The End of Ownership

Personal Property in the Digital Economy

The title-level DOI for this work is:

doi:10.7551/mitpress/10524.001.0001

8 The Internet of Things You Don't Own

> The door refused to open. It said, "Five cents, please."
>
> He searched his pockets. No more coins; nothing. "I'll pay you tomorrow," he told the door. Again he tried the knob. Again it remained locked tight. "What I pay you," he informed it, "is in the nature of a gratuity; I don't have to pay you."
>
> "I think otherwise," the door said. "Look in the purchase contract you signed when you bought this conapt."
>
> In his desk drawer he found the contract; since signing it he had found it necessary to refer to the document many times. Sure enough; payment to his door for opening and shutting constituted a mandatory fee. Not a tip.
>
> "You discover I'm right," the door said. It sounded smug.
>
> From the drawer beside the sink Joe Chip got a stainless steel knife; with it he began systematically to unscrew the bolt assembly of his apt's money-gulping door.
>
> "I'll sue you," the door said as the first screw fell out.
>
> Joe Chip said, "I've never been sued by a door. But I guess I can live through it."
>
> —*Ubik* by Philip K. Dick (1969)

Cars, refrigerators, televisions, Barbie dolls. When people buy these everyday objects, they rarely give much thought to whether or not they own them. We pay for them, so we think of them as our property. And historically, with the exception of the occasional lease or rental, we owned our personal possessions. They were ours to use as we saw fit. They were free to be shared, resold, modified, or repaired. That expectation is a deeply held one. When manufacturers tried to leverage the DMCA to control how we used our printers and garage door openers, a big reason courts pushed back was that the effort was so unexpected, so out of step with our understanding of our relationship to the things we buy.

But in the decade or so that followed those first bumbling attempts, we've witnessed a subtler and more effective strategy for convincing people

to cede control over everyday purchases. It relies less—or at least less obviously—on DRM and the threat of DMCA liability, and more on the appeal of new product features, and in particular those found in the smart devices that make up the so-called Internet of Things (IoT). IoT has become something of a buzzword, intended to cover a range of devices from smartphones and networked thermostats to self-driving cars and wearable technology. These products generally combine embedded software, network connectivity, microscopic sensors, and large-scale data analytics. In essence, they are computers. As Chief Justice John Roberts recently wrote about mobile phones: "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. ... It is no exaggeration to say that many of the more than 90 percent of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[1]

That's certainly true of our phones, but it's equally true of so many of the objects of modern life. Your car is a computer with wheels; a plane is a computer with wings; your watch, your child's toys, even your pacemaker are all computers at their core.[2] And as computers, they are susceptible to the same sort of external limitations and controls we've witnessed with previous generations of digital goods. Even if we resist it, we're accustomed to software telling us whether we can watch a digital movie. But what happens when computer code dictates when your light bulbs have to be replaced?[3] Or how fast you can drive?[4] Or whether you can fly your drone in a particular neighborhood?[5] Or what brand of cat litter you can use?[6] What are the social consequences of a smart mattress that collects and analyzes heart rate and breathing data, monitors your movements, and provides you a nightly summary?[7] That's what Samsung's new Sleepsense device promises. Samsung even suggests you track your loved ones by "simply put[ting] the sensor under their mattress ... to receive an analysis of the quality of their sleep via email." What could possibly go wrong?

With so many networked devices in their homes, consumers are relying on home automation hubs—devices that allow them to control their home security systems, lights, garage door openers, and entertainment systems from any place with an Internet connection. The maker of one such device, Revolv, was acquired by Google-owned IoT company Nest in 2014. The Revolv hub sold for $300 and touted a "lifetime subscription" for updates and new features.[8] But in April of 2016, Nest announced it would no longer

support the Revolv. What's more, Nest planned to exercise its software-enabled remote control over the devices to render them entirely inoperable. After a May 15 software update, it explained, "The Revolv app won't open and the hub won't work."[9] Alphabet, Google's recently-created parent company, which has its sights set on the self-driving car and medical device markets, decided it was within its rights to reduce a device that consumers bought to nothing more than an overpriced paperweight. Consider that before you buy a Google car.

