moz://a Internet Health Report

*Privacy Included: Rethinking the Smart Home

Special Edition

November 2019

moz://a Internet Health Report

*Privacy Included: Rethinking the Smart Home

Special Edition

November 2019

Credits

Editorial team: Solana Larsen, Sam Burton, Kasia Odrozek, Stefan Back, Jairus Khan
Illustrations: Xenia Latii
Print design: Agency of None

Thank you to all the topic experts and allies from a wide variety of disciplines who generously contributed ideas to this publication through interviews and in writing.

Stefan Baack, Owen Bennett, Cathleen Berger, Peter Bihr, Ashley Boyd, Lyall Bruce, Georgia Bullen, Sam Burton, Jen Caltrider, Bofu Chen, Irvin Chen, Kelly Davis, Selena Deckelmann, Ame Elliott, Felipe Fonseca, Ben Francis, Kathy Giori, Tony Gjerulfsen, Davide Gomba, Max von Grafenstein, Lisa Gutermuth, Jofish Kaye, Jairus Khan, Solana Larsen, Xenia Latii, Ben Moskowitz, Kasia Odrozek, Steve Penrod, Abigail Phillips, Bobby Richter, Becca Ricks, Chris Riley, Jon Rogers, Christiane Ruetten, Nicole Shadowen, Genia Shipova, Kevin Su, Peyton Sun, Mark Surman, James Teh, Michelle Thorne, Sofia Yan, Tammy Yang, Sarah Zatko

Copyright

Foreword

This special edition of the Internet Health Report is published as a companion to Mozilla's 2019 ***Privacy Not Included** buyer's guide. It is based on conversations with more than two dozen people working from different angles to better the global ecosystem for smart home devices.

The Internet Health Report is an open source publication that documents and explains the health of the internet across five issues: **decentralization**, **privacy and security**, **openness**, **web literacy**, and **digital inclusion**. The most recent annual version was published in April 2019.

Index

Feedback or comments?
Email us at internethealth@mozillafoundation.org

*Privacy Included

How Smart Homes Could be Wiser

The market for smart home devices is fraught with insecurity and privacy risks. If devices were designed with **privacy**, **security**, **interoperability** and **sustainability** in mind, things would be better. **But how?**

Jump to Solutions

It all started with a container of milk going bad in the refrigerator. Again.

As a software developer in Taipei, Taiwan who works long hours, Tammy Yang started dreaming of having a 'smart refrigerator' with a camera that would let her peek inside remotely from her phone. *"I would always forget what I had in the fridge,"* she laughs.

But when she started researching what to buy in 2017, she realized that regardless of whether she bought a connected refrigerator or a camera to mount inside, most options on the market involved sending data to 'the cloud'. *"I found it a bit creepy,"* she says. *"If I decide to drink a coke or a glass of milk at midnight, I just don't like the idea of my photo being uploaded to a cloud computer somewhere."*

It may be hard to imagine why information about something as basic as what you eat, or when you turn on the lights is valuable, but it's the kind of data that tells a story about when you are home and who you are. Extensive new research to monitor smart home devices in 2019 has revealed astonishing information about the types and quantities of personal data that are transmitted out of the home. Consumers aren't just oblivious to what smart doorbells or televisions know about them, they are frequently never told or given control over how their data will be shared or used for machine learning.

Considering how fun (and useful) it can be to see everyday objects come to life, it's no surprise that privacy concerns are often dismissed. But it is actually possible to create smart devices that are both fun and healthy for the smart home ecosystem. Why so few currently are, traces back to how devices are created, how the market is regulated, and what consumers and product developers themselves have come to terms with as an acceptable risk of convenience and low cost.

Few developers recognize how closely privacy and security are interrelated, or that security alone is not enough to create a good product, says Kathy Giori, a staff evangelist at Mozilla with years of experience at tech companies, including Qualcomm and Arduino. *"Every IoT workshop and conference I go to focuses only on security,"* she says. *"What about privacy? What about cross-brand interoperability? Without this, I don't want the device, no matter how secure it is."*

People want to know what is safe to buy, but unfortunately, it's tricky for internet health experts to wholeheartedly recommend IoT products. *"There really just aren't that many products to recommend, depending on how harshly you want to judge,"* says Peter Bihr, co-founder of the international ThingsCon community *"for fair, responsible, and human-centric technologies."*

What can be done? We know that if more devices were designed with privacy, security, interoperability and sustainability in mind things would be better. This article explores seven key areas for solutions, and summarises them on a 'cheat sheet' at the end.

