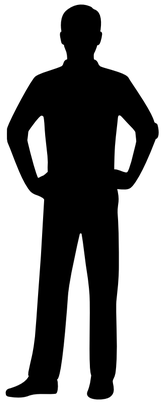
“I think we’re in this really weird state, where specific to smart home technology, it’s a little too basic for the IT technology nerds, and a little too complex for the run of the mill user. So, nobody’s happy.” (P29)

Smart home devices raises privacy concerns to diverse stakeholders

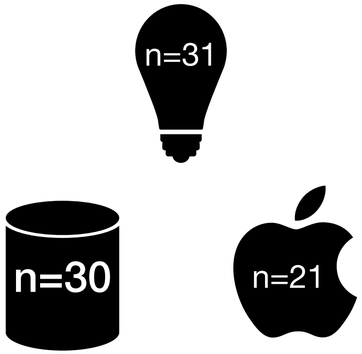
Image from https://www.stuff.tv/features/best-smart-home-devices/

Focus groups with 32 *privacy-conscious power users*

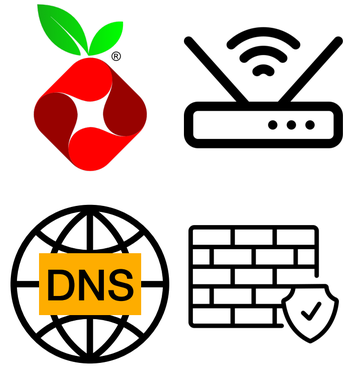
RQs: Challenges and ideas to make their smart home private and secure.



Mostly white (n=23), male (n=25), mid-30s (avg 36 yrs old)



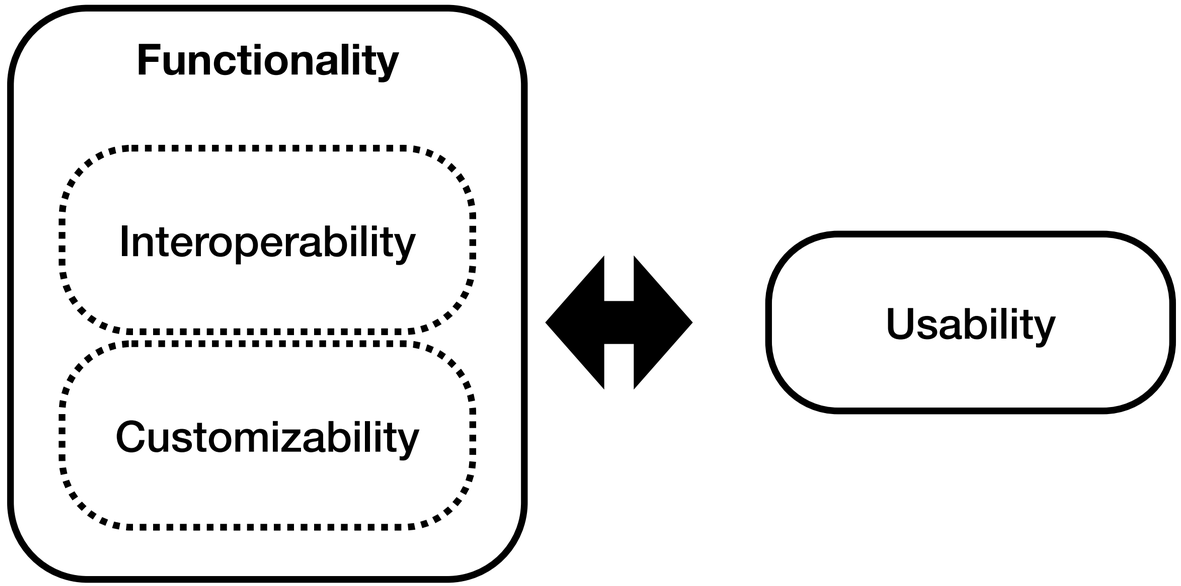
Smart home device and integration platform



Advanced network management (n=16)

