The End of Ownership

Personal Property in the Digital Economy

OA Funding Provided By:

The open access edition of this book was made possible by generous funding from Arcadia—a charitable fund of Lisbet Rausing and Peter Baldwin.

The title-level DOI for this work is:

doi:10.7551/mitpress/10524.001.0001

7 DRM and the Secret War inside Your Devices

In Ray Bradbury's iconic dystopian novel *Fahrenheit 451*, a war rages in a future society over the existence of books. Those in power seek to destroy them, both because of the controversial ideas they disclose and because of their perceived limited utility in a society filled with video-enabled walls and mobile media devices. Those who rebel against these rules hide books to preserve them for historical, political, and philosophical reasons. Bradbury's infamous firemen—shock troopers who kick down doors and incinerate homes where books are hidden—and their mechanical drone-like hounds that sniff out literary contraband are meant as provocations to incite our fears that the very book we hold in our hands might be taken away from us at a moment's notice in the name of "public happiness." By personifying this version of absolute control, Bradbury makes clear that notions of personal property or domestic privacy stand no chance in a society that values centralized authority over individual autonomy and cultural heritage.

As a commentary on the McCarthy Era, Bradbury's work is a reaction to a specific threat to our engagement with ideas and the cultural artifacts containing them. And although the particular brand of control Bradbury had in mind has not manifested itself in contemporary U.S. culture, there is a different sort of threat to our freedom to read, explore, and share ideas—one that is more subtle, but all the more dangerous for it. This threat doesn't kick down your door in the dead of the night; it already lives in your home. It's embedded into the media you buy and stored on the devices you carry in your pocket. It doesn't rely on physical force or the power of the state to enforce its rules, just the often unseen operation of software code.

Digital Rights Management (DRM) is the euphemism for a range of technologies implemented by copyright holders, device makers, retailers, and other intermediaries designed to control how, where, when, and whether consumers can use their books, movies, music, and other content. In a nutshell, DRM is a digital guard capable of silently monitoring your digital activity and enforcing any restrictions or limitations demanded by rights holders. DRM can prevent you from copying a file, even for legally permissible reasons like personal backups. It can restrict your iTunes purchases to Apple-authorized products. Or it can prevent you from using your Kindle's read-aloud function to listen to a book—even if you are blind.[1] It can stop your DVR from recording your favorite show if the copyright holder objects.[2] Through region coding, DRM can stop you from watching a DVD you bought on vacation in London or Tokyo on your TV at home, or from using printer ink purchased abroad. It can even prevent you from skipping commercials and trailers before watching a movie that you own.

Push the limits of these rules, and DRM will push back. At that point, you will discover that your media and devices serve another master. Most of the time, they obey your instructions. But when your commands conflict with those of copyright holders, your stuff betrays you. Perhaps it simply refuses to execute a command, or it may politely inform you that you've exceeded your authorization. DRM might even disable your access or your device altogether. Much like *Fahrenheit 451*'s firemen and their hounds, if rather less imposing, DRM treats our access to the products we lawfully acquire as contingent and impermanent. DRM creates a world in which our purchases aren't in our control. Even our very possession of them is contingent on rules established by an external authority.

Consider the Apple iTunes DRM. For reasons we will discuss, Apple no longer sells music burdened by DRM. But movies and television shows, not to mention apps, are still subject to DRM. Apple spells out the substantive constraints of its DRM in its Usage Rules, which it "reserves the right to modify ... at any time." Your behavior will be "monitored by Apple for compliance purposes," and Apple can "enforce [its] Usage Rules without notice." Those rules provide in part:

> - You shall be authorized to use iTunes Products only for personal, noncommercial use.
> - You shall be authorized to use iTunes Products on five iTunes-authorized devices at any time.
> - You shall be authorized to burn an audio playlist up to seven times.
> - You shall not be entitled to burn video iTunes Products or tone iTunes Products.

The specific restrictions imposed by any DRM system are less important than the underlying dynamic they represent. Those restrictions were not created by law. Nothing in the Copyright Act even hints that creating seven audio playlists is lawful, but the eighth crosses the line of infringement.

These rules are not the result of a legislative process or judicial analysis. They enshrine an agreement reached between a retailer and a set of publishers and foisted on the public. Unlike the law, DRM allows for automatic enforcement. We've replaced courts and due process with code and license terms. The law can account for context and tolerate gray areas. It can make exceptions. DRM cannot. It hardwires restrictions on consumer behavior into our devices, robbing them of functionality.

While not nearly as dramatic as flamethrowers and fighting robot dogs, the unilateral right to enforce such restrictions through DRM exerts many of the types of social control that Bradbury feared. Reading, listening, and watching become contingent and surveilled. That system dramatically shifts power and autonomy away from individuals in favor of retailers and rights holders, allowing for enforcement without anything approaching due process.