Improving the situation requires action on different levels, starting with the architecture of the devices themselves, how they are marketed and sold, and what rules govern the data they can transmit. Fortunately, because of the known risks, many developers, security experts, consumer groups and policy makers are working on solutions to make smart homes wiser.

Make your own things

Since Tammy Yang couldn't find a smart fridge that met her privacy needs, she decided to develop something herself. In 2017, she worked with a small team to create an open source, privacy-centric software called BerryNet that can do simple artificial intelligence (AI) processing directly on a device, without sending data to a cloud server.

In 2019, they created a hardware prototype for a camera home security system they call AIKEA and launched a Kickstarter campaign to cover manufacturing costs. The BerryNet team say their intention is mainly to offer a proof of concept and inspiration to others. *"We want to democratize the technology so people can build good projects,"* says Yang's colleague Bofu Chen.

If you really want to be in control of your data, this is one option: shun smart home devices from big companies like Amazon, Google, and Samsung, and build something that works on a local network yourself. There are open hardware, open design and maker communities worldwide and a plethora of inexpensive sensors, cameras and circuit boards like Raspberry Pi and Arduino.

Unfortunately, this doesn't help the average consumer who expects things to work out of the box. In today's booming market for IoT devices, people are confronted with an overwhelming array of product options, including thousands of cheap, generic devices that make their way up the retail chain under different brand names worldwide. But there is good advice to be found.

Rate more products on privacy and security

Becca Ricks has reviewed dozens of smart home products as a researcher for Mozilla's annual *Privacy Not Included buyer's guide. Based on privacy policies, app permissions, news reports and more, Mozilla assesses around 70 products in November 2019 against a set of Minimum Security Standards developed in partnership with Consumers International and Internet Society.

The purpose of these standards is to identify and promote practices that can help prevent the worst IoT privacy and security failings. But assessing whom to trust is still complex to untangle. *"Products sold by big companies like Amazon or Google can do security really well, but can also be the worst offenders in terms of privacy because of the data they collect,"* says Ricks. On the flip side, big companies can be preferable to niche ones with few security resources, she says.

Few mainstream product reviewers rate products on privacy and security, let alone interoperability and sustainability. But they could. *"I think consumers have started to demand better products, and that we'll soon see better products as a result,"* says Bihr. Taking inspiration from organic food certification and fair trade labels, Bihr launched an experimental Trustable Technology Mark in 2017 (with some Mozilla support) that has so far welcomed two products.

Consumer advocacy groups in a number of countries have been working to define their role in the context of smart devices, which in contrast contrary to a non-digital product, like shampoo, can change after it arrives in your home by virtue of being connected to the internet. How to track the security of a product over a longer period of time is something Consumer Reports in the United States first began exploring as part of a collective effort to develop a Digital Standard for privacy and security in 2017 together with Disconnect, Ranking Digital Rights, and The Cyber Independent Testing Lab.

The work has since culminated in the launch of a Digital Lab in 2019 funded by a $6 million USD grant from Craig Newmark Philanthropies. According to Consumer Reports, the lab is currently developing new methods for testing the privacy and security of digital devices, including routers and printers, as well as online services and platforms, like Amazon, Google and Facebook. Investigations into security flaws have directly resulted in fixes in the past, say Consumer Reports.

Demand more interoperability

With more smart devices entering the home, it's more of an ecosystem of devices than individual products.

Beyond privacy and security, seek even wiser smart home devices

A metaphor to wrap your mind around: the four-legged chair of the smart home.

Mozilla's Minimum Security Standards identify practices that help prevent the worst privacy and security failings in the Internet of Things (IoT). But that's just two legs of the chair. Even wiser devices for a healthy IoT ecosystem should incorporate interoperability and sustainability too.

Privacy

Is privacy at the core of its design? Is it easy to understand how it collects, processes, or shares data? Does it give real control over what data is shared? For example, is not sharing any data at all an option?