In this chapter, we look at a small sampling of IoT devices across a wide range of sectors and consider their consequences for ownership and consumer welfare more broadly. In many cases, these technologies offer real benefits. Yet the core cultural and legal shifts they represent strike another blow against ownership in the digital economy.

Jailbreaking Is Not a Crime

The exact origin of the Internet of Things is difficult to pinpoint, but one significant moment in its early history was the introduction of the iPhone on January 9, 2007. Steve Jobs told the assembled crowd, "Today, Apple is going to reinvent the phone."[10] He proceeded to wow them with "a revolutionary mobile phone, a widescreen iPod with touch controls, and a breakthrough Internet communications device" combined in a single product.[11] But like nearly every Apple product, the user experience was carefully choreographed and tightly controlled. iPhone users could only run Apple's iOS. They could only configure the settings Apple allowed them to access. They could only use Apple-approved mobile carriers. And they could only run the applications Apple provided. And later, once Apple launched its App Store, they could only install software that Apple approved—on the basis of opaque and inconsistent standards. What you could do with this remarkably powerful pocket computer depended entirely on what Apple let you do.

This walled-garden approach was a dramatic departure from the approach of general-purpose computers, including Macs, which allowed third-party applications and considerable freedom for user modification. In some ways, Apple's approach to the iPhone was more in line with an earlier phone maker, AT&T. During its decades-long reign as a telecommunications monopolist, AT&T—née Bell Telephone—used a number of strategies to maintain strict control over telephones. As the holder of Alexander Graham Bell's patents, AT&T had total control over the design, production, and distribution of phones. And even after those patents expired, it

extended that control by leasing phones rather than selling them, making certain that users didn't acquire property rights in their devices. They also used contractual provisions and legal threats to stamp out innovation, no matter how innocuous.

In the 1940s, AT&T exercised this power by targeting the Hushaphone, a small non-electronic accessory that attached over a telephone receiver to increase privacy and cut down on noise. AT&T forbade its use, and it took nearly a decade of legal battles before the D.C. Circuit rejected that restriction as an "unwarranted interference with the telephone subscriber's right reasonably to use his telephone in ways which are privately beneficial without becoming publicly detrimental."[12] This case, along with the FCC's subsequent *Carterphone* decision, which permitted the attachment of wireless technology to AT&T's phones, paved the way for competition and individual ownership of landline phones.

In some ways, Apple's control over the iPhone is a throwback to these bad old days. But it's one that many consumers happily accepted in exchange for the convenience of integrating all of their online activities into a single device. But not everyone was willing to go along quietly. Apple's restrictions sparked a movement to "jailbreak" iPhones in order to regain some semblance of ownership. "Jailbreaking" refers to the act of eliminating software restrictions and DRM that limit how phone owners can use their devices. With a jailbroken iPhone, you can install any software you choose, replace Apple's operating system with one you prefer, and customize the look and feel of your phone. Jailbreaking is related to, but distinct from, unlocking a mobile phone—the process of removing software locks that prevent you from switching wireless carriers—from AT&T to T-Mobile, for example.

