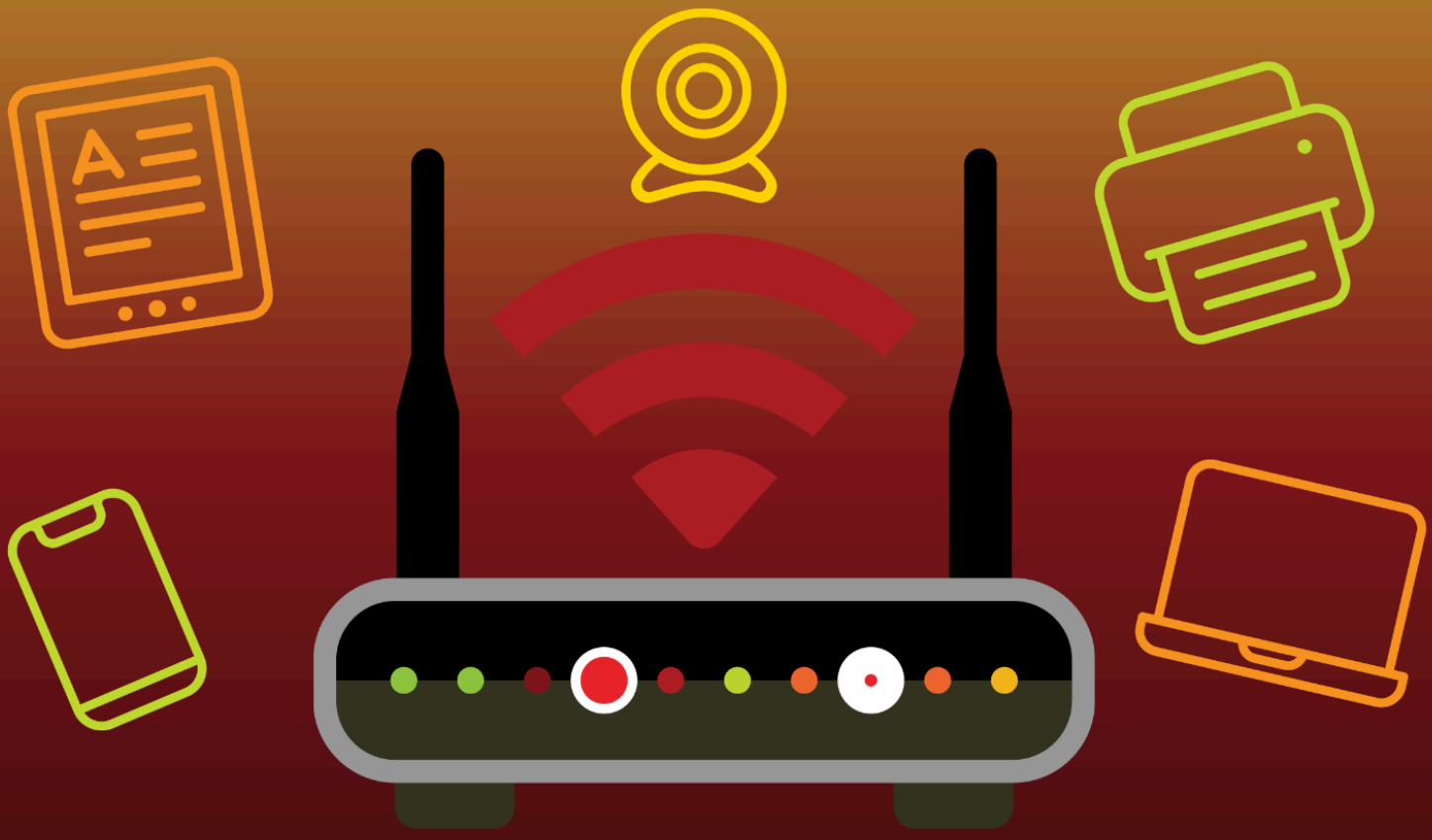

Longevity by Design

How to Build Long-lived Connected Products

BY STACEY HIGGINBOTHAM

NOVEMBER 19, 2025

CR Consumer Reports®

Introduction

Businesses are adding computing and connectivity to more and more products. Consumers can benefit from smarter products by saving money and time, but there are also risks. The way some businesses build and manage these smart devices has fostered a slow-moving crisis that reduces the overall longevity and safety of everyday objects. Products that used to behave and then break down in predictable ways, now fail when a product's connection to the cloud stops, after routine updates, or when the manufacturer decides to stop providing updates[1].