Security

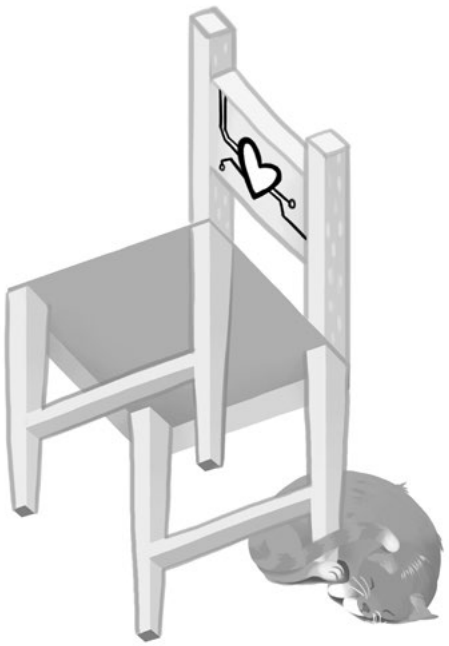
Does it encrypt all communications? Does it automatically support security updates? Does it require the use of strong passwords or two-factor authentication?

Interoperability

Does it use open standards or does it lock you into a specific brand or proprietary software and product family, like Amazon Alexa, Google Assistant, or Apple's HomeKit?

Sustainability

Is it designed to last or to be cheap and disposable? Is it commercially viable or will it soon end up 'bricked'? If installed in a home, can you easily and privately transfer ownership to someone else?



Kathy Giori, product developer on Mozilla's WebThings team:

"When I go to IoT events, the 'security' buzzword is all the rage, but no one ever mentions the three other legs of a chair needed for a decent smart home offering: privacy, interoperability, and sustainability. I wish more people would realize what happens when a consumer sits on that chair if it's missing one or more legs."

Predictably, because it happens in other realms too, big tech companies like Amazon, Apple, Google and Samsung see opportunities to shape the market to their own benefit and are each developing their own proprietary platforms as a mechanism to compete. In practice, that means your Amazon devices may not pair up with Google ones or interact with things you create yourself.

When companies lock buyers into *"product families"* they typically gain access to even more data about buyers for every additional product acquired of the same brand. This gives them a fuller portrait of users, which it uses to further develop commercial products and algorithms.

Pushing back on consolidation of power, and especially for the interoperability of different products via local networks (instead of always in the cloud) is likely to influence whether smaller-scale and more privacy-focused alternatives have the chance to co-exist. Jon Rogers, a professor of creative technology at the University of Dundee in Scotland says the vision for IoT products should be to become *"... like standard bike seats that just fit onto every bike."*

Drawing inspiration from the open web, Ben Francis, a staff software engineer at Mozilla has helped lead an effort to propose an open standard for IoT to a W3C working group for the Web of Things that includes Intel, Samsung, and Oracle as members. If adopted, it could enable World Wide Web technology itself to be a connector between different types of devices (breaking what he calls *"proprietary silos"*). *"It's a years long process for a standard to be adopted,"* says Francis. But he believes it would benefit the

Data about our bodies is about as personal and intimate as it gets. Here are two products designed to help us know our bodies better that earned high marks in Mozilla's *Privacy Not Included guide.

Withings
Body Scale

These scales don't just measure weight, but can also track other information like your heart rate, bone and muscle mass, or water retention. This can be very useful, but also very personal information. Withings promises that any data collected will not be shared with third parties.

Lioness
Vibrator

Mozilla reviewed this connected vibrator in 2018. It is designed to help women learn what gives them pleasure, by displaying data about orgasms in a smartphone app. Lioness is clear about how they treat data: encrypting databases, fully anonymizing user data, and they have built-in informed consent.

entire industry by making products more widely useful. He sees competing efforts to create formal IoT standards as a setback for consumers, and hopes the industry will eventually converge on a smaller number of data formats and protocols.

Mozilla's WebThings Gateway project puts the idea of a bridge between different devices into practice with a simple hub for controlling devices in a web browser, while maintaining private data inside a local network. In the past decade, open source communities have produced numerous home automation hub projects addressing aspects of the problem, from openHAB to the new and rapidly growing Home Assistant that works with over 1,400 products. Where WebThings Gateway is still unique is in bridging devices to a proposed web standard rather than an internal API.

One company that has made being interoperable and modular central to its mission is Snips, a French company that develops an open source AI voice platform for connected devices that (for relatively simple tasks) doesn't require internet access or any cloud processing or storage.