Jailbreaking is not a new practice. Similar homebrew communities formed around other devices long before the iPhone launched, from Xbox hacks to do-it-yourself DVRs.[13] But nothing galvanized that community more than the thought of turning Apple's powerful and ubiquitous product into an open platform. The first iPhone jailbreak was announced on July 10, 2007, just eleven days after the device launched. With each inevitable Apple software update, the jailbreaking community would free that new version within weeks, if not days.[14]

Although it didn't file suit, Apple insisted that jailbreaking was illegal. In 2009, the Electronic Frontier Foundation (EFF) filed a petition with the U.S. Copyright Office requesting formal permission for iPhone owners to jailbreak their devices without fearing anti-circumvention liability. This

provoked Apple to explain precisely why jailbreaking should be banned. Despite referring to consumers as "iPhone owners" throughout its filing, Apple asserted that "iPhone users are licensees, not owners, of the copies of iPhone operating software."[15] In other words, when you buy an iPhone, all you own is the physical hardware. The software stored on it that make it work and account for much of its value—from the operating system that enables basic functionality to the built-in Weather and Stocks apps—still belong to Apple.

While perhaps shocking to those with an iPhone in their pocket, this stance was a logical conclusion for Apple, a company with one foot in the software industry and a commitment to controlling the user experience that bordered on zealotry. And because Apple has consistently proven its nearly unrivaled skill as a designer of end user experiences, it succeeded in selling us DRM in the guise of a smart device. It made us believe that a bug was a feature. Consumers recoiled at the idea of these sorts of restrictions when Chamberlain and Lexmark tried to sneak them into our garage door openers and laser printers, but when Jobs offered us the same vision, we lined up to give Apple our money.

Eventually, the Copyright Office ruled in favor of the right to jailbreak phones. However, in doing so, it sidestepped the contentious issue of ownership and focused on jailbreaking as a fair use of Apple's copyrighted iOS. And in 2014, an otherwise hopelessly gridlocked Congress passed, and President Obama signed, the Unlocking Consumer Choice and Wireless Competition Act in response to a petition signed by over 100,000 Americans.[16] Although each of these measures suggests both that people still care deeply about owning their devices and that government can be responsive to those concerns, they are temporary fixes. Both the Copyright Office exemptions and the unlocking legislation expire after three years.

Apple's battle for ownership of our phones signaled the beginning of a much broader shift. Every day, we learn of yet another object that will come with embedded software, location detection sensors, and network connections that limit consumer control and surreptitiously communicate back to its corporate mother ship. And while companies like Apple are slowly making their devices more open and user-configurable as a result of public pressure and competitive threats from open-source mobile operating systems such as Android, whole other areas of our lives are becoming constrained and preconfigured for us, often without our knowledge.

Old MacDonald Licensed a Farm

Farmers have enough to worry about. Banks are coming to foreclose on their land. Locusts are eating their crops. Immigration policy is complicating their hiring practices. And corporate agri-business long ago redefined the economics of their way of life. On top of all of this, today's farmers have to contend with intellectual property.

It began with seeds. For years, Monsanto successfully sold Roundup, an herbicide that helped farmers control weeds and other unwanted vegetation. But Roundup also often damaged the crops themselves, so Monsanto began manufacturing crops resistant to Roundup. It patented so-called Roundup Ready soybeans and later added alfalfa, canola, corn, cotton, and sugar beets to the list of Roundup-resistant products.[17] Initially welcomed by many farmers, some were troubled by Monsanto's claim that its seeds were licensed for a single season, not sold. This meant that no matter how many seeds you saved, they couldn't be replanted the following year, a centuries-old farming practice. Instead, you had to buy new seeds from Monsanto or else contend with pests and less-effective pesticides.[18]

Seed patents were just the beginning of the IP frustrations facing farmers. Software has also found its way onto the farm. The iconic John Deere tractor now contains no less than eight control units—hardware and software components that regulate various functions, ranging from running the engine to adjusting the armrest to operating the hitch.[19] When tractors were purely mechanical, farmers could easily maintain, repair, and modify their own equipment as needed. But now, software stands in their way. That barrier is no accident. Tired of losing revenue to industrious farmers who repaired their own tractors or bargain hunters who took their equipment to an independent repair shop, John Deere decided to force their customers to have their equipment serviced by authorized John Deere dealers. By interposing a software layer between farmers and their tractors, John Deere created a practical hurdle. And by wrapping its software controls in DRM, it created a legal one. A quick glance at the John Deere owner's manual gives you a good indication of the result. Almost any problem—from high coolant temperature to a parking break that's not working or a seat that's too firm—ends the same way, with a trip to the John Deere dealer.[20]