Balancing functionality and usability

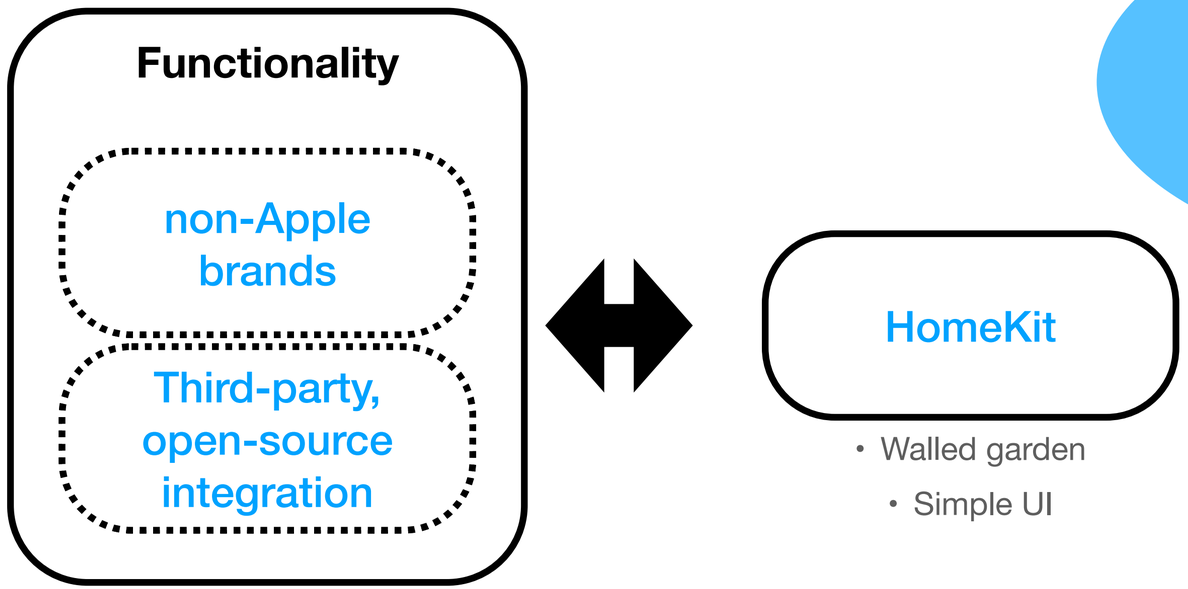
Facing trade-offs due to conflicting needs



Balancing functionality and usability

Facing trade-offs due to conflicting needs

It [Amazon Echo] wasn't my first choice for a smart device, but its capabilities were better than what I could find with my first choice [HomePod]. (P4)

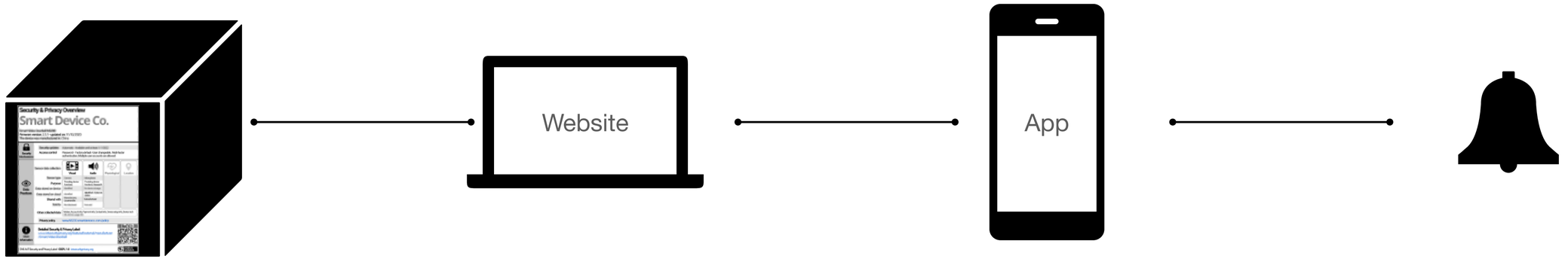


I'm sacrificing a lot of potential functionality and incurring greater cost for the sake of being in a more private environment. (P13)

