Testimony of Jonathan L. Zittrain
George Bemis Professor of International Law
Professor of Computer Science
Co-founder, Berkman Klein Center for Internet & Society
Harvard University

before the

Subcommittee on Competition Policy, Antitrust, and Consumer Rights
Committee on the Judiciary
United State Senate

June 15th, 2021

Chairwoman Klobuchar, Ranking Member Lee, and members of the subcommittee:

The Internet moment

In the late 1980s I was a sysop -- a "system operator," or online forum manager -- on CompuServe, one of the proprietary precursors to the mainstream Internet. CompuServe subscribers paid by the minute for news, weather, and to chat with one another; the company provided both the network and the orchestration of that content. It was a time of seemingly vibrant competition—an American wanting to get online in that era could choose not only CompuServe but also from among such competitors as The Source, Prodigy, America Online, MCI Mail, Delphi, and GEnie.

These services did not interoperate with one another. For example, while each had an implementation of electronic mail, you could only communicate with fellow subscribers to the same service. Which, if you only wanted to pay for one service, could make switching very onerous: to do so would entail leaving behind your existing communities, service offerings, and habits. The nominal availability of alternatives masked the sense of capture that an early adopter, or really any adopter, might experience after having invested in one service or another.

Moreover, the kinds of innovation that competition among services like these produced was at the margins. One might be a little cheaper than another or offer some exclusive content through an apt business deal with, say, a news service or a particular celebrity,

but all assumed that they would have to offer both network connectivity and their own content, under a transactional pay-per-use business model. In 1991, thirty years ago, the industry's big question was which one of those competing services would ultimately beat or buy out the others, winner take all.

Happily, it turned out, this industry was asking entirely the wrong question. All of these services were steamrolled by the arrival and growth of the mainstream Internet, a technology designed with a completely different architecture, ethos, and economic model.

The Internet's framers, in an unusual divergence from the spirit of both the corporate structures of the 1980s that the Internet eclipsed and the startup culture of the late 1990s and 2000s that the Internet spawned, implicitly foreswore making any money from their invention. They also did not anticipate raising and spending millions of dollars to build a centralized commercial network, much less to provide for the placement of content upon it.

The result was a network design in which *protocols* -- elegantly and precisely specified ways for disparate existing networks to communicate -- were developed and made available for anyone to implement, ranging from the makers of network hardware to developers of any piece of software that wished to speak "network" (or "email") with any other piece of software. Content would be provided by the network's users to one another rather than sourced from the network itself, from a hobbyist running their own blog server to a "voice-over-Internet-protocol" audio call mimicking legacy telephony to HBO streaming its latest hits.

This Internet, and the World Wide Web built upon it in a similar spirit -- a killer app whose inventor exclaimed, "This is for everyone" -- had and to this day have no CEO, no main menu, no "center" at all. These very absences the "unowned" Internet, and the content proliferating upon it from so many sources, to so quickly render the stove-piped proprietary information services thin and tinny by comparison, hopelessly behind in both service offerings and content. Those walled gardens soon retreated to become either small content outposts on the Internet themselves -- abandoning charging for "connect time" -- or to become simply commoditized Internet network on-ramp providers for the balance of the dial-up era. The latter strategy worked until the demands of broadband provision, something only possible through companies that had provided actual wires or specialized wireless links to subscribers, made it untenable. The entire pre-Internet sector of intense private competition had lost to a collective hallucination, a public good controlled by no one entity, including the government. That is, to an open protocol that

had garnered enough support to gain a momentum all its own, one still going more than thirty years on.

When the Internet became ubiquitous by the early 2000s -- with truly nothing meaningfully competing against Internet Protocol -- it eliminated the superficial competition among the proprietary information services and replaced it with a much more meaningful competition among anyone prepared to offer up a Web site or an Internet-aware app.