But it doesn't have to be this way. This paper explains this slow-moving crisis and how manufacturers should adapt their product design for longevity. Designing products for longevity will keep connected products safe, operational, and repairable over time, even after the manufacturer stops providing software and security updates.

Creating long-lived, secure consumer devices is essential for protecting consumer rights, our national security, and the environment. Consumer Reports also believes it will benefit manufacturers, which will gain a clear understanding of what it means to build and deploy a connected product responsibly.

The Longevity Crisis is a Business Challenge

Connecting a consumer device to the internet is often seen by manufacturers as an add-on feature, but connectivity changes the fundamental nature of a product offering and the business behind it. Companies that build connected products don't necessarily understand the obligations that arise when they add software and a cloud connection to their devices. And that lack of understanding means these products, which are often more expensive than unconnected products, die quickly, create security vulnerabilities, and risk damaging the product manufacturer's brand.

One way to address the frailty of connected devices is to design them to last as connected products for an extended and known period of time, and to then ensure they retain some functionality where possible once they are disconnected from the internet. Consumer Reports is proposing a set of recommendations as a means for manufacturers to build longevity into the design of their connected products.

---

[1] Bradley C and Barrera D (2023). Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity. Proceedings of the 2023 New Security Paradigms Workshop. 10.1145/3633500.3633501. (1-16). Online publication date: 18-Sep-2023. https://dl.acm.org/doi/10.1145/3633500.3633501

These recommendations are written for manufacturers, chip designers, software engineers and independent standards-setting groups. To increase consumer confidence in connected products, these recommendations should become part of the design methodology much like the Cybersecurity Infrastructure and Security Agency's Secure by Design recommendations have become table stakes for manufacturers trying to build secure products.

This report breaks down four areas where manufacturers can make choices that extend the longevity of a connected device. Much like building security into a product, these recommendations exist on a spectrum. The product's expected lifespan, cost, and the resources it uses should dictate how much a manufacturer might invest in longevity. A large appliance requires more investment in longevity than a connected light bulb. But every maker of a connected device should understand the compromises that come with adding connectivity. That starts with changing the business model and having a comprehensive understanding of what it means to release a connected product into the market.

Business Model

Connecting a device to the internet isn't just a technical shift; it requires a shift in business models due to ongoing costs over the lifetime of the product. The time frame for support and investment in ongoing monitoring and maintenance is similar to the more familiar obligations of a warranty, but generally continues for a longer period of time. If a company sells a connected product to a consumer, it should commit to maintaining that product for the reasonably anticipated lifespan of that product[2]. This is already the law in Europe under the Cyber Resilience Act[3] which will go into full effect December 2027.

So far, few companies have adapted to this shift. Those that have begun to think about the long term costs of supporting a connected device have generally provided a compelling subscription service paired with their hardware. Others will sell the hardware and limit the feature set of that hardware to a point where an additional subscription becomes compelling or even necessary. This is the case with many connected video cameras, where a consumer may only have a day or a few hours to check a recording before it disappears if they don't pay a monthly subscription fee. Other companies provide the hardware and charge a monthly or annual subscription where the subscription fee covers the cost of the hardware and upgrades, as is the case with the Whoop fitness tracker.

---

[2] S. Higginbotham. Hey Siri, Are You a Zombie? Consumer Reports Innovation Blog. Feb. 5, 2025. https://innovation.consumerreports.org/hey-siri-are-you-a-zombie/

[3]Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Article 13, Section 8. http://data.europa.eu/eli/reg/2024/2847/2024-11-20

To help companies recognize the ongoing cost of supporting products over time, either to help price a subscription or determine the true costs of a connected device, companies that build connected products should embrace the concept of a Digital bill of materials (BOM). Much like a physical bill of materials that sets a cost for each physical component of a product and is used to set the final selling price, a Digital BOM attempts to forecast the ongoing cost associated with a connected product. But understanding these costs requires companies to anticipate how long they plan to support a product and to share that information with customers. We recommend the following:

- **Manufacturers should establish a minimum supported life of the product which shall govern the expected maintenance costs.** Understanding how long a manufacturer plans to support a product and budgeting appropriately helps them ensure their business model and pricing can support the connected device over time. It also lets the consumer know how long their product will be updated so they can make an informed purchase decision.