It was a little frustrating because I wanted to get those [Nest thermostats] in HomeKit, which isn't super easy to do. So we've been using HomeAssistant to bridge everything together. (P21)

Data transparency in multiple consumer touchpoint

Information from objective sources, information about company/brand structures

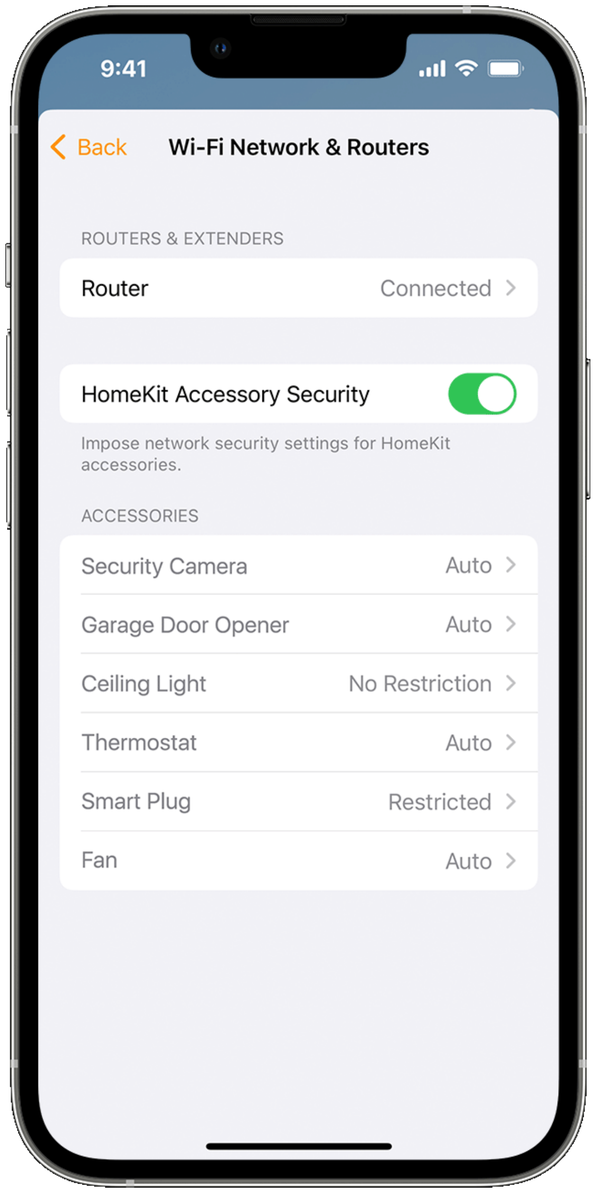


CMU IoT Security and Privacy Label

Visibility of devices and data

In a centralized visualization tool

- Device location and status
- Device commands and controls
- Filter function is important