Fed up with John Deere's tactics, a group of farmers petitioned the Copyright Office in February of 2015 for a temporary DMCA exemption, like the one granted to smartphone jailbreakers, that would give them clear legal authority to repair, upgrade, and modify their tractors. John Deere responded with adamant opposition, insisting that tractor owners had no

right to look under the digital hood, even if the fix was quick and technically simple.[21] Its argument hinged on ownership. John Deere claimed it owns the software, and not just as an abstract matter of copyright law. It owns the copies of its code embedded in the tractors it sells to farmers, code that is essential to the functioning of the equipment. Farmers, in John Deere's words, merely had "an implied license for the life of the vehicle to operate the vehicle."[22] That means you get to keep driving the tractor you bought from John Deere for tens of thousands of dollars unless and until it tells you otherwise.

John Deere's attitude toward ownership has a number of important implications that typify the core risks presented by the Internet of Things. Most obviously, by denying farmers the right to repair—a right entrenched enough that even patent protection can't disturb it[23]—John Deere has effectively raised the price of its products for farmers. It has also done serious harm to the market for repair services, which are less competitive since farmers have no real choice of mechanics.

Less obvious is the harm locking down tractors can have on innovation. Sir Isaac Newton once said, "If I have seen further, it is by standing on the shoulders of Giants."[24] Of course, Newton borrowed the phrase from Bernard of Chartres, but that only underscores the point. Innovation is, in nearly every instance, an incremental affair. Small contributions add up, sometimes in unexpected ways. As Eric von Hippel describes in *Democratizing Innovation,* user innovation—the process by which users take, modify, and improve upon manufactured goods—is a valuable source of new inventive contributions.[25] Farmers have a long history of just such ingenuity and creative problem solving. As MIT Media Lab researcher Ethan Zuckerman wrote: "If you've flown over the western U.S., you've seen green circles dotting the landscape. This is a model of irrigation that's far more efficient than setting up huge systems of piping—instead, fields are centered on a well and a rolling pipe rotates through the field. This technique was innovated by farmers, but is now in wide use. Ask the companies who manufacture these systems who invented them and they'll claim creation. Show them a photo of the systems developed by farmers, and they'll say, 'But you should have seen their welds—they sucked.'"[26]

Kyle Wiens, a self-described right to repair activist, sees farmers' innovations as part of a broader movement: "In the tech industry, we tend to talk about the exploding Maker Movement as if tinkering is something new. In fact, it's as old as dirt: farmers have been making, building, rebuilding, hacking, and tinkering with their equipment since chickens were feral. I've seen farmers do with rusty harvesters and old welders what modern Makers

do with Raspberry Pis and breadboards. There's even a crowdsourced magazine, *Farm Show*, that's catalogued thousands of clever farming inventions over the past three decades."[27]

But if farmers don't own the tools, equipment, and seeds they use on a daily basis, this potentially fertile ground for innovation will lie fallow.

Less Fast, More Furious

John Deere is not alone. Other vehicle manufacturers including Ferrari, Ford, General Motors, and Mercedes-Benz are finding new ways to use technology and law to weaken the property interests of drivers. These efforts take a number of forms—DRM that prevents repair and customization, software that monitors and controls your driving, even restrictions on vehicle resale. The car, once a symbol of freedom and independence, is increasingly a tool for control.