Imagine if a physical book publisher tried to create similar rules: you can read at night, but not during the day; you can read on the beach, but not on the subway; you can only loan the book to a friend once;[3] and you can't skip the preface.[4] None of us would feel compelled to comply with these demands. No court would call you an infringer, and few would even find an enforceable contract. And the publisher would have no way to find out about our violations or force compliance. But because digital works depend on software and often network connections, copyright owners can construct technologies that impose their whims on us. That power, particularly when it is reinforced through law, creates no shortage of harm.[5]

Smart Cows and Dumb Code

The first efforts to use technology to prevent copying emerged in the early days of the retail computer software industry. In those days, users shared time on mainframes and often wrote their own code. Later, hardware makers viewed software as a tool to drive computer sales. But once software was understood as an independently marketable product, some software makers saw the ease of copying floppy disks as a problem in need of a technological solution. Aside from casual sharing of software among friends and colleagues, swap meets and flea markets began to include computer software—both legitimate and infringing copies among their wares—or warez, if you are of a certain generation. This period of unauthorized distribution had some unexpected consequences; it led to later commercial success for companies that built loyal user bases for future products. It also encouraged innovation. One early video game, *Spacewar!*, was improved and developed in part through unauthorized copying. Even Bill Gates, whose attitude about copying shifted significantly during his tenure at Microsoft, learned to program on unauthorized software.

But understandably, most software companies wanted to cut down on unauthorized copies in order to improve sales. Some attempted to impose speed bumps—relatively minor impediments that would slow down the rate of copying and separate legitimate purchasers who wanted to make backups or share with a few friends from rogue copyists. These early DRM technologies included the linguistically and logistically awkward dongle—a hardware device that had to be inserted into the input/output port of your computer before the software would run. In other cases, DRM was tied to software documentation. For example, on launch a program would prompt the user with a question like, "What is the first word on page 14 of the user manual?" Of course, in response users began exchanging information about how to circumvent these systems, quickly diminishing them to mere annoyances, a pattern that would repeat itself with increasing speed for every DRM system to come.

In the 1990s, this small-scale arms race began to heat up as copying and storing large numbers of software titles became easier because of vast improvements in storage capacity and disk speeds. Coupled with the increasing ease of data transmission over the newly popular Internet and the introduction of peer-to-peer networks like Napster, designed for sharing files with a global community, the perceived need for DRM increased dramatically. Soon copyright holders, who now included Hollywood and the music industry in addition to software makers, invested more and more resources in the hopes of finding a technological fix to the problem of unauthorized copying.

But what proponents of this silver bullet strategy failed to understand, at least initially, is that every DRM system is susceptible to attack. That's theoretically true of every system for obscuring or encrypting information. But DRM, by its very nature, is particularly vulnerable. Normally, if you buy a lock to protect valuables inside your house, you lock the door to outsiders. And you keep the key safe in your pocket, sharing it only with insiders such as family or friends. Outsiders might try to break in, but as long as the lock is well made and they don't get their hands on the key, most will be deterred. With DRM, however, the threat is not from outsiders. It's the insiders rights holders worry will make off with the valuables.

A DRM system that locks out consumers altogether has no value. If Apple's DRM, for example, refused to let you watch a movie after paying for it, even the most fervent Apple loyalists would get their digital movies elsewhere. To let customers watch their movies, Apple has to share the key to this digital lock at some point. Since most of us are not particularly tech savvy, DRM makers share the key, but they hide it somewhere we are unlikely to find it. Cryptography works well in preventing attacks from outsiders who want to intercept a message. It is bound to fail when it is used to protect against misuse by the intended recipient of that message. Given enough time and users, discovering the key that unlocks any given DRM system becomes inevitable and often trivial. There are just too many ways to pick a lock from the inside.

And once a single sophisticated user unlocks a DRM system, it usually doesn't take long until the average person can remove that DRM with the push of a button—or simply download an unencumbered copy from the Internet. The inescapable challenge is what Mike Godwin, a pioneering technology lawyer, once called "the problem of the smart cow."[6] Imagine every single cow in the world locked up in a giant barn with a state-of-the-art lock. No matter how good the lock, eventually one cow will figure out how to escape. Once that cow is out, the other cows—no matter how unskilled at lock picking—are out too. This is the second fundamental flaw in the DRM approach. All it takes is one motivated and skilled person to defeat DRM.