- **Manufacturers should place their minimum supported life of the product on the product packaging and ensure it is disclosed at the point of sale**. Today a majority of consumer IoT devices don't have an easy way to find the product's end of life[4], leaving consumers spending their hard-earned cash on products that may lose support and stop working or become potential vectors for malware or attacks at an unknown or even undisclosed time. No one wants to spend hundreds of dollars on a connected device thinking it would last a decade only to discover it only has three years of support.

- **Manufacturers should create a Digital BOM with the following elements to help price in expectations for product:**
    - **The upfront, non-recurring engineering for the software.**
    - **The ongoing operational costs — such as bandwidth and cloud storage — tied to the minimum supported life of the product**
    - **The ongoing engineering costs — such as software development — tied to the minimum supported life of the product**

  A Digital Bill of Materials (BOM), which is a method of tracking how much it would cost to support a connected product securely and functionally over time. Much like a manufacturer might use a traditional bill of materials to calculate what a device costs to make, and then set its price accordingly, manufacturers can use a digital BOM to more appropriately price a connected product while taking into account how long they want it to operate. Using the digital BOM manufacturers then should plan for how long they plan to support the product, and let this plan determine when the manufacturer plans to stop

[4] U.S. Federal Trade Commission. "Smart Device Makers' Failure to Provide Updates May Leave You Smarting." Nov. 2024 https://www.ftc.gov/reports/smart-device-makers-failure-provide-updates-may-leave-you-smarting

supporting the product. The manufacturers should take this minimum support time frame and disclose it at the point of sale to consumers. We believe the exercise of calculating a Digital BOM could lead to several positive changes for the industry, including the ability to share the anticipated end of life with consumers at the point of purchase.

- **FASB (Financial Accounting Standards Board) and GASB (Governmental Accounting Standards Board) should clarify the method of GAAP accounting to reflect that a connected hardware sale creates an ongoing obligation. This should use the minimum supported life of the product as the expected length of time for the operating costs for the device.** Currently, there is room for interpretation when deciding whether or not revenue from a connected device should be classified under the Accounting Standards Codification 606 rules[5]. These rules govern whether a company that sells a connected product can count that sale as a one-time event for revenue recognition based on whether or not there is a one-time performance obligation or multiple performance obligations. Given the ongoing costs of maintaining a connected device, selling one, even if it doesn't have a subscription associated with it, should be considered an ongoing or multiple performance obligation.
- **Manufacturers should escrow the costs associated with a Digital BOM over the minimum supported life of the product in case of bankruptcy or sale.** If a company considers their planned support of a connected product as an ongoing obligation in a financial sense, then they should escrow the costs of fulfilling their obligation for the number of connected devices they have sold over the promised term of support. This ensures that in the case of bankruptcy or sale that the funds to continue supporting the product through the expected and disclosed minimum support time frame are enumerated and legally protected.

Software and The Cloud

In continuing with this theme of ongoing payments required to keep a connected device online, operational and secure, it's important to discuss how to think about the software and cloud requirements for connected devices. While it is possible to make a connected device that only connects to a mobile phone using Bluetooth, the majority of connected devices have some cloud dependencies. Additionally, the mobile app itself has cloud dependencies.

With those dependencies come ongoing cloud costs as well as engineering costs. When a connected device manufacturer stops paying, those devices tend to stop working abruptly, or fade gradually in utility as their applications lose functionality with each update of a mobile

[5] Sandie Kim, Mohanna Dissanayake, Michael Wrait and Previn Waas. Applying the Revenue Standard to Identify the Performance Obligations in Arrangements That Include Smart Devices, Updates, and Cloud-Based Services. Deloitte Technology Spotlight. April 2021. https://dart.deloitte.com/USDART/pdf/4d8a60c9-a211-11eb-8bbb-9790a765b6df

phone's operating system. Even in the case of a highly successful connected device, shifts in cloud or application architecture over time, mean that supporting a product over the years will require a specialized team and application stack that will gradually become more expensive to run. Ultimately, all cloud-connected products will have an end of life that may exceed their physical life as the costs associated with supporting it increase over time.