Modern cars, much like John Deere's tractors, rely on dozens of electronic control units. Access to the software code on those control units is necessary for many common repairs. The code is also crucial if a driver wants to change the default tuning of their vehicle to get more horsepower or better fuel efficiency from the engine, for example. Researchers investigating potential safety and security flaws likewise need to look under the metaphorical and literal hood. But control unit code is often inaccessible because carmakers use DRM to keep it under lock and key. Until recently, car owners who broke these software locks risked liability under the DMCA, not to mention voiding their warranties. That meant only people with permission from carmakers can do repairs or research without fear of liability. When car owners asked for permission to access the software that controls their vehicles, GM told the Copyright Office that car purchasers mistakenly "conflate ownership of a vehicle with ownership of the underlying computer software in a vehicle."[28] But when code is inseparable from the essential functions of the vehicle, ownership of a collection of spare parts provides little comfort. Even those who miss their car payments have begun to fear "The Remote Repo Man"—an embedded program that disables automobile operation when the purchaser fails to make their monthly payment with no ability to override, even in emergency circumstances such as rushing to the hospital.[29]

Mercedes-Benz has also followed suit. It offers mbrace, a feature that provides remote vehicle controls, service diagnostics, directions, and vehicle tracking. It also connects to Verizon to provide roadside assistance, emergency help, and even geographic, speed, and temporal restrictions on

teenage drivers.[30] These bells and whistles sometimes offer real benefits. But what Mercedes-Benz doesn't advertise is that the code running these features doesn't belong to you. As part of the Terms of Service, Mercedes-Benz insists that "you do not acquire any rights in such software, including any right to use or modify the software[.]"[31] They go on to state: "We may update the software contained in your Vehicle's systems or the Equipment from time to time. We may do this remotely without notifying you first. ... These software updates may affect or erase data that you have previously stored on the Equipment in your Vehicle (for example, specific route or destination information). We assume no responsibility for lost or erased (or otherwise affected) data." In other words, Mercedes can remotely enter your car without notice or consent to update or erase any digital information or feature at any time without taking any responsibility for damage that it might cause. If you own a copy of *1984*, don't store it in your E-Class.

Consumer advocates have pushed back against these efforts, passing a Right to Repair law in Massachusetts and pressuring manufacturers to negotiate a Memorandum of Understanding with aftermarket repair shops and part suppliers that allows those businesses access to diagnostic information for repair and replacement purposes, but not for automobile owners.[32] According to the Automaker's Alliance, "The real issue of concern here is that the sophisticated computers in vehicles are so intertwined that they shouldn't (for security and safety and environmental reasons) be allowed to be tinkered with."[33] But carmakers themselves have a troubled history with their own sophisticated systems. Recent experience suggests that extra eyes reviewing this code might be helpful. Half a million Fords were recalled because of software glitches that prevented their engines from shutting off.[34] And Chrysler recently recalled 1.4 million vehicles because their onboard infotainment systems were vulnerable to hackers. Independent researchers uncovered that flaw when they wirelessly hacked a Jeep driven by a colleague, giving them control over the vehicle's steering and braking.[35]

The notion that car owners can only control the parts of their vehicles that don't yet incorporate software or electronic sensors has serious implications for ownership. Under GM's theory, you can check the air pressure in your tires—for now—but you can't run a diagnostic test on your GPS to make sure you won't end up in a lake. Every time you put gas in your car, there are security, safety, and environmental risks. But unless you live in Oregon or New Jersey, you'd be shocked if you were locked out of your own gas tank. There are pressing public safety concerns associated with operating a car, but they should be addressed by accountable public agencies such

as the Department of Transportation, the DMV, state and highway patrols, and the EPA, not through private IP enforcement. As we learned from Volkswagen's "Defeat Device," which allowed it to cheat on federal emissions tests for its diesel vehicles,[36] intellectual property laws that protect embedded software from independent testing and examination have potentially massive consequences for the environment, public confidence, and vehicle resale value.[37]

Fortunately, the Copyright Office, along with the National Telecommunications and Information Administration, agreed to allow vehicle owners to break DRM and access the software in their cars for purposes of security research, personal modification, and repair under a special DMCA exemption.[38] However, as noted, these exemptions last only three years. They are hardly a permanent response to these problems.

