DOI:10.1145/2903749

Jason Schultz

Law and Technology
The Internet of Things We Don't Own?

Who will control the 'ordinary pursuits of life' in the digital economy?

Cars, refrigerators, televisions, wristwatches. When we buy these everyday objects, we rarely give much thought to whether or not we own them. We pay for them, we possess them, we wear them or put them in our garages or on our shelves, so we have very little reason to question their legal status or their loyalties. Yet in the last decade or so, we have witnessed a subtle and effective shift to cede control over our purchases, especially when they contain software.

It began with digital content. Movies started telling us where and when they could be played. Soon our music informed us how many devices it would live on. Then our library books began to automatically re-encrypt themselves on the date they became overdue. Now our phones will not allow us to delete certain apps; our televisions listen for when we take a bathroom break, and mattresses can keep tabs on where we slept last night.

The integration of such smart product features with ubiquitous network connectivity, microscopic sensors, large-scale analytics, social information sharing platforms, and cloud storage has created a new generation of embedded systems, the Internet of Things (IoT). It is not like the Internet we once knew, and it is not a particularly new idea: embedded computing systems have been around for decades. But the speed of adoption and the diverse capacities of these devices are unprecedented.

The era of IoT has brought more than technological and social shifts. It has also created unusual legal uncertainties. Historically, purchasing consumer goods, even electronic ones, was largely governed by two areas of law: property and contract. The good was a piece of property. The purchase agreement was a contract. Apart from the occasional equipment rental or lease, if money changed hands, the good went home with its new owner. Quid pro quo.

IoT manufacturers and distributors are quietly attempting to shift the rules of ownership.

Even goods subject to other laws, such a copyright or patent, generally fell within this framework. As patent or copyright owners sold off individual books, movies, or machines, the law would "exhaust" any remaining intellectual property rights in that particular copy, prohibiting the IP owner, in the words of the U.S. Supreme Court, from interfering with the rights of purchasers to use it "in the ordinary pursuits of life." That meant the purchaser could use the item as she saw fit and then dispose of it, including reselling it, under whatever conditions she chose. These exhaustion rules originated from the long-standing common law regime of personal property, which generally forbids subjecting objects to ongoing restrictions, especially restrictions on resale.