In response, DRM makers have pushed for tighter control over more components of the distribution and playback chains, undermining consumer ownership of their devices and software each step of the way. In the process, DRM has shifted from a largely benign form of authentication to a technologically embodied philosophy that views all users—customers included—as threat vectors, monitoring their actions and enforcing limits on their use of the things they buy. Lawful, mundane consumer behavior—watching movies, listening to music, reading ebooks, or making backup copies—are regulated by code. For many people, the frustration and inconvenience of DRM makes paying for content look like a poor value when DRM-free versions of the same works are widely available. When DRM treats paying customers like criminals, denying them the freedom to use their devices as they see fit, it actually encourages them to infringe.

The Battle for Your Living Room

The transition from a market in which people truly owned and controlled their devices to one tightly regulated by technologies that owe us no real allegiance can be illustrated in the contrast between two familiar technologies: the VCR and the DVD player. The VCR, which hit the U.S. market in the late 1970s, empowered the individual. By owning this device, people could assert a degree of control over their television viewing experience that we take for granted today, but was unheard of at the time. No longer subject to the minor tyranny of broadcast schedules, viewers could record shows and watch them at a time of their choosing and on their own terms.

Faced with this prospect, copyright holders were gripped by a hysteria that seems almost laughable in retrospect, but was earnestly felt at the time. Jack Valenti, president of the Motion Picture Association of America, testified before Congress—with a straight face—that "the VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone."[7] Unable to convince Congress to ban the VCR, a group of movie studios, led by Universal and Disney, sued device maker Sony in 1984.

Universal accused Sony of creating a piracy machine that allowed viewers to make illegal copies of broadcast television programs. Although the VCR was certainly used by some to create infringing stockpiles of shows and movies, it was also commonly used for legitimate purposes like time-shifting—the practice of recording a show to watch later. Some producers, notably PBS mainstay Fred Rogers, had no objections to viewers making recordings, in part because it enhanced consumer control. Rogers understood that once a person bought a VCR, it gave the buyer newfound power. Hollywood had no practical means of controlling what they did with their personal property. And once VCRs were in the market, neither did Sony. It had no way of tracking how people used the device, no knowledge of their choices, and no way to limit them. So the studios urged the U.S. Supreme Court to impose legal control over the design and use of the VCR instead. But the Court refused for two interrelated reasons.

First, the Supreme Court ruled that Sony could not be held responsible for designing and selling the VCR if it could be used for both legitimate and illegitimate purposes. If the design of general-purpose devices like a VCR were controlled by content owners, their functionality would be limited to features that supported Hollywood's business plans at the expense of Sony's interest in producing the most attractive device and the public's interest in controlling its viewing experience. Second, the Supreme Court decided that the VCR was in fact capable of substantial non-infringing uses. It found that many VCR owners used them for time-shifting, which the justices deemed a fair use of broadcast television programming. According to the Court's decision, "the business of supplying the equipment that makes such copying feasible should not be stifled simply because the equipment is used by some individuals to make unauthorized reproductions."

The *Sony* decision, while it benefitted device makers most directly, more subtly vindicated the personal property interests of consumers. It protected their right to acquire general-purpose technology, even if it could be used to infringe. It reaffirmed that we can use the devices we own in non-infringing ways despite the objections of copyright holders. And it protected our living rooms from the kind of surveillance and supervision that would be necessary to police the private use of property.

But the Court's decision in *Sony* sent shock waves through Hollywood. Unlike record labels and publishers, which were accustomed to the unavoidable loss of control that comes from selling copies to the public, the movie industry resisted loosening its grip on its works. Traditionally, studios were able to police public consumption of their works because viewers accessed them through public exhibition, not private taping or sales of copies. They were either shown in movie theaters or over broadcast television and could be tracked accordingly. Even the theaters that showed films didn't own the prints. They typically remained the property of the studio and had to be returned. The idea that an individual could own a copy of *The Good, the Bad and the Ugly*—by recording it from a broadcast, no less—represented a dramatic shift in the power dynamic between copyright holders and consumers.

Even after the VCR was introduced, Hollywood resisted the home video market. Titles were withheld from release or priced extravagantly. In part, that's because Hollywood had its own vision for the home video market, and it didn't include the record button. Universal and Disney supported a competing technology, DiscoVision, which allowed viewers to watch movies at home on large optical discs, predecessors to laser disc and DVD technology. But DiscoVision, unlike the VCR, didn't support recording over-the-air programming or private copying. The design of the technology precluded those lawful behaviors. And as a result, it didn't stand a chance in the market. Instead, Hollywood watched as the VCR emerged as the dominant technology.