Business models matter

In early 2018, Snips announced it would be launching a privacy-focused alternative to Amazon's Alexa and Google Assistant. *"We're making a very strong bet on people's willingness to trade, basically, a recognized brand for privacy,"* CEO and co-founder Rand Hindi told Fast Company at the time. But Snips's first steps into consumer hardware production were short-lived. Genia Shipova, vice president of marketing operations and communications says they saw greater interest from investors in business-to-business solutions and chose that route instead.

To makers of coffee machines, watches and any other objects that can be voice controlled, Snips offers custom solutions. Among their advantages, says Shipova, is that Snips charges a one-time fee per device, while voices from Amazon and Google charge per voice query. That means there are no variable ongoing costs, and no need for data sharing with Snips. For prototyping and for non-commercial use, Snips is free, which makes it popular among open hardware makers.

That AI 'on device' technology is gaining favor among mainstream product developers, including Qualcomm and Apple, has more to do with opportunities for mobile data efficiency and low power consumption than with privacy. Cloud computing is the core infrastructure for most of what humans and machines currently do online, and it has many advantages. For instance, it can make it easy to remote control devices from outside the home. With care, it can also be secure. It's an important option in the greater ecosystem for advanced processes and machine learning.

The most truly reliable way for privacy and security to be enhanced is to limit the collection of data as much as possible in the first place.

Mycroft, for instance, uses cloud computing for their multi-platform voice assistant — with data from users who opt-in only — to train an open source voice recognition system that is shared as an open data set. They market themselves as a privacy-minded alternative to Alexa and others. Born from a Kickstarter campaign in 2015, their second smart speaker device, the Mark II, will be on the market in early 2020. In 2018 they integrated Mozilla's text-to-speech engine DeepSpeech as an alternative to Google's to enhance user privacy. Boasting over 35,000 users and some notable partnerships, Mycroft is still a tiny competitor to giants like the Amazon Echo, but presents a laudable vision for an alternative to data surveillance business models.

By most accounts, it's an uphill struggle for companies who seek investment for privacy-centric ventures. *"For years, the people who give financial advice to startups in Silicon Valley have encouraged companies to collect as much user data as they can, so they can list it as an additional asset in case they get acquired,"* says Ame Elliott, the design director of Simply Secure, an organization that works through design to promote privacy and security.

Elliott sees it as a structural problem that internet companies are *"playing fast and loose with data"* without any regard for what happens to it when a company changes hands. *"In general, we have to move from seeing data as an asset to seeing it as a liability,"* she says.

Tony Gjerlufsen is the head of technology at SPACE10 in Copenhagen, Denmark, an independent research and design lab entirely dedicated to IKEA. He agrees that few companies are opting for a privacy-first approach.

Deciding if and when a smart home device should send data to the cloud is a critical part of its design. These two products are intentional about when they do, and earned high marks in Mozilla's *Privacy Not Included guide.

Roomba
690 Robot Vacuum

Roombas might vacuum up data as well as dust, but iRobot seems to take privacy seriously. The Roomba doesn't send all the information it collects to the cloud, because it doesn't need to. For example, the maps it makes of your home to help it navigate don't leave the device. Any data it does send to the cloud (say, for control via the app) is encrypted.

Mycroft
Mark I

Mycroft created the world's first open source voice assistant, and the Mark II is the smart speaker to match. Mycroft sends and receives data from 'the cloud' to function, but the software is designed with privacy at its core. The company has hit roadblocks in hardware development, but plan for the Mark II to be on the market in 2020 once it overcomes a few roadblocks in hardware development.

"There's an opportunism evident in the industry that says 'let's collect data now and see what we can use it for later.' Our philosophy is that you should be able to choose to say no to these opportunities." He says IKEA made the decision to leave out microphones in their new line of smart speakers based on a desire for simplicity and to minimize the risk of any trust being damaged between consumers and the brand. *"The pace of technology is so fast that many companies feel pressure to innovate before they can really understand the risks, but it's a minefield,"* says Gjerlufsen speaking of a broader range of companies that were not traditionally in 'tech' but now see themselves in some degree of competition with the likes of Google and Amazon.

Push for better privacy regulation

Public scandals around data and security breaches have certainly affected the behavior of technology industry in recent years, to some degree, as have the threat of government issued fines and other sanctions. The fear of losing trust is real and directly influences the bottom line.