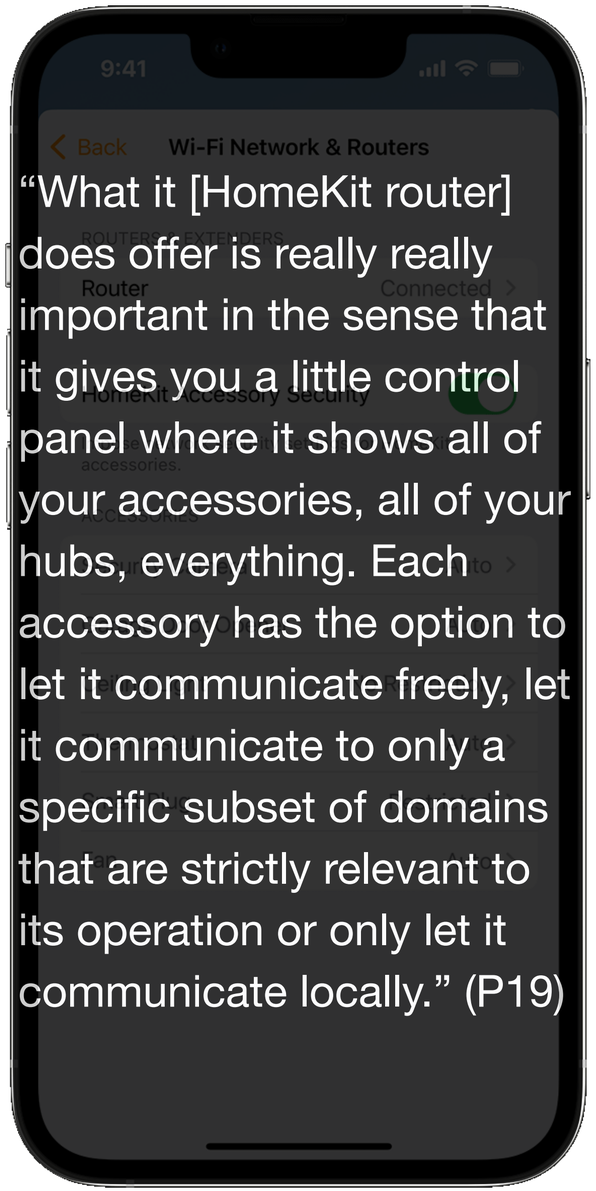


https://support.apple.com/en-us/HT210544

Visibility of devices and data

In a centralized visualization tool

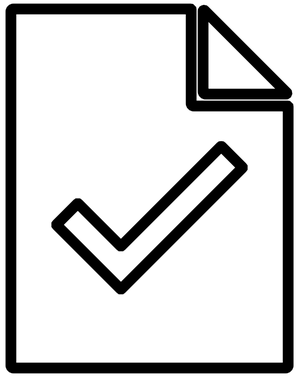
- Device location and status
- Device commands and controls
- Filter function is important

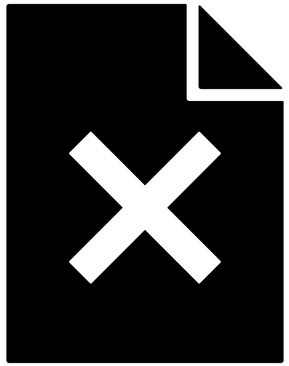


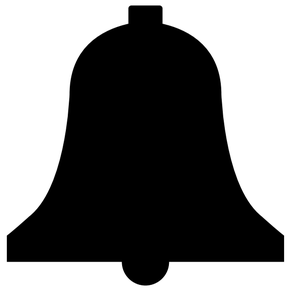
https://support.apple.com/en-us/HT210544

Data control

Network management (white/black list) and notifications.