But Hollywood learned its lesson. When it came time for home video—by then the movie industry's primary source of revenue—to make the transition to a digital format, the studios threw their weight behind the DVD, in part because it enabled the kind of control over copying that VHS tapes never did. When the DVD was introduced in 1996, virtually every commercial release featured a new DRM system called the Content Scramble System (CSS). By encrypting the contents of DVDs, CSS promised copyright holders much more control over what viewers did with the movies they purchased. Playing a movie requires a secret key, and those secret keys are only available to authorized devices. A device maker who wants to manufacture a DVD player has to get permission from the DVD Copy Control Association, an organization made up of major movie studios, DRM vendors, and Hollywood-friendly DVD manufacturers. Not surprisingly, device makers interested in adding features that Hollywood found threatening—like the ability to make backup copies of DVDs, record televised programming, save small clips for educational use, or even skip previews or advertisements—were not approved.[8] DVDs, like their Blu-ray successors, even use region coding to prevent playback of lawfully purchased and imported discs.

Through their tight control over the design of the DVD format, movie studios achieve the goals that the Supreme Court denied them in *Sony*. If Jack Valenti can get away with analogizing the VCR to the Boston strangler, we feel confident noting the parallels between the DVD player and the Trojan horse. Enticed by the prospect of high-quality digital home video, viewers embraced this new technology. But Hollywood understood the DVD format as a means to infiltrate our living rooms and to turn our home entertainment systems into covert assets. By controlling how we use the devices we assume we own, studios could regulate our private activities, including those outside the scope of any copyright interest.

DRM Goes to Washington

For a time, that strategy worked just as Hollywood had hoped. But like all DRM systems, CSS had a fatal cryptography problem baked into its design. It was only a matter of time until someone found the secret key that unlocked DVDs for licensed and unlicensed players alike. And in 1999, CSS was cracked. We will return to that story shortly, but first we should discuss the steps Hollywood took to prepare for this inevitable outcome. Copyright holders who enthusiastically adopted DRM understood that code alone would never be enough to maintain control over consumer behavior. They needed to enlist the law. But early cases gave copyright holders very little confidence that the courts would reinforce the non-legal rules DRM tried to implement.

Two cases from the period between the *Sony* decision and the introduction of the DVD illustrate the problem. The first involved software company Vault, an early DRM pioneer. It sold a program called Prolok that was intended to stop unauthorized copying of software. To do so, Prolok stored a digital fingerprint on disks and prevented computers from accessing the contents of those disks if the fingerprint was missing. Quaid Software looked at Prolok and saw an opportunity. It created a program called Ramkey and its own storage disks that imitated the Prolok fingerprint and effectively broke Vault's DRM. Quaid sold Ramkey as a backup utility, a function that Prolok prohibited legitimate purchasers of software from performing. Vault sued Quaid, claiming that defeating its DRM violated copyright law.

The Fifth Circuit Court of Appeals, much like the Supreme Court in *Sony*, decided the case by looking to the behavior of users who bought Ramkey. Although some were engaged in infringing distribution, a substantial number used it to make perfectly lawful backup copies of software they owned. Because backing up software you own is legal under the exhaustion principle and specifically section 117 of the Copyright Act, the court was convinced that Quaid couldn't be held responsible for those who used the program for less laudable purposes. Breaking, disabling, or avoiding DRM was not, in itself, illegal.

A few years later, the Ninth Circuit underscored that point in a case brought by Sega, developer of the Genesis video game console. Sega made its own titles for the Genesis system, but also licensed third-party developers to create compatible games. Accolade was unwilling to agree to Sega's licensing terms, which required that Sega, rather than Accolade, manufacture the game cartridges. So instead, Accolade decided to create Genesis games without Sega's approval. It purchased a Genesis console and three Sega game cartridges to discover the interface specifications that allowed the game to communicate with the console. In the process, Accolade discovered Sega's DRM, the trademark security system (TMSS). TMSS was, truth be told, a terrible DRM implementation, even by the low standards of the field. It consisted of little more than a twenty-byte initialization code followed by the letters S–E–G–A. The console searched the game cartridge for the initialization code in a specified location. If it found it, the game would load.[9] If not, gamers saw a blank screen. Accolade copied this lockout code onto its own cartridges to render them compatible with the Genesis hardware.

Sega sued, arguing that Accolade infringed its copyrights by copying its game code in the process of reverse engineering the Genesis interface and implementing TMSS. The court disagreed. Even though Accolade copied Sega's software code in its entirety, it had to in order to figure out how the Genesis communicated with games. That interface information and the TMSS lockout code are beyond the scope of copyright protection, the court held, because they serve a purely functional purpose. Just as in *Vault v. Quaid*, copyright holders were rebuffed in their efforts to use copyright law to stop consumers and competitors from defeating their DRM.

In response to these losses, copyright holders took their case to Congress. In the face of ubiquitous personal computing, new digital media formats, and the popularity of the Internet, they argued that some legislative intervention enshrining the DRM strategy was necessary. Their decade-long effort culminated in two laws—the Audio Home Recording Act (AHRA) and the Digital Millennium Copyright Act (DMCA). The first was narrowly focused on a single technology and is viewed by most legal commenters as a footnote—or perhaps a punchline—in the history of legal regulation of technology. The second was motivated by grander ambitions and has had a lasting impact, though not for the reasons its proponents anticipated.