For instance, Amazon, Google, Apple and Facebook Messenger all announced in 2019 that they would halt initiatives to have humans secretly review and transcribe audio recordings. And children's smart watches by the toy company VTech now collect less data (and no longer connect to the internet) ever since they were slammed with allegations by the U.S. Federal Trade Commission in 2018 that they violated rules for the protection of children's online privacy.

Efforts to establish comprehensive data privacy rules and accountability mechanisms around the world will make a huge difference in decreasing the degree of invasive data collection companies will even attempt. In the European Union, the General Data Protection Regulation (GDPR) has been praised by privacy advocates for creating stronger rights and protections for citizens, as well as for obliging companies to be more transparent and accountable in how they collect, store, and use personal data. Its broad scope has provided a crucial platform for civil society groups and individuals to seek enforcement through the courts and data protection authorities.

Too often, privacy regulations are maligned by parts of the tech industry as being costly and bad for business. Intensive lobbying efforts have deterred and frustrated many jurisdictions in their efforts to implement and enforce strong privacy regimes, including for IoT. The European Union is just one jurisdiction. Specifically, a proposed law complementary to the GDPR that would update the existing ePrivacy Directive (the 'ePrivacy regulation') is languishing as a consequence of tech sector lobbying. If passed, it would define machine-to-machine communication (say, from your refrigerator to a cloud server) as worthy of heightened privacy protections akin to private phones and messaging communication.

This is the type of regulation that will really make a difference to how personal data is protected.

Protect people

People can educate themselves about what products are the most private and secure, but the full burden should not rest on the individual. How could it, when so many companies are not transparent about what they do? Policymakers and industry stakeholders are exploring standards, certifications and other information-mechanisms to help consumers understand the security features and privacy risks of products, but far greater urgency and speed is needed to reduce the harms of today from multiplying.

For instance, to avoid amplifying DDoS attacks or becoming tools of surveillance, vendors could be doing more to shoulder responsibility for reaching the highest standards of security. Sarah Zatko, a chief scientist at the Cyber Independent Testing Lab in the United States, helped lead a study of the firmware of more than a thousand products in 2019. She says there could easily be more specific requirements for IoT security, akin to "the seat belts and airbags of software" since so many products use similar software source and build systems. *"Industry-standard safety features are generally taken for granted or assumed to be present. Without transparency, testing, or regulation, however, they're less omnipresent than one would hope,"* she says.

Ranking Digital Rights holds big technology and telecom companies accountable with a Corporate Responsibility Index based on a range of indicators they link to human rights, including privacy and data handling policies. The organization has recently drafted new indicators for data collec-

The collection and monetization of personal data is a dominant business model in IoT, but not the only one! These two products limit data collection and sharing, and earned high marks in Mozilla's *Privacy Not Included guide.

SYMFONISK
WiFi Bookshelf Speaker

Collecting less data can be good for business too. IKEA and Sonos decided not to add a microphone to this WiFi enabled bookshelf speaker, because it didn't really need one, and they could make the product more affordable without data collection and processing.

Petnet
SmartFeeder

If you want to pamper your dog or cat, data privacy may not be top-of-mind. But there is plenty that can go wrong with smart pet products. Thankfully, there are also products like Petnet's SmartFeeder that do not sell your data to third party advertisers.

tion, targeted ads and algorithmic systems that suggest more clear communication about informed consent and control over data will be key to a higher score. *"It's relevant to communicate to users whether data collected is essential to the function of a product or not,"* says program manager Lisa Gutermuth. *"Too often, more is collected than is actually needed,"* she says.

Professor of creative technology, Jon Rogers, says IoT devices are typically designed to work as seamlessly and invisibly as possible. Neither the hardware nor the computing processes are designed to be seen or understood by users. He suggests design could be part of an answer for how to make computers *"reappear"* and become easier for people to make clear decisions about.

Does it really need to be online?

Rogers makes a point about how certain home devices may collect data about who visits. *"If you visit a friend and they have an Alexa or an Amazon doorbell, what is the etiquette for letting people know that they may be recorded or photographed by a computer? It's normal for people to ask you to remove your shoes before entering a home, but we still haven't figured out what consent really looks like in these social contexts, let alone in public where cameras are everywhere."*

For all the countless efforts to make the smart home wiser, there is also a case to be made to hold back on connecting things uncritically. We could at least wait to buy pet surveillance devices until a privacy-respecting one lands on the market. So many shoddy products and technologies are destined to become e-waste within months. They may not even work in the most basic manner without an internet connection. It makes it all the more imperative to go for trustworthy products made with real care for human and earthly values for the sake of a healthier internet.