Technical requirements can extend the longevity of a cloud connected device in the case of a business failure, a decision to stop supporting the product, or the sale of a business to a company that no longer plans to support the product.

- **Manufacturers should develop their code to avoid cloud lock-in such as developing their code independently of a specific cloud provider.** Ensuring that a product's back end code is developed in ways that allow it to transfer between cloud services provides the ability to transfer the application between providers such as Microsoft Azure and Amazon Web services with minimal engineering costs. We have seen examples where the cloud back-end associated with a connected product was simply too expensive to re-engineer to move it to a referred host cloud, leaving the buyer of the connected product business unwilling or unable to continue support.

- **Manufacturers should maintain control of their DNS, URL registration, and root certificates and ensure they are managed by the organization, not an individual**. Should the employee in charge of any of these elements leave without a proper process in place, the product could become insecure or stop working. Maintaining control of these elements also ensures that in the wake of a sale, the information transfers with the company rather than an individual employee.

- **Manufacturers should have a plan for the end of device support or the death of the business. Longevity-promoting elements could include the following**
    - **Push a local API to the device for control when offline:** Allowing an API that usually runs in the cloud to run locally on a machine allows for a customer to still use the product within their own home or on a local server. When a company is going out of business or decides to stop supporting a connected device, creating and then sharing an API that can run locally allows product owners to download the API and continue to run the product and include it in a smart home system.
    - **Create a cloud-independent connection between the device and the mobile app to ensure a product doesn't need to connect out to a server to authenticate Wi-Fi:** This allows the end user to retain some useful features of a product even after cloud support has been shut down. If a device requires server-side access for Wi-Fi authentication, when the product gets disconnected from the Wi-Fi or the customer SSID changes after support has ended, a consumer can no longer control it using the app on their phone. Eventually an

unsupported mobile application will also fail, but allowing consumers to control their device by connecting it to the mobile app using something like Bluetooth could extend the longevity of a product by anywhere from a few months to a few years.

- **Ensure offline functionality for core features and disclose the potential lost features:** We can debate what features are considered "core" but a manufacturer should clearly define the core functions of their connected device and ensure those work without requiring internet access or an app. Manufacturers should also share what those core functions are, and provide proactive notification as to what features will be lost when support stops. This information should be provided at the point of sale.
- **Release product APIs and code to open source organizations:** There are excellent examples of open source projects that have kept older hardware operational. OpenWRT, which runs on routers, and The Rebble Alliance, which maintains software to keep Pebble watches working, are two. Those organizations show how to keep open source code accessible and secure, which could be a model for other organizations and manufacturers seeking to do the same. A manufacturer can allow consumers to repurpose the underlying hardware. In this scenario, the company may not provide the code used on the original device, but could provide a mechanism to wipe the existing DRM and code on the hardware to allow users to repurpose it.

Hardware

Hardware is often a roadblock for device longevity because the underlying chips used for computing or connectivity are generally supported by their manufacturers for a limited period of time which can range from five years for consumer products to 20 years for industrial applications. The longer the support timeframe, the more expensive the chip is. Like connected products, the silicon requires continuous software and security support while in operation. However, the makers of connected consumer products don't necessarily need to pay for industrial quality chips if they make a few longevity-preserving design decisions and chip manufacturers create a less-intensive support profile that provides security updates but not new features for a standard firmware profile. Our recommendations are as follows:

- **Manufacturers should design their hardware with modular boards that are easy to access for repair, replacement, and recyclability**. Designing the electronic components on a long-lived device such as a car or a large appliance to make it easy to replace or repair ensures that the product can last a decade or more, even as the electronics fail or radio standards change. Modular boards also make the product easier to repair, which benefits consumers and the environment.