The AHRA addressed digital audio tape (DAT), which was billed as the next hit format for recorded music after the introduction of CDs. Because DAT allowed for digital copying, copyright holders worried it would lead to widespread infringement. So they convinced Congress—in exchange for granting DAT player manufacturers immunity from copyright infringement claims—to require all DAT players to include DRM.[10] The statute makes it illegal for anyone to manufacture, distribute, or import a DAT player unless it incorporates the Serial Copy Management System (SCMS) or its equivalent. SCMS itself was a simple system that encoded data in DAT recordings that dictated whether additional copies could be made. A record company could, for example, prohibit copies altogether, permit a single copy to be made, or allow copies without restriction. Despite the deep degree of congressional oversight into the design of DAT—or perhaps because of it—the format was a flop in the United States.

Six years later, Congress took up the DRM question again. By the late 1990s, the Internet's potential as a digital marketplace had been recognized but not yet realized. Digital distribution of music and other content was technologically feasible, but because of understandable fears that their products would be freely and widely copied, copyright holders were reluctant to experiment with digital marketplaces. They argued that legal protection for their DRM schemes would give them the confidence necessary to take their first tentative steps toward online marketplaces. Congress responded by passing the Digital Millennium Copyright Act (DMCA) of 1998.

The act had two major components. The first created safe harbors from copyright liability for Internet intermediaries like search engines and ISPs. The second was meant to bolster DRM. Section 1201 of the DMCA made it unlawful to circumvent—that is, bypass, disable, or remove—any technological measure that restricted access to copyrighted material. Essentially, it made breaking DRM illegal, even if doing so did not result in copyright infringement. To return to Mike Godwin's cow parable, it's a rule meant to stop the smart cow. But the DMCA had a strategy for dealing with the dumb cows as well. Section 1201 made it illegal to make or distribute tools or technologies designed to circumvent. So even if some motivated teenager well outside the reach of the U.S. legal system cracked a new DRM scheme, anyone who shared a software program implementing that crack was on the hook as well. These anti-circumvention provisions are subject to a number of narrow and largely ineffective exemptions for activities like reverse engineering and encryption research. The Copyright Office even holds a process every three years to decide on temporary exemptions from these rules. The exemption process forces consumers to bear the heavy burden of establishing that their use of the devices and content they own are lawful. And these exemptions only address potential liability under the DMCA; they offer no protection against traditional copyright infringement claims. Even when exemptions are granted, they are based on existing harms to consumer rights that often highlight the absurd overreach of section 1201. Since their implementation, the anti-circumvention rules have consistently undermined the property relationship between consumers and their stuff by giving legal weight to DRM's intervention.

DRM Goes (Back) to Court

Fresh off their victory in Congress, copyright holders began targeting defendants who made or distributed tools that helped defeat DRM. And their track record in those cases suggests that the DMCA gave copyright holders just what they had asked for.

In the first of these disputes, RealNetworks—an early provider of streaming media content—sued a company called Streambox. RealNetworks developed technology for streaming audio and video files. It relied on a digital "secret handshake" between its server and its player to ensure that third-party applications could not stream RealMedia files. Without the secret handshake, an application was denied access. Streambox developed the "VCR," an application that mimicked the secret handshake to interoperate with RealNetworks' server in order to enable the same sort of time-shifting the Supreme Court okayed in *Sony*. Yet when RealNetworks sued, the court had no trouble finding that the VCR software circumvented RealNetworks' DRM because section 1201 had shifted the balance of power in favor of copyright holders.

After this promising test run, copyright holders set their sights on a bigger target. A Norwegian teenager named Jon Johansen solved the puzzle of CSS, the DRM on DVDs, in 1999. He then wrote a simple program called

DeCSS, which decrypted the content of any DVD. Johansen's goal was to enable DVD playback for users of Linux operating systems. Although there were plenty of licensed DVD player software options for Windows and Mac users, there wasn't a single Linux-compatible program on the market. That meant those Linux users who had lawfully purchased DVDs couldn't watch them on their desktops or laptops.