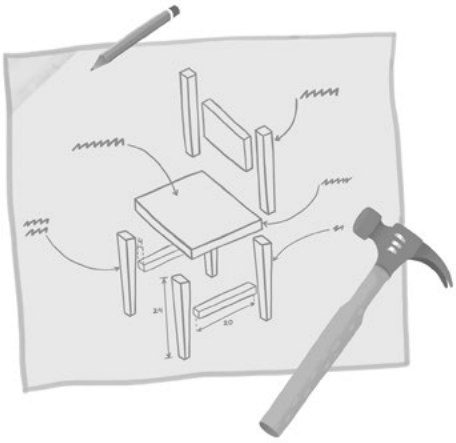
Back in Taipei, the BerryNet team say they feel optimistic that people around them are becoming more aware of the importance of privacy, and not just because of security breaches. *"People are starting to care about privacy in IoT, and developing solutions to monitor and control personal data in ways where the data belongs to you,"* says Yang, whose new company is a member of the global non-profit association for self-determination over personal data, MyData.

Bofu Chen says he feels inspired by forecasts that say scaling the Internet of Things from billions of devices to hundreds of billions in coming years, will lead to such complexity that decentralized data processing and private-by-design solutions will gain an even greater advantage.

"I feel good about the future and about what is possible," he says.

What Can be Done?

The market for smart home devices is fraught with insecurity and privacy risks. **What can be done?**



1 Make Your own Things

The miracle of IoT is how easy it has become to create automated systems. If you want your smart devices to do only simple things (e.g., turning stuff on and off) do you really need cloud servers? No! You can build simple IoT devices on local networks (or repurpose used equipment) that keep your privacy intact. Join open hardware, open design and maker communities worldwide to help design alternative futures where technology giants don't control everything.

2 Rate More Products on Privacy and Security

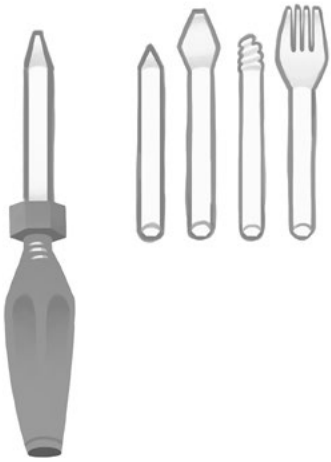
It's exceedingly rare for mainstream product reviewers and consumer protection groups to call out smart home devices and gadgets on their approach to privacy and security, let alone interoperability or sustainability. Retailers could choose to display privacy policies and terms and conditions of connected devices they sell and commit to upholding good standards. We need to uplift products that actually seek meaningful consent from users before grabbing data.

3 Business Models Matter

Too many business models are focused on monetizing personal data, putting both privacy and security at risk. Storing or processing data in the cloud isn't inherently bad, but with smart home products there is an ongoing cost to keeping a device and its data secure. It's time for more innovation around business models that incentivize long term software development, decentralized (edge) data processing, and open standards for greater sustainability.

4 Push for Better Privacy Regulation

We know this: strong data privacy regulations can lead to better protection for all internet users and greater trust in digital services. The rise of IoT only increases the urgency for expanding what constitutes personal data (say, machine-to-machine communication between your refrigerator and a cloud server, or data gathered through device tracking, including your location) and giving recognition to the special sensitivity around this personal data.



5 Demand More Interoperability

"Product families" by the likes of Amazon, Google and Samsung tend to use their own protocols, data formats and cloud services, rather than interoperable open standards. With more focused industry standardization efforts (there are many competing efforts) devices from different makers could co-exist more easily. This would benefit competition and probably lower costs while increasing choice.

6 Protect People

Individual consumers shouldn't be saddled with the full responsibility for ensuring that IoT products meet security and privacy standards. Policymakers and industry stakeholders should explore standards, certifications and other information-conveying mechanisms to help consumers understand the security features and privacy risks of products. Worldwide, we need transparency around the supply chain for technology that ends up in our homes.