Not satisfied with controlling who repairs your vehicle, carmakers want to decide how you drive as well. Ford sells a car equipped with its Intelligent Speed Limiter, which uses onboard cameras to scan road signs for speed limits and then adjusts the fuel to prevent drivers from exceeding posted limits.[39] This sort of technology gives Ford an immense amount of information about your driving habits. As a Ford executive boasted in 2014, "We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing."[40] And while there may be good reason to embrace tools that reduce speeding and increase safety, they fundamentally change what it means to own the car you drive and the autonomy we are used to having inside it. As vehicles move toward computer-assisted and self-driving, the incidents of ownership will likely grow more and more distant.

For Ferrari, the antipathy toward owners reached new levels. The company now requires customers to sign a Right of First Refusal Agreement that bars the new owner of a $200,000 car from selling it without checking with Ferrari first.[41] The relevant part of the agreement reads: "Customer hereby grants to Dealer, as a material consideration for the opportunity to purchase [the vehicle], an option to repurchase the [vehicle] at its market value (but in no event more than the original Manufacturer's Suggested Retail Price) at any time within two (2) years of the date of delivery."

Granted, this is a purely contractual restriction. But it provides a window into the sort of control carmakers want over owners. Even more than contracts, software and the DMCA might give it to them.

Free as in Coffee

Those in the free software movement are fond of distinguishing between two ways in which we use the word "free." "Free as in beer" refers to price. "Free as in speech" refers to liberty, the freedom you have to use a thing as you choose.[42] Until recently, you could be confident that if you overheard someone talking about free coffee, it meant Starbucks was running a promotion. But thanks to Keurig, the maker of the popular K-Cup brewing system, conversations about coffee now have to account for questions of liberty as well.

The Keurig saga began in 2012, when several of the coffee company's key patents expired. Those patents covered its pod-based brewing system. Users placed single-serving portions of coffee or other brewed beverages in the machine, hit a button, and got a consistent drink each time. Without patent protection, Keurig had to contend with competition. As it turned out, Keurig wasn't a fan. Rival companies started producing compatible pods and undercutting Keurig's prices. In response, Keurig released new machines featuring "Keurig 2.0 Brewing Technology which reads each lid to deliver on the promise of excellent quality beverages."[43] Marketing speak aside, what that meant was that Keurig's machines would only accept pods embedded with a code that verified your coffee came from a licensed supplier. And it also killed off its generic pod that let you supply your own coffee grounds. If you tried to brew rogue coffee, your Keurig machine greeted you with this cheerful message:

The public reaction was swift and vicious. Angry Facebook posts and irate Amazon reviews flooded the Internet. As Brian Barrett wrote, "A coffee maker limiting your choice of grind seems as out of place as a frying pan dictating your eggs."[44] It didn't take long for competitors to capitalize on this outrage by cracking the Keurig DRM.[45] Coffee drinkers even figured out how to defeat it with a single piece of tape.[46] Soon Keurig was persuaded to reverse course, at least in part. It appears to be sticking to its guns when it comes to blocking pods from competitors, but it announced plans to reintroduce the My K-Cup product that allowed coffee drinkers to fill their own pods. Nonetheless, the company and its investors have paid a price for its overreach. Keurig stock dropped by 10 percent in the wake of the DRM controversy.[47]

The Keurig example shows that people still care deeply about owning and controlling their devices and that they have the potential to make their voices heard in the marketplace. But it also cautions that market pressure is often only partly effective in protecting consumer interests.