Whether you had a PC or a Mac or something else entirely, and whether you variously connected from home, a public library, or an office, sometimes wired, sometimes wireless, the full range of the Internet's offerings were on tap. A single flexible, freely-available shared protocol, open to third party contribution with little or no gatekeeping, promoted competition through anyone's building upon its generative base. Once started, its gravitation was irresistible. It became a monopoly with no monopolist behind it, and thus no means of cornering or exploiting it. It was a commons.

This realization of the Internet was not inevitable. As its predecessors make clear, it certainly did not have to be designed the way it was. For the Internet to become ubiquitous required a special alchemy comprising the moment it went mainstream, the unusual ethos and capacity of its designers, the pent-up supply of independent software and content developers ready to provide new Web sites, and the angel and venture communities anxious to fund them. There was also comparatively tiny but absolutely vital funding from the National Science Foundation to support some of the basic research and initial network linkages to prove out the eccentric theory of the Internet's layered design -- its insight to separate network from content, and to "packetize" information flows so that they could share a common network pipe even if from disparate sources and destinations, rather than needing dedicated network lines at the ready for exclusive dedication to every given single connection between two parties.

Whatever the many problems befalling the Internet and those of us who use it today -- and there are many -- we are, on balance, in an incalculably better and freer place than we were thirty years ago, and than we likely would be today had the early metered models of network-with-content continued to force us to choose one ecosystem over another, or, through consolidation, experience collectively a single (no doubt government-regulated) monopoly provider of information who would approve each new digital service or content offering.

The yearslong and, in a narrow sense, fruitless battles over the "set top box" -- back in the day when it was assumed that monopoly or duopoly cable television providers would be the only way to serve broadband services into Americans' homes, and those providers would be the only sources for those junction boxes -- demonstrate how fraught the effort can be to enable even a fraction of the Internet's capacity for permissionless innovation. (Google and Amazon were, understandably, fiercely interested in promoting competition in that realm.) Without the Internet, the product of even intense competition among the proprietary network providers -- each competing rationally -- would have fallen short. And that's because the benefits of interoperability can help everyone, even as no one party is in a position to want to invest in that interoperability until it has magically already happened.

The Internet of Things moment

The Internet's moment offers a number of important lessons for the topic of today's hearing on protecting competition and innovation in home technologies. In ways that at least rhyme if not repeat, today's development of the Internet of Things -- that is, Internet-aware devices that react to the bits they receive and send out bits of their own -- is at a fork like that of the proprietary information services in the 1980s. There is a layer of genuine if superficial competition among competing ecosystems to connect people with the things whose features they'd like to control over the Internet -- usually through their mobile phones. Amazon, Google, and Apple are among those offering smart home systems to control such things as light bulbs, thermostats, and speakers. And some makers of devices, whether particular brands of light bulbs, dishwashers, or home security systems, offer single-purpose mobile phone apps or Web sites through which to control those things over the Internet.

I say superficial because this kind of competition offers the worst of both worlds. It's fragmented enough to be frustrating for consumers wanting to furnish their houses, requiring them to accrue a motley assortment of stovepiped apps for each new device, or to be eagle-eyed about what's compatible with what when a device tries to use a broader control platform and interface offered by a bigger company like Amazon, Google, or Apple. And once a consumer has made an investment in one of those systems, each new physical device purchased for use with that system can serve to lock the consumer into that standard, even if a competing ecosystem turns out to be more desirable if there were a clean slate. That undermines a critical form of consumer self-defense, which is the basis for fulsome market competition. If one of the big providers stops patching its control platform or producing good hardware, there's no

easy opportunity to decamp for another ecosystem without putting a lot of stuff up for auction on eBay or making a significant contribution to a landfill -- some of which might have to be literally pried out of the walls before decommissioning. The closest pre-Internet-of-things analogy might be that of Microsoft ending security patches for the version of Windows XP that many bank ATMs run -- with few ready alternatives for the banks.