7 Does it Really Need to be Online?

The technology industry may present the idea of the smart home as a kind of inevitable evolution, but is it really? Considering the cost of human labor, data exposure and energy expenditure needed to speak with an AI robot, is it worth it? Projects like the Internet of Shit may amuse you by mocking e-sneakers, but connecting things more responsibly (and with more data kept within the home) is actually the right thing to do: for the internet and the planet.

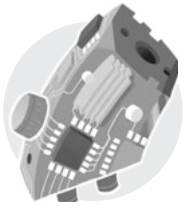
*Privacy Included

5 Key Decisions for Every Smart Device

There may be just one brand name on the box, but when you speak to a smart home assistant or jog with a fitness tracker you're interacting not with a single technology, but with a number of deeply connected technologies that may also be manufactured and maintained by different companies. In the design of any smart device there are decisions about five key components that will have lasting impact on the privacy, security, interoperability and sustainability of the product — and therefore also on the wider ecosystem of the Internet of Things (IoT).

Decisions about ▼

1 Hardware



Affordable hardware makes IoT accessible to startups and open hardware creators. But with low cost, poor quality may follow. Is a device designed sustainably or will it quickly end up as e-waste? An aesthetic of sleek surfaces, glued parts, and tiny size often trumps access to repair and replace parts. Low prices may also signal hidden motives to collect data. Hardware determines whether devices connect to networks via Wi-Fi, Bluetooth, ZigBee, or mobile connections, like 5G.

2 Software

Any IoT device counts on several different kinds of software to function. As on any computer or phone, there is an operating system. A range of free and open source solutions are popular among IoT developers. An app to control a device, as well as software for data collection or machine learning is often purchased as a service. For security, software should incorporate best practices, like automatic software updates and encrypting all network communications by default.

3 Interoperability

Often connected 'things' in a home can't work together because of brand ecosystems. For instance, using Apple AirPlay with Amazon's Fire TV is not easy. Network protocols like WiFi and Bluetooth can enable workarounds, but interoperability should be a critical component of a healthier IoT ecosystem. Projects like Mozilla WebThings and HomeAssistant let users control a variety of smart devices from a single platform, even when they aren't designed to talk to each other.

4 Data

Personal data collection and monetization is a dominant business model in today's IoT ecosystem, but there are also responsible creators who chose to minimize data collection to protect user privacy (or sometimes simply to lower costs). Most devices need to store and process data to function. This can happen either on a cloud server or locally on a device within a home network. Business models that treat data as a liability instead of an asset are still too scarce.

5 Usability

Devices in the home that can be spoken to, automated, or controlled through the web, can bring opportunities of convenience and greater independence to people with different accessibility needs and digital literacy skills. But only through intentional design. User interfaces can also nudge people toward better privacy and security by requiring a change of default passwords to stronger ones. They can also help communicate what data is collected, processed and shared.

*Privacy Included

Securing the Internet of Things

April 2018

Editor's note: We first published this article as a spotlight feature of the 2018 Internet Health Report, and are sharing it again now as part of our *Privacy Included special edition. It explains why smart home security matters to the health of the internet, even if you don't own any connected 'things' yourself. There is no shortage of stories about security gone wrong – and this article presents more questions than answers. But it's also true that in the short time since its publication, a lot of thinking and action has evolved about what to do. – ***Solana Larsen***

Somewhere in Vietnam, a man is searching for a shoe box in a storage room, a woman is slicing bread in Argentina and a child sits restlessly on his mother's lap in a waiting area of what appears to be a pharmacy in France. A cow is being milked in Germany.

They are being filmed by online security cameras without passwords assigned. They surely don't know they can be watched by anyone who looks for insecure cameras on the internet. Whoever set up the camera could choose to restrict access with a password. But without that protection, they are just there, broadcasting via the network. They don't have to be hacked.

Now consider that the number of internet connected devices is expected to double from 2015 to 2020. That's 30 billion devices worldwide. For every device with either no password or a bad one, the internet becomes a little more fragile and dangerous. But people buy things, connect them to the internet and never think about securing them as long as they work.

Fitness trackers, kitchen appliances, light bulbs... This year, we will be listened to, watched, recognized and recorded by phones, digital assistants and cameras like never before.