- **Manufacturers should build with at least twice the memory needed upon launch to preserve the ability to update the hardware with new software and bug fixes**. During a software update, the manufacturer needs to deliver a payload of software that is usually larger than the current software package. This means that manufacturers who only design in enough memory to run their current software will not have enough to store and then run updates. This limits the ability for the hardware to support security updates or even new protocols, such as the smart home interoperability protocol, Matter.
- **Manufacturers should build for cryptographic agility to ensure that the device can transition to new algorithms when existing ones are cracked. This also prepares for the inevitable post-quantum world**.
  The government and technology industry are preparing for the inevitable day when current encryption mechanisms are broken as quantum computing reaches a point where it can be effectively used to crack the math behind today's encryption algorithms. Already the National Institute of Standards and Technology has approved new algorithms for lightweight IoT devices[6] as well as quantum-safe algorithms used by more robust computing platforms. However, IoT device manufacturers still have to use appropriate memory and computing power to remain crypto-agile and be able to use the newer algorithms when necessary. Remaining cryptographically agile will also require software and server-side changes that a manufacturer should consider in the initial design[7]. This is especially important for products that have long lives such as a car or large appliance, or where maintaining security is essential. For example, a light bulb or temperature sensor might not need to be upgradable to new encryption algorithms, but a car or oven would.
- **Chip providers should create standard, stable versions of their firmware that can be frozen after the end of support, and run beyond the traditional update cycle, receiving critical updates if needed**.
  Chip companies often provide a limited number of firmware updates to manufacturers who install their products. Generally, firmware updates occur every 12-18 months and can address security vulnerabilities as well as update the code to run more efficiently or to add new features. These updates will generally last for about two or three years of the product's lifespan. Chip providers can create a frozen and stable version of their firmware that will continue to get security updates over a longer period of time at no additional cost to the manufacturer of a device. To make this economically viable for the chip manufacturer, the company purchasing the chip must avoid customizing the

[6] Meltem Sönmez Turan, Kerry A. McKay, Donghoon Chang, Jinkeon Kang, John Kelsey (2025) Ascon-Based Lightweight Cryptography Standards for Constrained Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-232. https://doi.org/10.6028/NIST.SP.800-232

[7] Barker E, Chen L, Cooper D, Moody D, Regenscheid A, Souppaya M, Newhouse B, Housley R, Turner S, Barker W, Scarfone K (2025) Considerations for Achieving Crypto Agility: Strategies and Practices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 39 2pd. https://doi.org/10.6028/NIST.CSWP.39.2pd

firmware outside of a standardized version, or figure out a way to fall back to the supported and standardized version at the time when free support ends.

- **Manufacturers should consider adopting the standardized implementation of their silicon that can accept security updates beyond the traditional update cycle**. Manufacturers often pay more for updates after the free support ends, which should become part of the costs in the digital BOM. But if the expected profit margins for a connected product don't support the ongoing price of firmware updates for the silicon, manufacturers should avoid customizing the firmware outside of a standardized and supported version, or figure out a way to fall back to the supported and standardized version at the time when free support ends.

Legal

In addition to the hardware, software and business challenges, manufacturers trying to build long-lived connected devices, also face legal and regulatory constraints. Business contracts can affect how a product functions. For example, a connected product's ability to talk to Alexa or Siri may rely on Amazon or Apple continuing a developer program that provides access to Alexa APIs. Or support for a particular music-streaming service in a connected speaker might rely on the two platforms continuing to share data.

Standards bodies and government agencies both have a role to play in making it less onerous to update devices without requiring a manufacturer to go through a recertification process. The goal should be on the reduction of unnecessary certifications for minor software or firmware changes as well as a considered approach to security certifications across a product that might require separate certifications for different aspects of the product. This will reduce the cost of maintaining connected devices.

- **Manufacturers should ensure that their cloud provider contract allows them to move all data, libraries, and dependencies from one provider to another.** This ability to switch helps ensure manufacturers can bring the cloud back-end in house if necessary and allows for transfers if the company is sold or needs to adjust costs. Otherwise when a cloud provider stops supporting a particular cloud service, the manufacturer may find it easier to kill an entire line of products. Or, when a company gets sold, the acquiring company might kill the acquired products to avoid maintaining infrastructure on two different clouds.
- **Manufacturers should establish contracts with third-party providers for advertised functionality of a product**.
  Many connected products are purchased by consumers that want to combine features from other platforms, such as the ability to connect a Spotify account to a car or use Alexa to turn on a set of connected lights. But these features are often dependent on services and relationships outside of the manufacturer's control. Establishing contracts

that outline the obligations that a third party provides, especially when it relates to an advertised feature, is essential to avoid accusations of unfair or deceptive advertising[8].