Because control for smart devices is typically built upon a mobile phone's triggering, one's initial upstream choice of smartphone could end up with long-term lock-in. Just as many of us idiosyncratically possess phone numbers with area codes frozen from wherever we were in 2006, a decision about what mobile platform on which to start a teenager -- perhaps simply mirroring that of their parents -- can have yearslong implications. For example, buying the iPhone brings along with it Siri, Apple's virtual assistant. Siri is the way that a consumer might expect to control their smart devices. In turn, Apple decides what devices Siri will work with. If Apple were an upstart, it might importune as many smart device makers as possible to build towards compatibility with Siri. Because it's not an upstart, the power flows in the opposite direction: anyone building a smart device will likely want to make sure that it can work with commands issued by the phone owner to Siri. That can put a smart device maker in a vise, as one operating system maker may make demands upon it in order to include it in its ecosystem -- demands that influence what arrangements the device maker can enjoy with other operating system makers. To be sure, someone browsing the smart electronics aisles at Best Buy or Staples will find plenty of products that can be controlled by different IoT control platforms. For instance, if you want to buy a Wyze smart plug, or a Phillips Hue smart light bulb, you'll find the products are compatible with both Amazon Alexa and Google Nest devices. Connecting similar devices with the Apple HomeKit can be a bit trickier, though there are "hacky workarounds," such as Homebridge that people with extra time on their hands can use to connect them up.

But the give-and-take between control platform makers and device makers rarely takes place in public view, and little precludes platform makers from shifting the technical terms of compatibility. This might bear on developers' abilities to make their technologies available to consumers at all, given what we know of the inflexibility of the terms sometimes set by the large players. For example, the European Commission's recent report from its inquiry into the Internet of Things describes how the requirements imposed by the largest players for independent developers to gain access to their ecosystems "may even require changes to products during the development or production process" and that by imposing these requirements, they may "be able to limit

the functionalities of third-party smart devices and consumer IoT services, compared to their own."

And the operating system makers themselves can end up on all sides of these deals. I doubt it would surprise anyone if Apple announced next week that it was making smart light bulbs, the way that Amazon makes Echo speakers -- which are not only capable of playing news and music, but receiving commands to feed to Amazon's assistant, Alexa. Alexa can help with purchases (most seamlessly, naturally, if they're placed at Amazon.com) and with controlling devices that are Alexa-compatible. The worst-case plausible scenario in the jostling among device makers and competing OS manufacturers is something like this: thanks to the iPhone your parents got for you as a teenager, your photos and calendar are in Apple iCloud; your purchased apps are iPhone apps; and your devices are arranged around compatibility with Siri. When you're shopping for your first apartment or home in your thirties you may need to know if its appliances indicate that it's a Siri residence versus an Alexa one. This makes about as much sense as if the color your childhood bedroom was painted had some bearing on what car you could drive and apartment you'd want to rent ten years later. This kind of lock-in can sometimes be quite willful, such as in the realm of instant messaging apps, which remain all over the map on interoperability with one another. And at least one major app, Apple's iMessage, even resists cross-platform compatibility, working only on Apple operating systems.

It's possible that these competing Internet of Things ecosystems will converge to a single one, through acquisitions and runaway network effects by a single winning competitor. After all, the more users a system accrues, the more device developers will seek to be compatible with that system, in turn drawing more users. It would be the equivalent of AOL winning the proprietary online services wars, with no dark horse Internet to displace it. Or, say, Uber beating out Lyft and lesser-known worker cooperatives by constraining how readily consumers or drivers would want to switch between those apps, respectively. Apple, theoretically, could even take sides in that competition by selecting a single rideshare service as its business partner to fulfill any requests Siri gets to "find me a ride home."