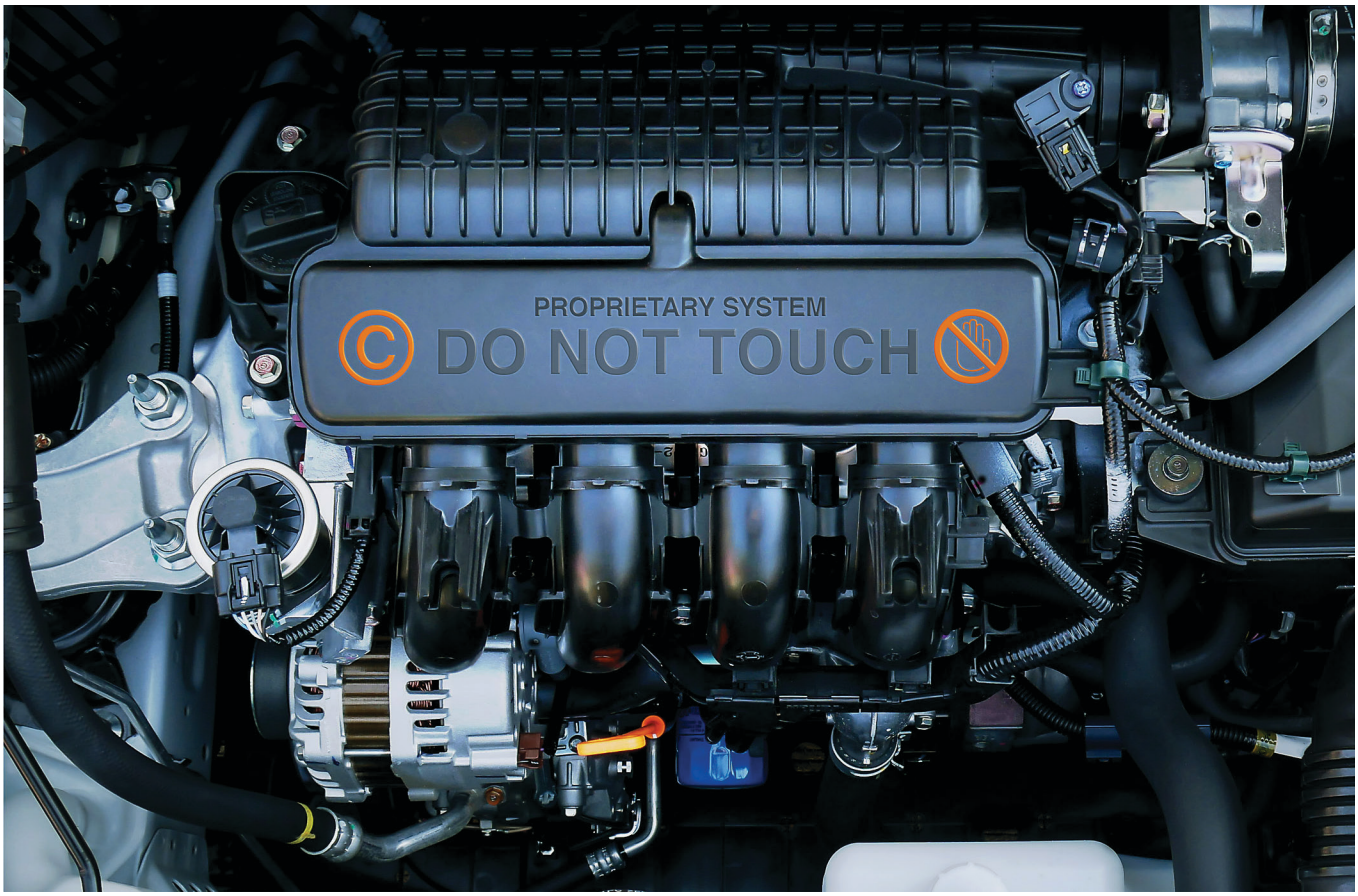

IMAGE COLLAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES

But that approach is under threat. Digital goods have pushed us away from traditional legal models, and, drawing from the world of software, now come with ubiquitous "Terms of Service" that few if any of us read. Within the dense legalistic language of these documents, IoT manufacturers and distributors are quietly attempting to shift the rules of ownership. For example, many now claim we do not own our phones, our cars, or even our televisions: we are merely "licensing" them. Others assert that when our devices break, it is illegal for anyone other than the manufacturer to diagnose the problem, let alone fix it. And others go even further, claiming any data captured by the device belongs to them and not the users who bought the device and created that data. And while users and consumer advocates have generally pushed back on these assertions, device manufacturers continue to push this view of the world upon us.

The exact origin of this shift 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." Like nearly every Apple product, the iPhone user experience was carefully choreographed and tightly controlled. What Jobs did not tell the crowd was that Apple's legal strategy to maintain ownership and control of the devices in our pockets and purses was equally choreographed and controlled.

Eleven days after the iPhone debuted, a group of skillful Apple enthusiasts decided to test its technological and legal limits by "jailbreaking" the phone. This led to a cycle where Apple would upgrade its systems to break the jailbreak and the jailbreakers would upgrade their breaks to free their phones from the upgrade. This battle over who "owns" the device continues to this day, with Apple insisting that "iPhone users are licensees, not owners, of the copies of iPhone operating software."

As contested ownership over smartphones has become more of a mainstream debate, the battle over IoT ownership has moved into more traditional pursuits of ordinary life. For example, just last year, farmers found out that many of them may no longer own the equipment they purchased, including even vehicles such as tractors and combine harvesters. Even 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. When tractors were purely mechanical, farmers could easily maintain, repair, and modify their own equipment as needed. But now, software stands in their way. 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 interpose a software layer between farmers and their tractors, claiming it retained ownership and that farmers merely had "an implied license for the life of the vehicle to operate the vehicle."