- **Manufacturers should review the code used in their physical product and back end infrastructure.**
  There may be requirements associated with some of the underlying code that prevent the manufacturer from open sourcing the code if the company fails. As an opposite example, OpenWrt, which was used to open up routers, has become one of the most celebrated open source projects. OpenWrt was enabled because Linksys, which built the original WRT54G series of routers, built them using software licensed under the GNU General Public Licenses (the GPLs). The GPLs require that companies distributing software under these licenses allow customers to make practical changes to the software, including installing those changes onto the device they purchased. For example, the WRT54G ran Linux, and thus Linksys was required to provide the complete source code for Linux and other software under the GPLs. As often happens in this situation, a community project was created from the source release, and OpenWrt now runs on many other routers that ship with Linux.

  Linksys was required to open up the code to developers under the terms of that license, and since then the OpenWrt project has been able to adapt the code to run on other routers.
- **Standards bodies and government regulators should clarify when a software change merits a need to recertify a device**. The goal should be on the reduction of unnecessary recertifications for minor software changes, thus reducing the cost of maintaining connected devices. Recertifications should prioritize security and focus on devices with the most power to cause harm. This is a fine line to walk, because software changes can alter the performance or security of a device, but forcing a recertification for every software or even minor component change can also make it impossible to create flexibility in supply chains or even update software when vulnerabilities are discovered. The Food and Drug Administration in 2017 developed a pilot program to address the need for flexibility in certification of medical devices containing software, and produced a 2022 report that called for the agency to develop a new model for certification that took a more adaptive approach. As opposed to requiring a full certification process for each change, the report recommended using a model that looked at the manufacturer's prior transparency, culture of quality and safety, and product reviews over time to create a more efficient review process that can adapt to product changes over time[9]. It's worth

[8] U.S. Federal Trade Commission. "Smart Device Makers' Failure to Provide Updates May Leave You Smarting." Nov. 2024
https://www.ftc.gov/reports/smart-device-makers-failure-provide-updates-may-leave-you-smarting
[9] US Food and Drug Administration. "The Software Precertification (Pre-Cert) Pilot Program: Tailored Total Product Lifecycle Approaches and Key Findings." September 2022.
https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-software-precertification-pre-cert-pilot-program

noting that the report recommended that product submissions and data about the products be stored in a standardized and structured data. This makes it easy to automate keeping devices and software up to date and communicating their status to others.

- **Standards bodies and government regulators should consolidate security certifications where possible.**
  Connected products contain components that all may have to undergo individual certifications. For example, a connected door lock might need to comply with Builders Hardware Manufacturers Association/America National Standards Institute hardware-based certifications, a cloud-based security assessment such as SOC-2, a security certification as part of getting Wi-Fi certified and more. Some of these certifications overlap. As governments build out security standards such as the U.S. Cyber Trust Mark, they should incorporate existing standards and allow companies that meet those certifications to apply their existing security certs to acquire these overarching certifications such as the Cyber Trust Mark.

Conclusion

After more than a decade of connected device sales, it's clear consumers believe these products can offer value when they are secure and supported over the long term. It is equally clear that many companies launched connected devices to capitalize on the hype around the smart home without considering the products' long-term security or longevity. While concerns around device security are being addressed with the U.S. Cyber Trust Mark, and some state laws that require companies to secure their connected devices, addressing the longevity of these devices is still a relatively new idea.

However, if the technology ecosystem does not address both security and longevity it risks the creation of millions of devices that will fail from a lack of software support long before their physical components degrade. This leaves consumers frustrated at the shortened lifespan of these "smart devices" and our landfills full of products that could still function if just a bit more forethought were put into their continued operation during the initial design.

Consumer Reports would like to thank Afero, Arm, Cleveland State University College of Law, Mutually Human, Particle, Open Home Foundation, U.S. PIRG Education Fund, Secure Resilient Future Foundation, Michael Dow, now retired from Silicon Labs, and others for participating in this paper.