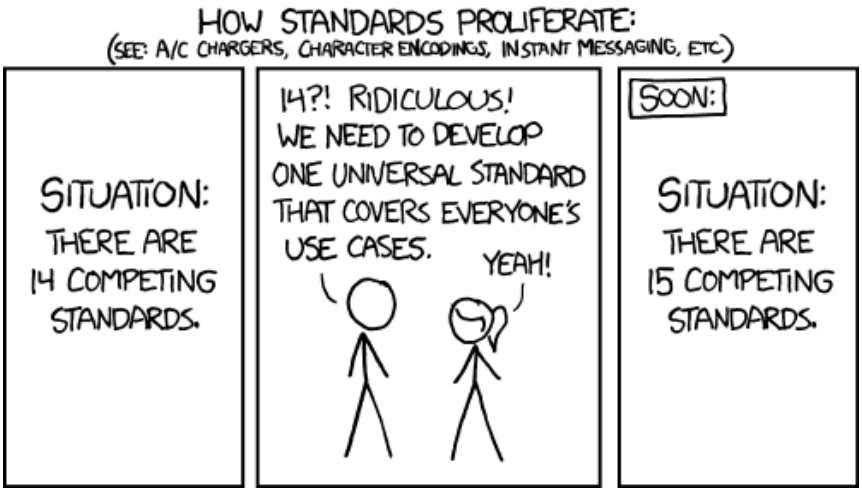
We saw exactly that maneuver in play when Apple struck a deal with Google to cement Google Search as the default search engine on Safari, now subject to an antitrust suit by the Department of Justice. (A similar deal has provided enormous financial support to Mozilla in its shepherding of the Firefox browser.) The market behemoths aren't shy about striking deals with one another if it means everyone gets to consolidate market shares, as in this instance where a dominant player in one market (Apple, for mobile)

uses that position to extract rents for preserving the position of the dominant player in another market (Google, for search). Each big player vying in the Internet of Things domain -- including some of those testifying today -- would be within its rights to think it owed its shareholders an attempt at these kinds of winner-take-all plays.

Or, each player might also see the value of interoperability, the way that CompuServe and AOL might have arranged to exchange emails with one another as a way of increasing their appeal to their respective subscribers. And we see some efforts, which we can credit as genuine if not destined for certain success, in today's home technologies. For example, the Connectivity Standards Alliance has subsumed several previous efforts to achieve interoperability, and now leads the development of Matter (confusingly, formerly known as CHIP), a standard backed by Amazon, Google, Apple, and numerous other industry participants which, if widely adopted and not captured by a handful of interested parties, could allow independently developed devices to interact with the major mobile operating systems and, in some cases, directly with one another. Another example is Iotivity, underwritten by various companies in the smart device space such as LG and Samsung. These consortia bear some resemblance to the kinds of grassroots processes, including both individual and corporate contributions, that fused Internet Protocol. But the most active consortia in the home technology space more closely resemble those of, say, the entertainment industry in the governing roles of the corporate sponsors. These elements were distinctly absent in the guiding organization for Internet Protocol -- the Internet Engineering Task Force, "open to any interested individual," with a "volunteer core."

These efforts might work. They also might not; there are reasons why a play for interoperability might, at a crucial moment, see a break by a major player for the exit if they think they can end up taking everything. (Worries about security could provide both a pretext and a genuine reason for such a closing-up.) Indeed, even as Matter perhaps is gaining momentum in the industry, Amazon has been involved in it while also freelancing its own Internet of Things-related protocols, such as Sidewalk, which provides a form of mesh networking among compatible devices. Moreover, these initiatives are about ways for devices to interact with control systems or one another, which on its own terms does not speak to the question of dominance among the user-facing front-ends like Alexa, Siri, and Google Assistant.

And, without trusted industry-wide buy in, any new unifying standard risks becoming just yet another instrument in a cacophony. As Randall Munroe succinctly puts it:



There's another area in which potentially salutary competition could be fostered, a counterpart to the "demand side" of user interfaces to control home technologies through such things as mobile platforms' digital assistants. We should consider for a moment the "supply side" of the home technologies themselves.

Crack open most smart devices and you'll find them running some flavor of a GNU/Linux operating system -- an OS that itself emerged in a decentralized, unowned way. (You can see why, if a device would benefit from having an operating system at all, its maker might choose one that doesn't exact per-unit licensing fees.) It might turn out that independent software developers, whether for whimsy or profit, could build new functionalities into the devices that their makers did not foresee or have the time or financing to build themselves. After all, the iPhone itself, like the iPod before it, was completely closed at the time of its introduction: wholly programmed by Apple. Only later did Apple unveil a software development kit and corresponding App Store to allow users to choose from among what would become nearly two million Apple-vetted third-party apps.