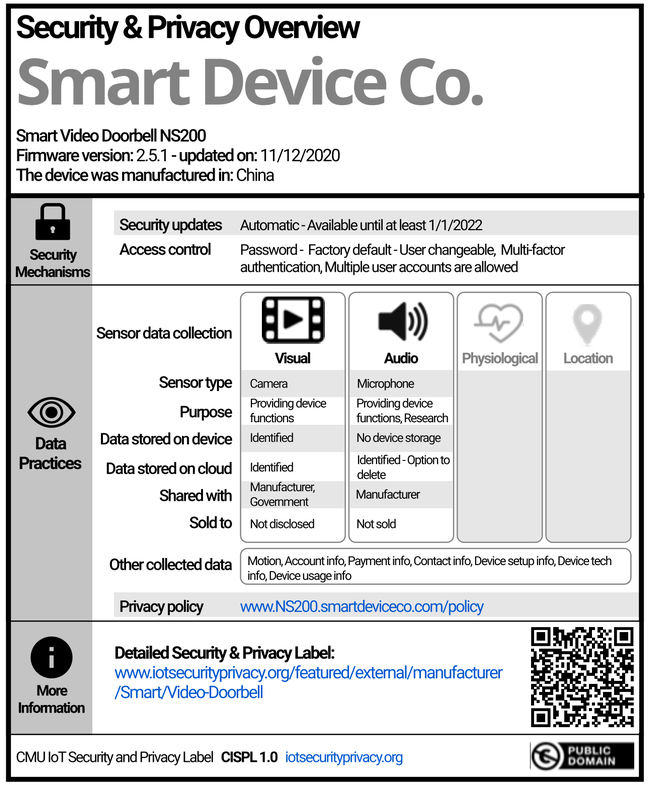


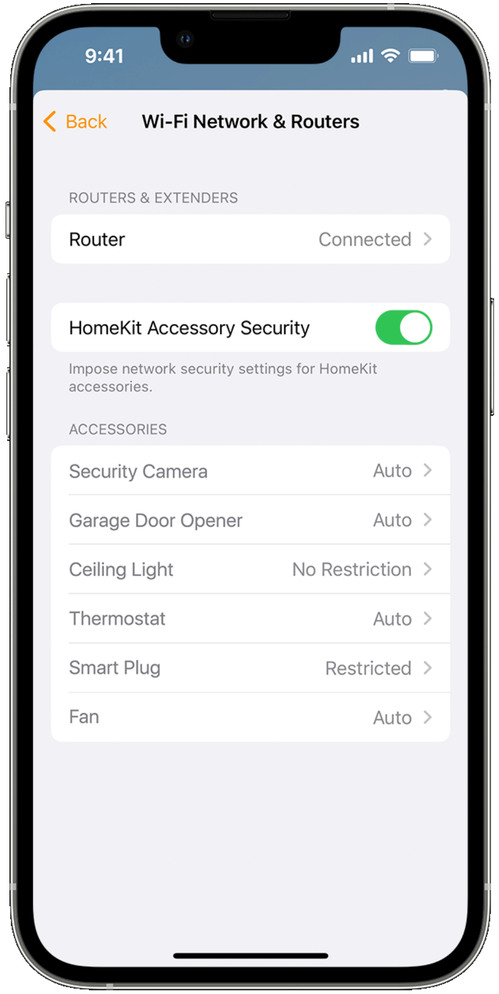


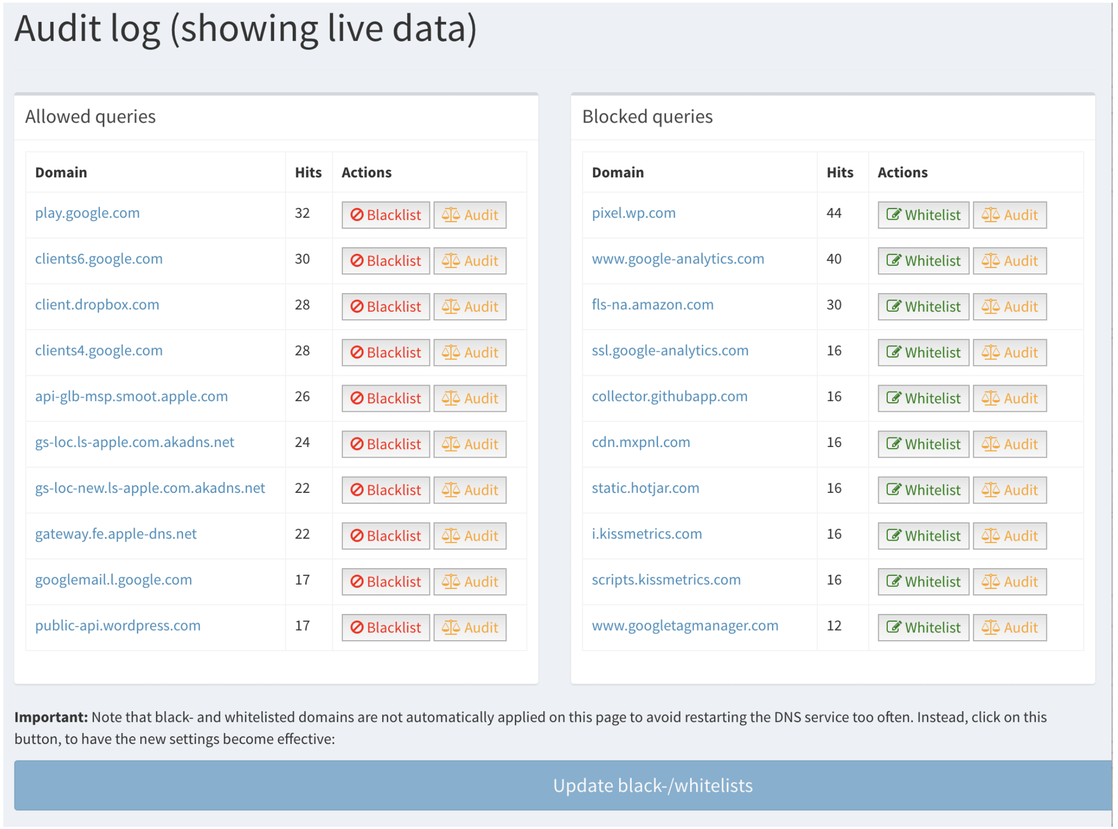
“I went and just [black listed] it [unnecessary endpoints] from my router so that it can only talk within my network, but it can’t reach out and talk to anybody outside.” (P25)