Open the Pod Bay Doors, Barbie

At this point, it should come as no surprise that the Internet of Things threatens our sense of control over the devices we purchase. However, those threats aren't limited to intellectual property and DRM; they also include battles for control over information about our behavior and our inner lives. One troubling example is the Wi-Fi-enabled Hello Barbie doll from Mattel. This IoT Barbie looks like many of her predecessors but offers a unique feature. She can engage in conversation with a child and learn about them in the process. Barbie does this by recording her conversations and transmitting them via network connections to ToyTalk, a third-party cloud-based speech recognition service. ToyTalk then uses software and data analytics to analyze those conversations and deliver personalized responses. It's an impressive trick, but the implications for our sense of ownership are quite shocking. For many children, talking to toy dolls is a way to share their unfiltered thoughts, dreams, and fears in a safe, private environment. But according to the terms of the Hello Barbie EULA, ToyTalk and its unnamed partners have wide latitude to make use of information about your child's conversations in ways that few parents would anticipate:

> All information, materials and content ... is owned by ToyTalk or is used with permission. ...
>
> You agree that ToyTalk and its licensors and contractors may use, transcribe and store. ... Recordings and any speech data contained therein, including your

> voice and likeness as may be captured therein, to provide and maintain the ToyTalk App, to develop, tune, test, enhance or improve speech recognition technology and artificial intelligence algorithms, to develop acoustic and language models and for other research and development purposes. ...
>
> By using any Service, you consent to ToyTalk's collection, use and/or disclosure of your personal information as described in this Policy. By allowing other people to use the Service via your account, you are confirming that you have the right to consent on their behalf to ToyTalk's collection, use and disclosure of their personal information as described below.

In other words, ToyTalk claims to own anything you, your child, or even their friends say to Barbie. Conversations with the doll are corporate property. The safety and privacy of a child's bedroom is compromised by the collection, sharing, and commercial use of those conversations. And while these services may offer benefits, they come with significant new risks. Shortly after the IoT-enabled Barbie shipped, security vulnerabilities that could allow hackers to intercept a child's conversations with the doll were revealed.[48] And those worries aren't just hypothetical. Around the same time, VTech—maker of the children's smartwatch Kidizoom and InnoTab mobile device—disclosed that more than six million children had their personal information, including photos and chat messages, stolen from VTech's servers.[49]

Hello Barbie is just the latest example of this trend of networked appliances. Samsung shipped a SmartTV with a default listening mode—and accompanying privacy policy—intended to continuously eavesdrop on viewers and send audio back via the cloud for analysis.[50] In a pitch to investors, Vizio recently touted the fact that its smart televisions will be able to detect any content that users watch, regardless of the source, and use that information to customize advertising and programming.[51] The June smart oven features cameras and software that can recognize the food you cook.[52] Google's Nest thermostat takes a similar approach to learning about you. Amazon's Echo, Apple's Siri, Microsoft's Cortana, and Google Now go a step further by encouraging us to interact with disembodied soothing, friendly, and—by default—female voices. Science tells us that we engage more readily with technology that mimics human interaction. A recent study showed that gamblers risk more on slot machines with humanlike features.[53] Of course, such services have the potential to offer real benefits. But such a service relationship comes not only with divided loyalties but also diminished autonomy. It is very different from owning an object completely and suggests we should be mindful of exactly who controls our relationship

with any object we purchase. A person's home may be their castle, but their appliances may belong to someone else.

Our Bodies, Our Servers

As if our connection to the Internet of Things wasn't intimate enough, network-enabled and software-dependent devices are now inside our bodies. When open source advocate Karen Sandler found out at age thirty-one that she could die suddenly from a heart condition, she did what most of us would do. She went to the doctor to fix it. In her case, that meant implanting a pacemaker-defibrillator in her chest to give her heart a jolt in the event it gave out. The device—about the size of an avocado—was literally a life-saving invention. But because it ran proprietary software, Sandler had no way to tell how it worked or how likely it was to fail. As she explained in an interview, "A statistic came out recently that 25 percent of all medical device recalls in the last few years have been due to software failure. When you read these statistics it becomes very personal."[54]