There could be a highly generative path by which makers of home technologies could choose to allow -- at a user's own risk -- choice in what kind of software will run on a device's operating system, which could also make easier the continued functioning of that device if the manufacturer vanishes. For example, one company, Moddable, is developing an openly-licensed toolkit to make it comparatively easy for would-be

independent software developers to make substitute software for potentially long-lasting hardware.

Remedies

So what should we do? It's true that in this area, as in so many that concern generative technologies and dynamic markets, the line between "too early to tell" and "too late to do anything about it" is vanishingly thin. To intervene too early countenances all the well-known worries about government policymakers substituting their own central planning for the efficiencies and creativities of a vibrant marketplace. But late interventions can be at least as undesirable, upsetting settled (if at a poor equilibrium) markets and technologies in ways that governments rarely dare to do. We collectively lucked out when the soft mud that was Internet Protocol became concrete before all existing stakeholders had a chance to argue about what a digital network should look like -- because if there were such a chance, the incommensurable demands that would be placed upon it would result either in paralysis or a network so locked down that very little that was truly new could be built upon it.

The marketplace for smart devices is, of course, broadly known, and has attracted enough commercial stakeholders to take the original playbook for successful Internetworking -- developed quietly among academically-minded network engineers for the 1970s and 1980s before unexpectedly crashing onto the mainstream scene in the 1990s -- off the table. But there's still plenty that policymakers can and should do.

First, Congress needs to update and reform the law of antitrust. It should articulate a coherent vision around which sorts of potential ultimate landscapes for an Internet of Things ecosystem would represent comparatively stagnant failures and which ones would be vibrant. This may be *easier* than it sounds -- I suspect everyone testifying today, for example, will offer no objection to the idea of an environment in which consumers can have a choice of operating systems as well as interfaces with which to interact with smart devices, and similarly, in which developers of devices aren't yoked to a monopolized bottleneck that can make or break their business. How much they mean it is no doubt another story -- but here any hypocrisy would be a virtue, as it might lend itself to a surprising consensus about the role of competition within common standards, and a stated appreciation for the kind of environment the Internet itself provided thirty years ago and still largely does today.

A vision supporting that kind of environment can then find itself realized in clearer legislative definitions of, for example, what counts as a "market" here in antitrust terms. Unlike markets for, say, milk or pig iron, the products and services of information technology are so consummately shaped by the companies that produce them that they can all too readily declare what's subject to competition and what is simply part of their product offering. For example, Apple might someday say that Siri is inextricably linked with iOS, and that iOS *means* Siri. Today, a particularly determined iPhone user can install the Google Assistant on their phone and then create an odd bucket brigade between Siri and that interloper. I doubt you've seen anyone saying, "Hey Siri: Hey Google, what's the weather," to have Siri ask Google to listen to your question about the weather, but it's -- by Apple's sufferance -- possible for the moment. But you can't eliminate Siri from the chain. And Apple might say that it would unduly degrade the iPhone experience to allow Siri to be wholly supplanted by any other assistant, even at the user's request.

This bears a striking similarity to the Microsoft antitrust case at the turn of the century, where Microsoft stridently argued that its own browser, Internet Explorer, was so central to its users' experience that those placing Microsoft Windows on new PCs were not to be permitted to substitute, say, Netscape for Internet Explorer, if they wanted to be able to offer their PC purchasers Windows at all.

Microsoft went so far as to try to "bolt" Internet Explorer into Windows, such that when the company was ordered by the judge hearing the case to allow PC makers to substitute other browsers, Microsoft told PC makers that they could only implement this option if they did so in a way that typically prevented the system from booting at all.