Consideration of non-power users

How to make these usable?

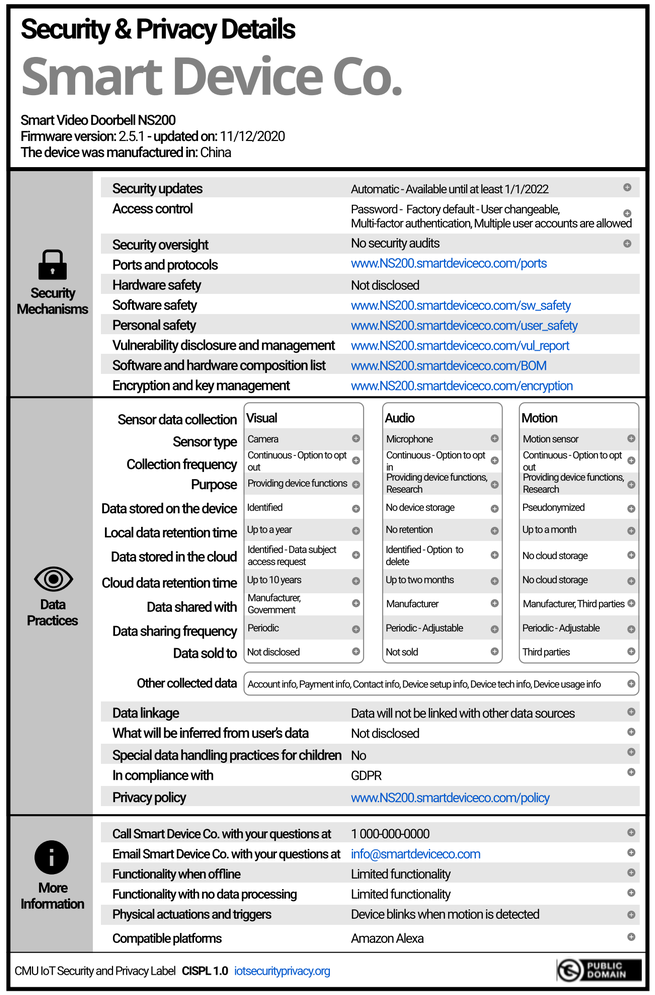






Consideration of non-power users

How to make these usable?



Security & Privacy Details

Smart Device Co.

Smart Video Doorbell NS200
Firmware version: 2.5.1 - updated on: 11/12/2020
The device was manufactured in: China

Security Mechanisms

Security updates	Automatic - Available until at least 1/1/2022
Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed
Security oversight	No security audits
Ports and protocols	www.NS200.smartdeviceco.com/ports
Hardware safety	Not disclosed
Software safety	www.NS200.smartdeviceco.com/sw_safety
Personal safety	www.NS200.smartdeviceco.com/user_safety
Vulnerability disclosure and management	www.NS200.smartdeviceco.com/vul_report
Software and hardware composition list	www.NS200.smartdeviceco.com/BOM
Encryption and key management	www.NS200.smartdeviceco.com/encryption