It turns out that Sandler's questions about her pacemaker weren't so easy to answer. Much like Apple and its iPhone, pacemaker manufacturers won't let patients look inside or test the devices they purchase. Nor are you allowed to read the data from your own device while you are at home or on the road—even in the midst of a medical emergency.[55] Instead, you can only access your health data from manufacturer-approved sources. And until recently, you couldn't even test your device to make sure it is functioning correctly or was running the latest software or security update. The reason for such restrictions? According to a filing with the Copyright Office, the Advanced Medical Technology Association "believe[s] that patients have an inherent right to access their own medical data, however, this in and of itself does not necessitate bypass of any intellectual property protections."[56] In other words, even if you own the physical parts of the pacemaker, the manufacturer's copyright trumps any claim you might have to see how it works or what data it collects on you—even when it is implanted inside your body.

Dana Lewis proved what patients can do when they own their devices and control their care. Lewis is a diabetic living in Seattle who relies on a glucose monitor and a handheld wireless device to alert her when her blood sugar is too high or low.[57] Yet Lewis often wasn't able to hear the alarm, especially when she was sleeping. So she and her partner, Scott Leibrand, built a new program that displayed blood sugar levels with new louder alarms and a snooze button. They even added the ability to send the

information to other mobile devices, such as Leibrand's Pebble watch. Next they turned to Lewis's insulin regime. Traditionally diabetics control their insulin levels manually. But Lewis and Leibrand began experimenting with the data to devise an algorithm specific to Lewis's needs—something that would automate and adapt based on the data her device was sending out. It could predict her insulin needs thirty, sixty, and even ninety minutes in the future. Eventually they hope to produce an artificial pancreas that will essentially automate this process. No IP law, and certainly not one designed to stop infringers from sharing movies online, should stand in the way of patients adapting equipment they own to keep them alive.

These concerns are not limited to those of us with life-threatening conditions. More than 20 percent of Americans currently use "wearables"—computing devices attached directly to your body.[58] When you buy a Fitbit wearable tracker, its Terms of Sale specifically state that "to the extent the Products contain or consist of software in any form ... such Software is licensed to you, not sold[.] Terms such as 'sell' and 'purchase,' as used in these Terms, apply only to the extent the Products consist of items other than Software."[59] Again all you own is the shell and the components. Everything digital—including physical storage media—belongs to Fitbit. While Fitbit's privacy policy does promise to remove personally identifiable information whenever it shares your records with third parties, it reserves the right to keep everything else indefinitely, even after you delete your account.[60] Every move you make, every step you take, Fitbit will be tracking you. And as Kate Crawford wrote, because the type of information collected by these devices is so personal, and so intimate, it is almost as if the device itself becomes a more authoritative source about us than we are.[61]

Network security has also become an issue for medical devices. From insulin pumps to cochlear implants and powered prosthetic joints, more and more medical devices rely on transmitting medical data to providers through Wi-Fi and Bluetooth protocols.[62] These connections have already opened the door to numerous security issues.[63] Even former Vice President Dick Cheney claims to have switched off the wireless functionality on his own pacemaker to prevent terrorists from hacking it.[64] Fortunately, much like with vehicle security testing, the Copyright Office granted an exemption for testing exterior medical devices and passively testing those that are implanted in ways that don't affect functionality.[65] The ability to innovate and improve these devices, however, remains highly contested.

Karen Sandler's dream of an open source pacemaker may inspire us, but it also presents complications. Open source could allow patients to examine, test, and improve devices in ways far more flexible and permissive

than the current proprietary model, but they don't give us autonomy in quite the same way as analog ownership. Instead they offer a future with different, more user-friendly restrictions to navigate. Focusing on medical devices, the argument for individual ownership and control resonates more viscerally. For the rest of the stuff we buy, the stakes may be lower, but the arguments are the same. If you don't own your devices, you can't repair or customize them. You can't innovate with them. And in the end, the products you buy may end up using you more than you use them.