If I can buy an iPhone but choose what assistant I can directly invoke with a few words, that's a meaningful form of competition at the "assistant" layer. And that layer is important for the purposes of today's hearing, because it's the assistants that in turn translate people's requests and desires into commands to a smart device like a lamp or a door lock -- if the smart device maker is amenable and allowed by the maker of the assistant to connect. In fact, it is at the assistant layer that today's IoT landscape sees perhaps the most striking similarities to Microsoft's antitrust (mis)adventures decades ago, with the European Commission's inquiry into the state of consumer IoT reporting that voice assistant providers "would only licence their voice assistants together with other types of software, technology or applications and not on a stand-alone basis."

So, the law of competition can and should be shaped to recognize when what is offered as a single bundle of operating system and feature is best construed as an undesirable

vertical integration of one platform with another platform (even if conveniently labeled as a single platform). Once recognized, the law can then incentivize the provision of competition at each concentric layer above that of the operating system, in particular favoring the provision of common interfaces for any developer to be able to use for its new devices.

My choice of phone shouldn't roll into a necessary choice of assistant. And any given assistant should be able to be commanded to interact with any number of devices willing to adhere to a common protocol for giving it simple commands. That is, not only should I be able to swap Siri for Alexa for the Google Assistant on any phone, I should be able to ask any of those assistants to connect with any device whose makers have gone to the trouble to be able to parse common protocols to control smart devices. Gatekeeping of such connections -- whether in the name of quality or security -- should earn the kind of scrutiny that exclusive app stores are earning today, where the competition permitted by the operating system maker can be strategic and selective as much as it can be fulsome. To be sure, this kind of interoperability brings its own challenges. Steve Jobs's famous refrain of "It just works!" when introducing one groundbreaking product after another at developer conferences -- products innovative in their seamless user interfaces more than in raw functionality -- is made easier when a company has control over most if not all aspects of its platforms. But the law can set out standards here that are coherent and interpretable, and in turn offer companies, not least Apple, a level playing field and calculable rules on which to develop these systems.

Second, it's entirely fitting for a government to actively subsidize public goods like a common defense, a highway system, and, throughout the Internet's evolution, the public interest development of standards and protocols to interlink otherwise-disparate systems. These subsidies for the development of Internet protocols, often expressed as grants to individual networking researchers at universities by such organizations as the National Science Foundation, were absolutely instrumental in the coalescence of Internet standards and the leasing of wholesale commercial networks on which to test them. (They also inspired some legislators to advertise their own foresight in having facilitated such strategic funding.) Alongside other basic science research support, this was perhaps some of the best bang for the buck that the American taxpayer has received in the history of the country. Government support in the tens of millions over a course of decades resulted in a flourishing of a networked economy measured in trillions.

Further, government procurement standards could be devised to favor the acquisition of smart devices and operating systems for use by the government in its role as

technology consumer that subscribe to the open standards flowing from these efforts. (Just this approach is in use in the recently-passed law to promote more rigorous security standards for the Internet of Things.)

Third, Congress should consider what balance is appropriate to strike between vendors who might resist competition and consumers and third-party developers who might try to spark it anyway. For example, in a fascinating application of artificial intelligence, researchers are developing RL-IoT, a system by which outside developers might discern how to communicate with otherwise non-interoperable IoT devices, potentially linking modern, smarter systems, to those which might fall behind the state of the art and fail to offer any documentation of how they behave. Or consider the other "supply side" interventions discussed earlier -- those of third parties who, on behalf of consumers, seek to run entirely new code on existing device hardware. Perhaps under some circumstances the law should require disclosure of functionalities, or outright openness to the running of new code, as a way of reducing consumer lock-in. At the very least, there might be wise limits to place on the ways that proprietary vendors might invoke the law, including the law of copyright and paracopyright (such as the anti-circumvention provisions of the Digital Millennium Copyright Act), to foreclose such unwanted competition in the absence of a mandate to allow it. Many of these questions fall under what's often debated as the "freedom to tinker," and the coming deluge of smart home technology will reignite that debate, not just for unusually inquisitive and bold ham radio types, but for consumers who, at the press of a button, could implement in their own devices what those pioneers might build.