Data Practices

	Visual	Audio	Motion
Sensor data collection	Camera	Microphone	Motion sensor
Sensor type	Continuous - Option to opt out	Continuous - Option to opt in	Continuous - Option to opt out
Collection frequency	Providing device functions	Providing device functions, Research	Providing device functions, Research
Purpose	Identified	No device storage	Pseudonymized
Data stored on the device	Up to a year	No retention	Up to a month
Local data retention time	Identified - Data subject access request	Identified - Option to delete	No cloud storage
Data stored in the cloud	Up to 10 years	Up to two months	No cloud storage
Cloud data retention time	Manufacturer, Government	Manufacturer	Manufacturer, Third parties
Data shared with	Periodic	Periodic - Adjustable	Periodic - Adjustable
Data sharing frequency	Not disclosed	Not sold	Third parties
Data sold to			

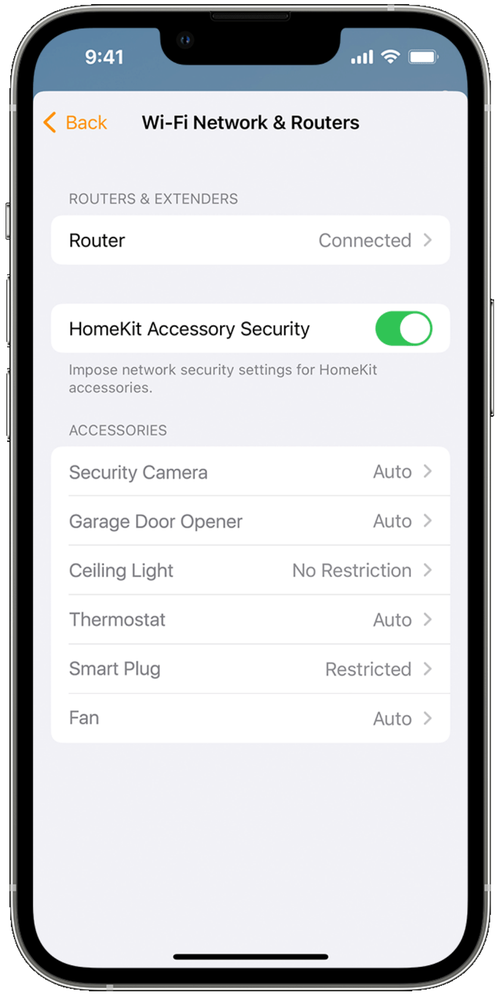
Other collected data: Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info

