Microsoft Research DRM talk

by

Cory Doctorow (cory@eff.org)

June 17, 2004

This talk was originally given to Microsoft's Research Group and other interested parties from within the company at their Redmond offices on June 17, 2004. (See public domain notice.)

EFF website: EFF (Donate)
Cory Doctorow's personal site: Craphound
Cory Doctorow's group weblog: BoingBoing

Introduction

Greetings fellow pirates! Arrrrr!

I'm here today to talk to you about copyright, technology and DRM. I work for the Electronic Frontier Foundation on copyright stuff (mostly), and I live in London. I'm not a lawyer—I'm a kind of mouthpiece/activist type, though occasionally they shave me and stuff me into my Bar Mitzvah suit and send me to a standards body or the UN to stir up trouble. I spend about three weeks a month on the road doing completely weird stuff like going to Microsoft to talk about DRM.

I lead a double life: I'm also a science fiction writer. That means I've got a dog in this fight, because I've been dreaming of making my living from writing since I was 12 years old. Admittedly, my IP-based biz isn't as big as yours, but I guarantee you that it's every bit as important to me as yours is to you.

Here's what I'm here to convince you of:

1. That DRM systems don't work
2. That DRM systems are bad for society
3. That DRM systems are bad for business
4. That DRM systems are bad for artists
5. That DRM is a bad business-move for MSFT

It's a big brief, this talk. Microsoft has sunk a lot of capital into DRM systems, and spent a lot of time sending folks like Martha and Brian and Peter around to various smoke-filled rooms to make sure that Microsoft DRM finds a hospitable home in the future world. Companies like Microsoft steer like old Buicks, and this issue has a lot of forward momentum that will be hard to soak up without driving the engine block back into the driver's compartment. At best I think that Microsoft might convert some of that momentum on DRM into angular momentum, and in so doing, save all our asses.

Let's dive into it.

1. DRM systems don't work

This bit breaks down into two parts:

1. **A quick refresher course in crypto theory**
2. **Applying that to DRM**

Cryptography—secret writing—is the practice of keeping secrets. It involves three parties: a sender, a receiver and an attacker (actually, there can be more attackers, senders and recipients, but let's keep this simple). We usually call these people Alice, Bob and Carol.

Let's say we're in the days of the Caesar, the Gallic War. You need to send messages back and forth to your generals, and you'd prefer that the enemy doesn't get hold of them. You can rely on the idea that anyone who intercepts your message is probably illiterate, but that's a tough bet to stake your empire on. You can put your messages into the hands of reliable messengers who'll chew them up and swallow them if captured—but that doesn't help you if Brad Pitt and his men in skirts skewer him with an arrow before he knows what's hit him.

So you encipher your message with something like ROT-13, where every character is rotated halfway through the alphabet. They used to do this with non-worksafe material on Usenet, back when anyone on Usenet cared about work-safe-ness—A would become N, B is O, C is P, and so forth. To decipher, you just add 13 more, so N goes to A, O to B yadda yadda.

Well, this is pretty lame: as soon as anyone figures out your algorithm, your secret is gonezored.

So if you're Caesar, you spend a lot of time worrying about keeping the existence of your messengers and their payloads secret. Get that? You're Augustus and you need to send a message to Brad without Caceous (a word I'm reliably informed means "cheese-like, or pertaining to cheese") getting his hands on it. You give the message to Diatomaceous, the fleetest runner in the empire, and you encipher it with ROT-13 and send him out of the garrison in the pitchest hour of the night, making sure no one knows that you've sent it out. Caceous has spies everywhere, in the garrison and staked out on the road, and if one of them puts an arrow through Diatomaceous, they'll have their hands on the message, and then if they figure out the cipher, you're borked. So the existence of the message is a secret. The cipher is a secret. The ciphertext is a secret. That's a lot of secrets, and the more secrets you've got, the less secure you are, especially if any of those secrets are shared. Shared secrets aren't really all that secret any longer.

Time passes, stuff happens, and then Tesla invents the radio and Marconi takes credit for it. This is both good news and bad news for crypto: on the one hand, your messages can get to anywhere with a receiver and an antenna, which is great for the brave fifth columnists working behind the enemy lines. On the other hand, anyone with an antenna can listen in on the message, which means that it's no longer practical to keep the existence of the message a secret. Any time Adolf sends a message to Berlin, he can assume Churchill overhears it.

Which is OK, because now we have computers — big, bulky primitive mechanical computers, but computers still. Computers are machines for rearranging numbers, and so scientists on both sides engage in a fiendish competition to invent the most cleverest method they can for rearranging numerically represented text so that the other side can't unscramble it. The existence of the message isn't a secret anymore, but the cipher is.