We're still early in this build-out, and what both can spark some beneficial market surprises and potentially result in undesirable anti-competitive cul-de-sacs is the fact that so many players in this space are sitting on massive stockpiles of cash and rivers of income -- these could be used for research and development, and they can also be used to defend their preeminence, as with the Google-Apple deal currently under challenge.

Amazon and Google, here today, are not only their well-known consumer-facing brands. They are also holding companies so large and influential that they could become serious market players anywhere they choose to play. Next week's headlines could hypothetically feature Apple getting into the car business -- or Tesla getting into the smartphone business. Google is already into both, and cars and phones join nearly every other physical object that boasts a battery or a power cord as an element of the Internet of Things. This dizzying game of musical chairs of companies and products would be all to the good if the makers of each had their functionality compatible with

evolving common standards of communications with the others. It's a proposition as powerful as that behind why the Internet and Web are better than CompuServe, and yet there is, in 2021, no inevitability that it will be brought to life.

Finally, I'd be remiss if I did not point out other areas in which public policymaking would be helpful -- indeed, might be desperately needed -- for the emerging Internet of Things, especially to the extent that making a product "smart" serves to transform it from singly-purchased product into ongoing service.

First, as a matter of both competition and security, devices that lose connectivity should be able to continue to function at some reasonable level without the internet, especially when they are substitutes for pre-Internet appliances, whether cars or coffee makers. That is, if they lose the ability to be smart, they should still be no less dumb than their analog counterparts. Devices should document what they can and can't do when voluntarily or involuntarily in "airplane mode," removed from connectivity. This is a matter of security so that refrigerators, cars, and light bulbs can still work if the Internet goes down. It's also a matter of competition so that people can still choose to use these products even if they no longer wish to pay some monthly subscription demanded by the original vendor, or if the original vendor goes bankrupt or pivots to an upgraded or unrelated product line.

Second, producers of devices above a certain threshold of popularity and adoption should be required to escrow the devices' operating systems and code, as well as post a bond to be cashed should the producers intemperately abandon the products. The money and code can be used to charter a non-profit foundation to maintain basic functionality for the devices to an approximation of a normal product life, or perhaps even beyond. The Firefox browser emerged from the abandonment of Netscape many years ago, and the Mozilla community that has grown around it has not only continued to innovate new features but to keep other browser-makers on their toes as a result.

Third, and I say this as someone who historically has not broken the glass and pulled the fire alarm for every possible concern about digital privacy over the past thirty years, the Internet of Things stands to become a privacy apocalypse.

The devices composing home technologies have an array of sensors -- microphones and cameras are quite common -- and they are always powered up and Internet-connected, which also means they can garner an immediate sense of where they are physically located. This opens up entirely new avenues of government-mandated monitoring, and in the United States the ground rules for such

surveillance are as yet poorly understood, since they were developed around *communications* technologies, that is, devices put into use only when one person is trying to communicate with others, such as telephones. They were also forged at a time when entrusting documents and other information to third parties was a comparatively rare and deliberate act -- making the law commensurately less protective. Smart home technologies flip this baseline, standing to quietly stream all sorts of in-home activity to third parties, where it would be unduly too-readily obtainable through government process. Not to mention the prospect that these devices will be deployed in jurisdictions that do not embrace the rule of law.

I believe the opportunities for expansion of government surveillance are so great that in the medium to long term they will vastly outweigh whatever hurdles law enforcement has encountered with the rise of encrypted messaging apps and the often-invoked problem of "going dark." A Congress concerned with civil liberties should be laying down consistent, transparent, and appropriately restrictive rules of the road now, before habits of surveillance for home technologies are established and then deemed indispensable even as today they are barely in use.