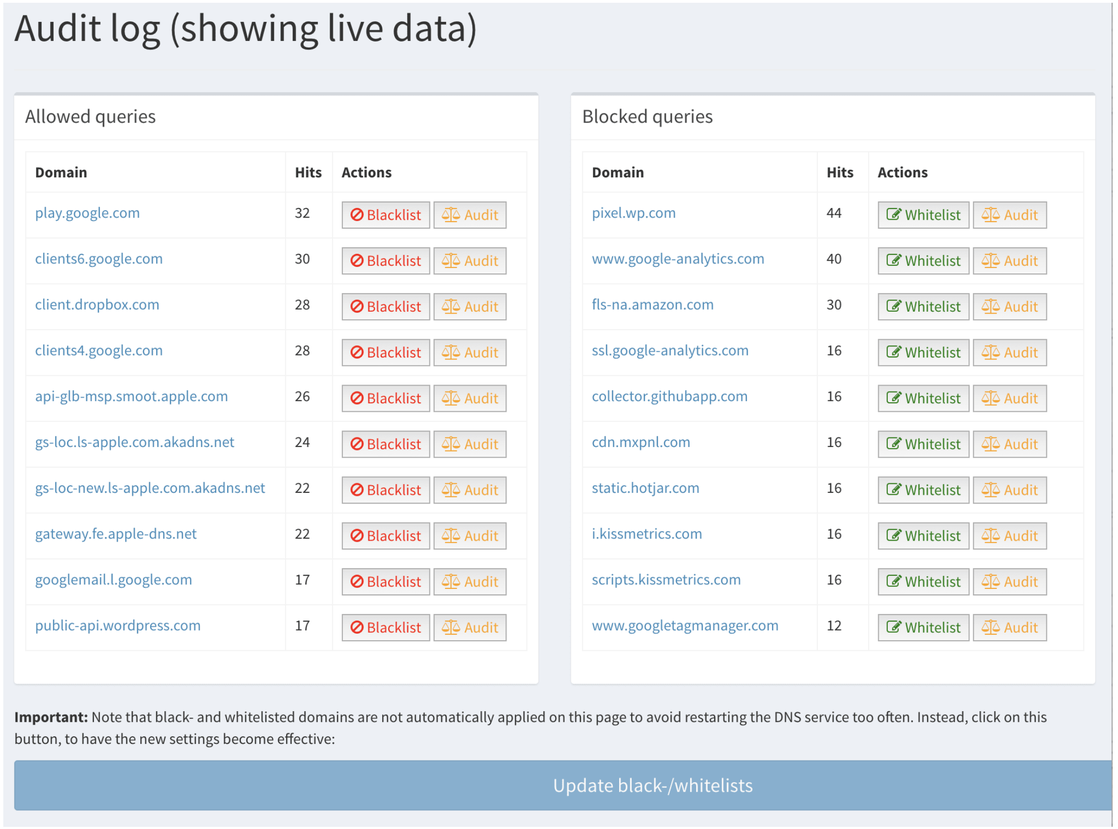
Data linkage	Data will not be linked with other data sources
What will be inferred from user's data	Not disclosed
Special data handling practices for children	No
In compliance with	GDPR
Privacy policy	www.NS200.smartdeviceco.com/policy

More Information

Call Smart Device Co. with your questions at	1 000-000-0000
Email Smart Device Co. with your questions at	info@smartdeviceco.com
Functionality when offline	Limited functionality
Functionality with no data processing	Limited functionality
Physical actuations and triggers	Device blinks when motion is detected
Compatible platforms	Amazon Alexa

CMU IoT Security and Privacy Label **CISPL 1.0** iotsecurityprivacy.org PUBLIC DOMAIN





Audit log (showing live data)

Allowed queries

Domain	Hits	Actions
play.google.com	32	Blacklist Audit
clients6.google.com	30	Blacklist Audit
client.dropbox.com	28	Blacklist Audit
clients4.google.com	28	Blacklist Audit
api-glb-msp.smoot.apple.com	26	Blacklist Audit
gs-loc.ls-apple.com.akadns.net	24	Blacklist Audit
gs-loc-new.ls-apple.com.akadns.net	22	Blacklist Audit
gateway.fe.apple-dns.net	22	Blacklist Audit
googlemail.l.google.com	17	Blacklist Audit
public-api.wordpress.com	17	Blacklist Audit

Blocked queries

Domain	Hits	Actions
pixel.wp.com	44	Whitelist Audit
www.google-analytics.com	40	Whitelist Audit
fls-na.amazon.com	30	Whitelist Audit
ssl.google-analytics.com	16	Whitelist Audit
collector.githubapp.com	16	Whitelist Audit
cdn.mxpnl.com	16	Whitelist Audit
static.hotjar.com	16	Whitelist Audit
i.kissmetrics.com	16	Whitelist Audit
scripts.kissmetrics.com	16	Whitelist Audit
www.googletagmanager.com	12	Whitelist Audit

Important: Note that black- and whitelisted domains are not automatically applied on this page to avoid restarting the DNS service too often. Instead, click on this button, to have the new settings become effective:

Update black-/whitelists

Policy Matters

“How do we balance doing more of this [adding more devices] without it being a burden for ourselves? If something’s not working at one point or a burden in terms of privacy, we still want to make sure that we’re keeping our stuff private as much as possible in this day and age.” (P17)

Thank you! Questions?

sypark@umd.edu

COLLEGE OF
INFORMATION
STUDIES

MARQUETTE
UNIVERSITY

BE THE DIFFERENCE.