Data will be collected that is vulnerable to hacks and breaches. We could worry about creeps on the lookout for unsuspecting naked people, or financial fraud, or invasive advertising or political manipulation. Do cars share our driving habits with insurance companies? Do vacuum cleaners trade in information about the layout of our homes? To most people, these are hypothetical risks, hardly outweighed by the enjoyment of the Internet of Things (IoT).

The reality is that the *"attack surface"* of the internet is growing and that we have already had a taste of the nasty consequences.

In December 2017, three young men pleaded guilty in a US federal court to creating a strain of malware (malicious software) called Mirai in 2016 that enslaved thousands upon thousands of webcams, baby monitors and other devices with factory default usernames and passwords that performed targeted *"DDoS attacks"* to bring down websites and networks. When the authors publicly shared the code to obscure their own identity, Mirai botnets multiplied, and began competing against each other (and still do) for control over devices around the world, eventually succeeding in temporarily shutting down parts of the internet in the US and Europe, through a large-scale attack on the internet performance management company Dyn. In Europe, banks and internet service providers were extorted. In New Jersey, a university was.

Offering *"security services"* (veiled extortion) was part of the devious original plan of Mirai's authors, as was racking up dollars by creating fake botnet traffic on online ads. At the time, some security experts suspected government actors like China or Russia must be testing the resilience of the internet. The actual villains were less ominous, but the risk of all these insecure *"things"* still exists and the scale grows bigger with every new connected device.

For all the hype around gadgets and home appliances, many of the industries most impacted by IoT will be health care, transportation, energy and utilities. There are great opportunities for improving the efficiency and quality of public services, health and infrastructure.

Inexpensive hardware and decentralized innovation is also delivering the internet to more people, in more shapes and forms than ever. While that is something to celebrate, unfortunately in today's throwaway culture, internet devices are rarely designed to stay safe and secure over time.

Since all software is vulnerable to attack or malfunction with age, automatic software updates are a must. Small companies selling cheap IoT devices, without the resources and expertise of companies like Google, Apple or Amazon, will find this harder to do on their own.

Who do we hold accountable when the path from manufacturer to consumer is so opaque? Could there be regulations and industry codes of conduct to ensure the use of strong, random and unique passwords on internet devices? Could there be technical security devices that form a shield around a person's personal IoT network? Could there someday be dependable trustmarks for IoT – like the labels on organic food or energy efficient appliances? What role is there for designers? These and many other ideas need research, exploration and further discussion in 2018.

The key problem is that IoT is growing faster and bigger than we could have imagined. Some of the risks posed are personal (like being embarrassed or perhaps being injured by a hacked car) while other risks are at the system or environmental level (like hospitals or the electric grid being taken down). Either way, it's going to be costly to fix when things go wrong.

One of the great opportunities of the moment for advocacy is in the home – being smarter consumers and especially advocating as parents on behalf of children who ought to be protected from insecure toys that contain hidden microphones, cameras or other personal data recorders. Dolls like 'Hello Barbie' and 'My Friend Cayla' that listen and speak to children have attracted negative headlines for being easily hacked. Germany is one country that bans Cayla as a *"concealed transmitting device"*. Where else could traditional consumer safety regulations be leveraged?

We need to grapple with how we handle these issues as a society today: what we can leave up to industry, what we can leave up to consumer choice and what we need to regulate.

Further Reading

The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things by Consumers International and Internet Society *(May 2019)*

The House that Spied on me by Kashmir Hill and Surya Mattu, *Gizmodo (July 2018)*

Anatomy of an AI System: The Amazon Echo As An Anatomical Map of Human Labor, Data and Planetary Resources by Kate Crawford and Vladan Joler, AI Now Institute and Share Lab, *(September 2018)*

Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices by Hooman Mohajeri Moghaddam, Gunes Acar, Ben Burgess, Arunesh Mathur, Danny Yuxing Huang,Nick Feamster, Edward W. Felten, Prateek Mittal, Arvind Narayanan *(September 2019)*

Gender and IoT by Leonie Tanczer, Simon Parkin, George Danezis, Trupti Patel, Isabel Lopez-Neira, Julia Slupska, UCL Department of Science, Technology, Engineering and Public Policy *(2019)*

Which? Investigation Reveals 'Staggering' Level of Smart Home Surveillance by Andrew Laughlin, Which? *(June 2018)*