When DeCSS was subsequently published across the Internet for the world to see, it caught the attention of Eric Corley, a journalist and publisher of *2600: The Hacker Quarterly*. For years, *2600* served as a news outlet and forum for the hacker community, broadly defined. Corley wrote a story about DeCSS and published it on his website, along with the DeCSS code and links to other sites hosting the code. As he would reiterate later in court, Corley added the code to the story because "in a journalistic world, … you have to show your evidence."[11]

Eight movie studios quickly filed suit against Corley and others, claiming that by publishing DeCSS they trafficked in technologies that circumvented DRM in violation of section 1201. The defendants pointed to a number of non-infringing uses DeCSS made possible. They included the time-shifting so crucial in *Sony* and the backups found lawful in *Vault.* Even more intuitively, they argued that DVD owners had the right to play their discs on their own hardware, just like any other item of personal property. But the court held that the legality of these uses was irrelevant to the question of anti-circumvention liability. That charge did not hinge on any act of infringement, much less the question of substantial non-infringing use. The studios had succeeded in Congress where they had previously failed in the courts. Breaking DRM was unlawful, regardless of the reason. Personal property rights had to give way to copyright owner control. DeCSS was banned, and other courts soon followed suit.[12]

A Failure, at Best

Given these decisive early legal victories, copyright holders could be forgiven for deeming the DMCA a rousing success. But any champagne popping that happened in 2001 would soon prove premature. Even from the perspective of copyright holders, the DMCA's anti-circumvention provisions would be charitably described as a mixed bag. And from the perspective of the public, the DMCA has been an unmitigated disaster. It has jeopardized their privacy and security, impeded innovation and encouraged lock-in, and paved the way for an unprecedented loss of control over the devices they own.

The DMCA has not achieved its stated goals. Almost every major commercial DRM system introduced since it was enacted has been broken, and at an increasingly rapid pace.[13] It took three years from the introduction of DVDs for Johansen to crack CSS—not bad, considering he was twelve at the time CSS was released. By the time Apple launched its iTunes FairPlay DRM in 2003, Johansen had more coding experience under his belt. He circumvented that one within a few months. A few years later, the "unbreakable" BD+ DRM used on Blu-ray discs was broken within a month. Princeton researcher Ed Felten led a team that defeated the music industry's Secure Digital Music Initiative in just a matter of weeks. And game maker Ubisoft's DRM didn't even last a day.[14] It would appear there are just too many smart cows out there. Nor has the DMCA been effective in clamping down on the availability of circumvention tools for the rest of us. Any middle schooler with a smartphone and a few minutes to spare can find them. Or so we've been told. As a result, titles protected by DRM find their way to file sharing networks and other sources of infringing material just as quickly as their non-DRMed counterparts.[15]

The other pitch for the DMCA—that it was necessary to convince copyright holders to risk the waters of digital distribution—turned out to be false. It may have been true in the late 1990s, but it certainly isn't anymore. In fact, DRM often hurts copyright holders as much as it helps them. The market rewards publishers who abandon DRM and punishes those who insist on it.[16] This rise and fall of DRM for digital music downloads is instructive. When Apple launched the iTunes Music Store, the first licensed digital music download store to feature content from the major labels, every track was wrapped in its FairPlay DRM. To hear Steve Jobs tell it, the labels insisted on DRM, and Apple played along. As he wrote in his widely circulated open letter, Thoughts on Music: "When Apple approached these companies to license their music to distribute legally over the Internet, they were extremely cautious and required Apple to protect their music from being illegally copied. The solution was to create a DRM system, which envelopes each song purchased from the iTunes store in special and secret software so that it cannot be played on unauthorized devices."[17] If that's the case, the labels came to regret their insistence once they discovered that DRM benefitted Apple much more than it did copyright holders.

Through a combination of being first, creating a seamless experience for end users, and designing gorgeous devices, Apple soon became the top music retailer in the world. Once it established its dominant position, record labels got their first glimpse of the dangers of DRM. Apple's FairPlay-protected tracks, which music fans collectively spent tens of millions of dollars buying, couldn't be played on competing hardware. The costs of switching from an iPod to a Zune—remember those?—were too high for most people to bear. That hurt competition among device makers and music stores alike. So DRM reinforced Apple's dominant position and weakened the labels' leverage to negotiate over prices, promotions, and other concerns.

Apple was so committed to maintaining this tight control over the retail download market that when one-time DRM crusader RealNetworks created a software tool called Harmony that allowed customers of its competing music store to replicate FairPlay DRM so that tracks purchased from RealNetworks could be loaded on iPods, Apple called them hackers and threatened a DMCA suit. Nearly a decade later, a key Apple engineer even testified that the company's DRM was part of an anti-competitive strategy.[18]

At this point, the labels figured out that the only way out of this mess was to free themselves from the chains of DRM. As Cory Doctorow explains in his book *Information Doesn't Want to Be Free*:

> The labels came to realize that they'd been caught in yet another roach motel: their customers had bought millions of dollars' worth of Apple-locked music, and if the labels left the iTunes Store, the listeners would be hard-pressed to follow them. ... But Amazon offered the labels a lateral move: give up on digital rights management (DRM) software and sell your music as "unprotected" MP3s (which also play on iPods), and you can start to wean your customers off the iTunes Store—or at least weaken its whip-hand over your business. You can set your own pricing, Amazon said; we'll help you with the promos you're looking for, and together we can get some competition into the market. The music industry bought into it, and iTunes dropped DRM not long afterward.[19]

A Disaster, at Worst

As bad as DRM ended up being for the music industry, it has been worse for the public. The lock-in problems that finally convinced the record labels to jettison DRM, for example, were felt acutely by consumers. Many of us are attracted to digital copies because of their relatively low prices. Oddly, digital copies are more than occasionally more expensive than their digital counterparts. But digital usually wins on sticker price. When you can pay $8.99 for an ebook instead of $22.99 for a hardcover, it seems like an easy call. But those low prices are misleading. If you can't resell your books, you can't recoup any of your costs. Tired of the latest dystopian young adult novel? Too bad; you're stuck with it. Before DRM, you could always head down to the local used bookstore or flea market to sell your hardbacks and paperbacks. With DRM, your purchases are tied to a particular technology platform. And that fact raises the cost of switching to a new platform, which in turn means less competition and higher prices.

Because it often requires ongoing communication or authentication, DRM focuses on the present rather than the future. Content is generally most valuable in the initial period after its release.[20] After that, content producers, DRM vendors, and device manufacturers have significantly reduced incentives to respond to concerns about DRM. The short history of DRM is littered with the remains of failed or abandoned protection measures, too often leaving the files they supposedly protected locked away. This leads to problems of unavailability and obsolescence. It also creates serious barriers to preservation. Even without DRM, these are thorny issues. DRM only makes them worse.

Ownership unfettered by DRM encourages innovation, customization, exploration, and repair.[21] This "freedom to tinker," as Ed Felten calls it, allows individuals to contribute to technologies, often in ways that the original manufacturer can't or won't.[22] We see this threat most vividly in connection with the growing class of software-controlled and network-connected devices that make up the so-called Internet of Things. We turn to those in chapter 8. But it's equally true for digital media.

For example, when gamers discovered a way to change the appearance of characters in *Ninja Gaiden*, *Dead or Alive 3*, and *Dead or Alive Xtreme Beach Volleyball*—admittedly, in some cases to make them appear nude—video game publisher Tecmo sued.[23] These enhancements didn't enable infringement; they could only be used by owners of the games in question. If anything they added to the appeal of and demand for the games. Nonetheless, Tecmo sued the tinkerers who created the modifications and the website that hosted them. The suit was dropped only after the site was taken down. Similarly, Blizzard—the maker of *World of Warcraft*—used the DMCA to target volunteers who developed software that allowed owners of its games to play together online.[24] Years later, Blizzard again relied on the DMCA to stamp out a program called Glider that allowed players to automate repetitive tasks like farming, crafting, and collecting items.[25]

There's no shortage of DRM horror stories, but perhaps the most egregious one took place in 2005, when Sony—once a staunch defender of consumer autonomy—hijacked the computers of nearly two million customers.[26] Sony, gripped by the fear of peer-to-peer infringement, decided it was necessary to prevent CD owners from copying their music to their computers. Writing software that prevents CD ripping is an easy enough task. But since people own their computers, they can decide what software to install and what software to delete. That posed a problem for Sony since, of course, no one would actually want to install a program that crippled their computer and made their CDs less valuable. So Sony needed a way to hide its DRM on customers' computers to prevent them from deleting it.

Sony used a tool called a rootkit, rarely employed by legitimate software developers, to achieve this subterfuge. Rootkits are programs that covertly modify a computer's operating system to blind it to certain files and processes. Once a computer has been compromised by a rootkit, it hides any files that meet certain criteria from both the computer's user and the machine's operating system. So if you open a folder containing a malicious program on a rootkit-infected computer, you won't see it. Or if you use an activity monitor to view the processes currently running on your machine, the hidden program—in this case Sony's DRM—won't be visible.[27]

If all Sony's rootkit did was allow it to hide its copy protection software, that would be bad enough. It's an underhanded move that denies people the right to control what code is running on hardware that they own. But the impact of the rootkit went well beyond DRM. It created security vulnerabilities that left users open to an array of potential attacks. Sony's rootkit was programmed to hide any file or process that began with the prefix "sys." If an attacker wanted to install malicious code on your machine and make sure it went unnoticed by you, your operating system, and your anti-virus software, all they would have to do is add that prefix to the file name.