At least as worrisome, if not moreso, is the fact that these devices can be in a position to communicate what they see and hear back to their vendors, or to anyone the vendors designate, in way that is completely unmonitored by both consumers and those concerned with their protection, whether non-profits like Consumers Union or government actors like the FTC or state attorneys general. It is past time for Congress to itself, or through blandishment or mandate to the FTC, create standards for data collection and transmission for home technologies, rather than simply carrying over the more lenient baselines from the Internet environment that except for the most egregious practices merely require a privacy policy to be elucidated -- whatever its contents -- and, through state regulation like that of California, compel some rapid-fire decision prompts to users about accepting cookies. This is especially important given the previously-discussed lock-in that hardware-based environments can produce. If my oven, or set of in-ceiling speakers, have updates to their privacy policies that I wish to reject, I may have no alternative short of junking those devices -- a very different situation from simply choosing to no longer use a Web site or app, where the more modest problem of data portability might be my biggest worry.

There's an antitrust lens to the privacy landscape as well, when, as the European Commission report describes, "certain consumer IoT players, in particular the leading voice assistant providers, can impose standard terms and conditions that limit data use by third parties, while reserving extensive data use possibilities for themselves."

Finally, there are acute problems around security. It's one thing for a vendor to directly betray its customers by surveilling them in unexpected ways; it's another for any number of third parties to be able to do it thanks to lax security by that vendor. And because we're talking about physical objects, surveillance isn't the only risk. Over five years ago, researchers were able to hack a Jeep from afar, "taking over dashboard functions, steering, transmission and brakes." Chrysler's resulting recall of over a million vehicles took the form of sending USB drives to affected customers, who were to fix the Jeeps by plugging the drives into their dashboards.

There should be subsidized "red teaming" of smart products, looking first for vulnerabilities and, more important, for the kinds of systemic issues that can arise in interconnected and interoperable systems. For example, one group of researchers found a bug in the Zigbee Light Link protocol (Zigbee has since been absorbed by the Connectivity Standards Alliance mentioned earlier) that, in their words:

> By plugging in a single infected lamp anywhere in the city, an attacker can create a chain reaction in which a worm can jump from any lamp to all its physical neighbors, and thus stealthily infect the whole city if the density of smart lamps is high enough.

If there come to be tens of millions of products from a single vendor running proprietary, opaque software, a single vulnerability within the resulting monoculture could be exploited broadly and simultaneously. (Worse than a single flawed Jeep being remotely run off the road is a million Jeeps being remotely run off the road.)

Of course, while the damage from having all one's eggs in one compromised basket could be catastrophic, there are also plenty of risks in a more variegated ecosystem, since the resulting mosaic of vendors will no doubt have different commitments to security. If there are to be competing providers of software on both the demand side (e.g., the digital assistants and control systems) and the supply side (the smart devices themselves), it will be that much more important to be able to audit how they work and to have some form of screening to assure a minimal level of security against both unintended vulnerabilities and outright scams. The state of the art for this for our legacy consumer and enterprise information technology is a messy, unsatisfying combination of whack-a-mole antivirus software and best efforts vetting in app stores by judges whose decisions are opaque, and who belong to companies who themselves are competitors in the space.

There's a dire need to version up these approaches, or supplant them entirely, with trusted mechanisms that can better isolate ongoing security decisions from the controlling platforms' business strategies. There could come to be an accepted role for traditional public safety regulators or quasi-regulators like the non-profit Underwriters Laboratories, as there is for the review of minimal safety for food, children's toys, automobiles, and even table lamps. Even without the complications of third-party competition in software, Internet-connected smart devices should simply be rated for safety and security.

I'm very grateful for your having chartered today's hearing, while we're still in the "too early to tell" stage for the shape of Internet-aware home technologies. I imagine the very act of asking some of the leading companies to weigh in today conveys a message that Congress is involved and watching, mindful of the forking paths that could lead us closer or further from an environment of meaningful competition and inclusivity that in turn sparks a new round of innovation and creativity -- while minding privacy and security.

These issues are deeply important even if they might seem, deceptively, not urgent, and I thank you for the opportunity to share my thoughts on this topic today.