John Deere is not alone. Other vehicle manufacturers including Ferrari, Ford, General Motors, and Mercedes-Benz are finding new ways to use tech-

nology 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 her vehicle to get more horsepower or better fuel efficiency from the engine, the ambition of a growing group of car purchasers concerned about the environment calling themselves "eco-modders" and "hyper-milers." Yet under the ownership rules of the auto manufacturers, these hobbyists run the risk of becoming copyright infringers.

Such shifts in the battle over IoT ownership are also reaching into the security and safety research communities. As our vehicles incorporate greater computational systems with increased complexity, independent testing of their safety and security will increasingly require access to the copyrighted code inside them. Under the traditional law of personal property ownership, all researchers had to do was purchase a vehicle and then test it; manufacturers had no power to object other than to void the warranty. Despite Ford recalling half a million vehicles due to software glitches, Chrysler recalling 1.4 million vehicles because their infotainment systems were vulnerable to hackers, and notorious scandals such as the Volkswagen's "Defeat Device" that allowed it to cheat on emissions tests for diesel vehicles, we see more and more automakers claiming the code inside our cars is proprietary and access to it without their authorization is illegal. 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 this does not cover automobile owners.

So what does the law have to say about the question of IT ownership?

Nor are our children immune from this shift. Most children have imaginary friends and/or play with dolls. And while we are often surprised at the intensity of these relationships, we have historically understood they were private and ephemeral. Not anymore. Mattel's new WiFi-enabled Hello Barbie doll comes fully equipped with a built-in microphone and a cloud-based machine learning system to "personalize" your child's experience. However, what Barbie won't tell you or your child is that every single word or sound made in her presence will be recorded and transmitted back to Barbie's ML master archive for research purposes. In order to discover that, you would have to read her online Privacy Policy and Terms of Use. With the introduction of this capacity in our children's toys and other home devices such as the Nest thermostat and the Samsung "listening" SmartTV, the sense of privacy and autonomy we used to enjoy in our homes and with the objects we owned has become yet another contested space in the IoT era.

So what does the law have to say about the question of IoT ownership? To date, neither the courts nor Congress have resolved the question. In general, the courts are split on the exact rules for who "owns" embedded copyrighted media, including software. Some have taken a somewhat technocratic approach, simply deferring to whatever words the maker puts in her license or TOS, regardless of whether or not those words accurately reflect the realities of the transaction. Other judges, however, have been more cautious, recognizing that consumer expectations play an important role in transactions, especially those involving physical objects. The Supreme Court has come close to weighing in on the issue in some of its recent patent and copyright cases, but has not given us a definitive rule.

Even the Copyright Office has avoided opining, for example, choosing to grant smartphone jailbreakers an exemption from anti-circumvention liability under copyright law's fair use doctrine instead of declaring them owners with the right to modify embedded software. Recently, Congress has taken more action with Rep. Blake Farenthold introducing the You Own Devices Act (YODA), both houses beginning to examine the possibility of updating the copyright exhaustion rules for the digital age, and Senators Grassley and Leahy specifically asking the Copyright Office to analyze "how copyright shapes our interactions with software in things we own." The Commerce Department also recently issued a White Paper expressing concerns for consumers and the market if IoT manufacturers begin placing restrictions on the freedom to resell devices. But while many of these voices are asking good questions, none have provided the answers we need.

To find the answers, we will need to have a more open and honest conversation about ownership—in the courts, in Congress, and in the technical communities that are designing the IoT ecosystem. Hiding these conflicts and questions in shadowy TOS and embedded firmware code will only further confuse consumers and courts and ultimately complicate instead of clarify the rules we want when it comes to our ability to enjoy the ordinary use of these objects, including our ability to use them privately, to customize them to our needs, and even to part with them as we please. C

Jason Schultz (SchultzJ@exchange.law.nyu.edu) is Professor of Clinical Law at New York University's School of Law.

The argument in this column is further explored in the author's forthcoming book *The End of Ownership: Personal Property in the Digital Economy* (MIT Press, Fall 2016), with co-author Aaron Perzanowski.