The range of attacks that could exploit this vulnerability is limitless. The user's data could be altered, deleted, or even held for ransom; the machine could be rendered inoperable; a program could sniff sensitive passwords or collect financial records and other personal data. The list goes on; just use your imagination. The threat was more than theoretical. Within days of the public learning about the rootkit, malicious code leveraging it was spreading across the Internet. A program called Backdoor.Ryknos was transmitted via spam email. Once on a user's system, it opened a communications channel that let the attacker remotely control the user's system—downloading, deleting, and executing files, and gathering and sending information from the compromised machine. So while Sony customers nominally owned their computers, they no longer controlled them.

After independent discovery of the rootkit by at least three different groups of researchers—one of which, in full disclosure, was represented by one of this book's authors—Sony was forced to confront its decision when Mark Russinovich went public with his findings. The response from Sony—then the world's second-largest record label—was underwhelming. First, it downplayed the importance of the rootkit. Thomas Hesse, president of

Global Digital Business, asked, “Most people, I think, don’t even know what a rootkit is, so why should they care about it?” Eventually, Sony released tools to uninstall its DRM and the associated rootkit, but those tools caused security concerns of their own. Finally, Sony recalled millions of unsold infected CDs.

The Sony rootkit incident reveals, in an admittedly dramatic fashion, the underlying problems with DRM. The devices and content that consumers reasonably believe they own are guided by secret loyalties and hidden agendas that run counter to consumers’ best interests. The things we buy are technologically tethered to their creators, subject to ongoing surveillance, recall, or even destruction. They are not under our control. The rootkit incident also exemplifies the attitude behind DRM. We are not to be trusted, not even with our own computers. And our interests in autonomy, security, and privacy are secondary to rights holders’ perceived need for greater control over our behavior. Copyright holders, in condemning infringement, often implore the public to show greater respect for property rights. They might try taking their own advice.

The Effort to Copyright Garage Door Openers

In light of the power the DMCA created to control how people use technology, it was only a matter of time until DRM spread beyond traditional entertainment industries to companies in other sectors. Soon we began to see DRM inside common everyday devices like garage door openers, printers, and coffeemakers. These efforts sought to control consumer behavior not out of a fear of infringement, but as a strategy to reduce competition from firms that wanted to lure customers away with cheaper alternatives. With section 1201 as a powerful new tool, electronics companies had strong incentives to put DRM everywhere.

As DRM-restricted products hit the market, competitors of course found ways to circumvent those controls. Predictably, litigation soon followed. One of the first examples was in 2002, when Chamberlain, a maker of garage door openers, sued its competitor Skylink for making an inexpensive universal remote that could be programmed to open almost any garage door, including those made by Chamberlain. Skylink marketed its remotes as replacements for customers who lost their original Chamberlain remote or as an additional remote for drivers who had second or third vehicles. Chamberlain sold its own replacement remotes for a hefty sum, a market it wanted to control exclusively. So Chamberlain embedded DRM in its garage door opener that required remotes to send a proprietary code before they could open the door. After some experimentation, Skylink discovered the algorithm for this secret code and built it into its own remote.

Chamberlain sued, arguing this was an act of circumvention. The court, recognizing the obvious tension between the personal property rights of owners of garage door openers and the claimed IP rights of Chamberlain, rejected this attempt to expand the reach of the DMCA. As the district court explained, "A homeowner who purchases a Chamberlain [garage door opener] owns it and has a right to use it."[28] The owner of the device can use it in ways that conflict with the prerogative of its manufacturer. On appeal, the Federal Circuit held that claims under section 1201 needed to establish some relationship between the circumvention of DRM and a plausible act of copyright infringement. But that nexus was missing here because "consumers who purchase a product containing a copy of embedded software have the inherent legal right to use that copy of the software."[29] Again, ownership undermined the effort to control how consumers used their devices.

A similar case was filed that same year by printer manufacturer Lexmark against Static Control Components, Inc. (SCC), an aftermarket supplier of replacement parts and ink cartridges. Much like razor companies that make most of their money on replacement blades, Lexmark relied heavily on sales of expensive ink cartridges. SCC competed by selling its own compatible cartridges. Like Chamberlain, Lexmark embedded DRM in its printers and cartridges that prevented its printers from accepting non-Lexmark cartridges. SCC reverse engineered the system and designed its own cartridges to be compatible by fooling Lexmark's DRM. Lexmark sued SCC, claiming that by plugging a rival cartridge into the printer, owners of Lexmark printers were circumventing the company's DRM. But like Chamberlain, Lexmark was rebuffed. As the court explained it, "Purchase of a Lexmark printer ... allows 'access' to the program" that runs the device.[30] So Lexmark's effort to assert ongoing control over that piece of personal property failed.

These cases show that courts are still sensitive to the concerns of private property owners, at least in some circumstances. But they also illustrate the deep desire among device makers to retain control over consumer devices after they have been sold. As we explore in more detail in chapter 8, there are tools aside from the DMCA that they can use to make that vision a reality.