

Smart Homes

Raul Camilo, Catherine Javadian, and Matthew Markowitz

Article Summary

- Smart Home Technologies are designed to serve their manufacturers
 - Amazon Alexa
 - Google Nest
- Google and Amazon have filed patent applications that expand the abilities of their devices to monitor
 - Even when not directly addressed
- Cannot rely on regulators
 - Consumers must fight back by never buying these devices in the first place

Background

- Amazon Alexa
 - Speaker attached to a microphone
 - Perform commands (playing music, browsing the web)
- Google Nest
 - Collection of devices
 - Automate various aspects of the home (controlling the thermostat, monitoring for intruders)



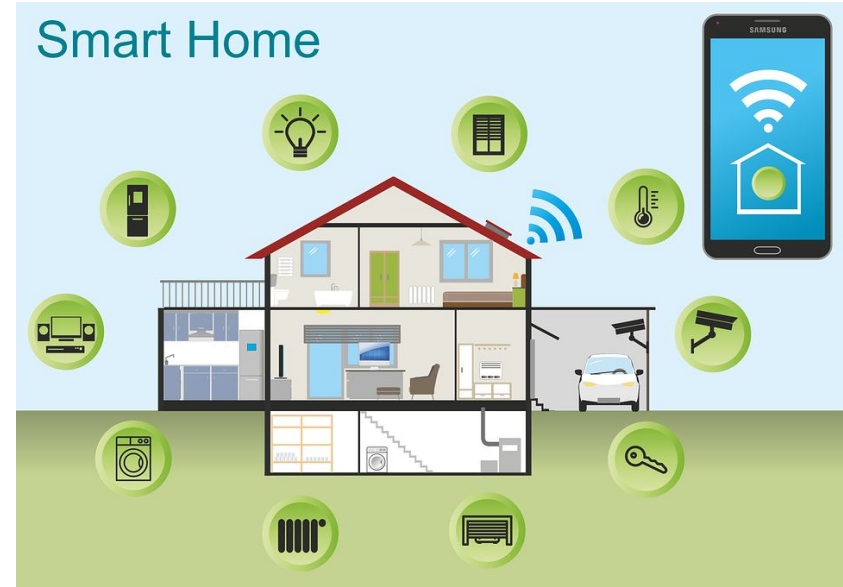
Common Smart Devices

- Home assistant (Amazon Alexa, Google Assistant)
- Heating system (Ecobee4)
- Fridge (GE, Kenmore)
- Lighting (Phillips Hue)
- Security System (Nest)
- Vacuums (Roomba)



How do they work?

- Located around the house
 - Connected via wireless/wired network
- Controlled using a smartphone, computer, or home assistant
- Learn user patterns over time and automate processes



The Rise of Smart Devices

- Household penetration is 32.0% in 2018 in the US
 - Expected to hit 53.1% by 2022 in the US
- Market expected to grow annually by 17 percent and become a \$58.68 billion industry by 2020
- 70% of people with smart home technology would buy another device
- Integrating into people's everyday lives
 - Learning about their habits and behaviors

Stakeholders

- Consumers
- Device Manufacturers
 - Amazon, Google, etc.
- Law Enforcement

Advantages for Each Stakeholder

- Consumers
 - Convenience
 - Optimizing appliances and energy
 - Saving money on bills
- Device Manufacturers
 - Monetary gain
 - Understanding its consumers and collection of data
 - Seeing how users interact with the device
- Law Enforcement
 - Surveillance
 - Can be used in cases

Disadvantages For Each Stakeholder

- Consumers
 - Decreased privacy
 - Security concerns
 - Transparency of data collection
 - Amazon's Echo - "release account and other personal information when we believe release is appropriate to comply with the law"
- Device Manufacturers
 - Remain liable for damages that may occur
 - Security vulnerabilities
 - Implications with 1st and 4th Amendment rights
- Law Enforcement
 - Unexplored field that must be legislated
 - Implications with 1st and 4th Amendment rights

Major Impacts

- Can provide undeniably useful features
 - Automatically adjusting the thermostat
 - Effective security features
- Adoption and surveillance
 - Government sought data on 525 Nest account holders
 - ~20% of cases were approved
 - Private information about home life
 - Increasing presence in society

Positive Impact Case Study

- In New Mexico, a man named Eduardo Barrios got into a domestic dispute with his girlfriend.
- A currently unidentified smart home device called 911 in response to threatening statements that it heard.
- SWAT officers arrived at their home, and found Barrios wielding a firearm.
- The officers were then able to de-escalate the situation and bring the woman and daughter to safety.
- This smart home device could have potentially saved the woman and daughter's life.

Negative Impact Case Study

- Security researchers at Microsoft explored the security of Samsung SmartThings devices.
- These researchers made many interesting discoveries.
 - Since the security of devices are tied to account credentials, the theft of these credentials could put user's security at risk (for example, by making a fake login page for the smart devices).
 - Permission exploits in the app sdk can allow attackers to perform malicious acts such as the theft of a user's door pin.
- Since even traditional locks can be attacked (lock picking) does using smart home devices for security necessitate more risk than what is already considered acceptable?

Future

- Smart home technology will be included with the real estate cost of houses
- Water, electricity, and energy consumption will be reduced as devices become better adjusted to consumer's schedules
- New devices will become IoT devices and can be vulnerable to attacks
- Machines will be able to detect hardware problems early on and alert user
- Data collected from these devices will produce ads that are more personalized to each individual
- Energy consumption from these devices in many homes may overload power grids

Ethical Dilemmas

- What are our rights when it comes to privacy with smart homes?
 - Privacy Paradox
 - 4th Amendment
- Does the convenience of smart home devices outweigh security?
 - Explicit consent
- How do we feel about smart home devices learning our habits and behaviors?
- Is it possible that smart home devices will know us better than the most significant people in our lives?

Stances

- Convenience of smart home devices outweigh privacy concerns
 - Improving everyday life
 - Smart home device calling 911 when threatening comments are heard
- Privacy regulations should be implemented
 - Transparency between consumers and manufacturers
 - Mutual agreement of what the standards for privacy are
- Smart home devices should be banned all together
 - More harm than good
 - Theft of credentials and personal information

Codes of Ethics

- No standard code of ethics for the internet of things
- Francine Berman and Vinton Cerf drafted a list of aspects that will need to be considered for the development of an IoT code of ethics
 - What are user's rights to privacy in the IoT?
 - Who holds accountability for decisions that are made by autonomous systems?
 - How can ethical practices of IoT be promoted?
- A standard code of ethics should be implemented sooner rather than later to help advance the field

Sources

- <https://techcrunch.com/2018/06/03/will-smart-home-tech-make-us-care-more-about-privacy/>
- <https://www.forbes.com/sites/thomasbrewster/2018/10/13/smart-home-surveillance-governments-tell-googles-nest-to-hand-over-data-300-times/#7b3d04262cfa>
- <https://medium.com/viewpoints/smart-devices-are-exploiting-our-convenience-we-shouldnt-let-them-5288698acfdf>
- <https://www.the-ambient.com/features/smart-home-device-sales-estimates-442>
- <https://www.ahs.com/home-matters/real-estate/smart-homes-grow-demand/>

Sources Cont.

- <https://www.sciencealert.com/a-smart-home-speaker-may-have-saved-a-life-by-calling-cops-to-a-domestic-dispute>
- <https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/>
- <https://cacm.acm.org/magazines/2017/2/212443-social-and-ethical-behavior-in-the-internet-of-things/fulltext>
- <https://www.futureofeverything.io/future-smart-home-technology/>