But this is still too many secrets. If Bobby intercepts one of Adolf's Enigma machines, he can give Churchill all kinds of intelligence. I mean, this was good news for Churchill and us, but bad news for Adolf. And at the end of the day, it's bad news for anyone who wants to keep a secret.

Enter keys: a cipher that uses a key is still more secure. Even if the cipher is disclosed, even if the ciphertext is intercepted, without the key (or a break), the message is secret. Post-war, this is doubly important as we begin to realize what I think of as Schneier's Law: "any person can invent a security system so clever that she or he can't think of how to break it." This means that the only experimental methodology for discovering if you've made mistakes in your cipher is to tell all the smart people you can about it and ask them to think of ways to break it. Without this critical step, you'll eventually end up living in a fool's paradise, where your attacker has broken your cipher ages ago and is quietly decrypting all her intercepts of your messages, snickering at you.

Best of all, there's only one secret: the key. And with dual-key crypto it becomes a lot easier for Alice and Bob to keep their keys secret from Carol, even if they've never met. So long as Alice and Bob can keep their keys secret, they can assume that Carol won't gain access to their cleartext messages, even though she has access to the cipher and the ciphertext. Conveniently enough, the keys are the shortest and simplest of the secrets, too: hence even easier to keep away from Carol. Hooray for Bob and Alice.

Now, let's apply this to DRM.

In DRM, the attacker is ***also the recipient***. It's not Alice and Bob and Carol, it's just Alice and Bob. Alice sells Bob a DVD. She sells Bob a DVD player. The DVD has a movie on it—say, *Pirates of the Caribbean*—and it's enciphered with an algorithm called CSS — Content Scrambling System. The DVD player has a CSS un-scrambler.

Now, let's take stock of what's a secret here: the cipher is well-known. The ciphertext is most assuredly in enemy hands, arrr. So what? As long as the key is secret from the attacker, we're golden.

But there's the rub. Alice wants Bob to buy *Pirates of the Caribbean* from her. Bob will only buy *Pirates of the Caribbean* if he can descramble the CSS-encrypted VOB—video object—on his DVD player. Otherwise, the disc is only useful to Bob as a drinks-coaster. So Alice has to provide Bob—the attacker—with the key, the cipher and the ciphertext.

Hilarity ensues.

DRM systems are broken in minutes, sometimes days. Rarely, months. It's not because the people who think them up are stupid. It's not because the people who break them are smart. It's not because there's a flaw in the algorithms. At the end of the day, all DRM systems share a common vulnerability: they provide their attackers with ciphertext, the cipher and the key. At this point, the secret isn't a secret anymore.

2. DRM systems are bad for society

Raise your hand if you're thinking something like, "But DRM doesn't have to be proof against smart attackers, only average individuals! It's like a speedbump!"

Put your hand down.

This is a fallacy for two reasons: one technical, and one social. They're both bad for society, though.

Here's the technical reason: I don't need to be a cracker to break your DRM. I only need to know how to search Google, or Kazaa, or any of the other general-purpose search tools for the cleartext that someone smarter than me has extracted.

Raise your hand if you're thinking something like, "But NGSCB can solve this problem: we'll lock the secrets up on the logic board and goop it all up with epoxy."

Put your hand down.

Raise your hand if you're a co-author of the Darknet paper.

Everyone in the first group, meet the co-authors of the Darknet paper. This is a paper that says, among other things, that DRM will fail for this very reason. Put your hands down, guys.

Here's the social reason that DRM fails: keeping an honest user honest is like keeping a tall user tall. DRM vendors tell us that their technology is meant to be proof against average users, not organized criminal gangs like the Ukranian pirates who stamp out millions of high-quality counterfeits. It's not meant to be proof against sophisticated college kids. It's not meant to be proof against anyone who knows how to edit her registry, or hold down the shift key at the right moment, or use a search engine. At the end of the day, the user DRM is meant to defend against is the most unsophisticated and least capable among us.

Here's a true story about a user I know who was stopped by DRM. She's smart, college educated, and knows nothing about electronics. She has three kids. She has a DVD in the living room and an old VHS deck in the kids' playroom. One day, she brought home the *Toy Story* DVD for the kids. That's a substantial investment, and given the generally jam-smeared character of everything the kids get their paws on, she decided to tape the DVD off to VHS and give that to the kids—that way she could make a fresh VHS copy when the first one went south. She cabled her DVD into her VHS and pressed play on the DVD and record on the VCR and waited.

Before I go farther, I want us all to stop a moment and marvel at this. Here is someone who is practically technophobic, but who was able to construct a mental model of sufficient accuracy that she figured out that she could connect her cables in the right order and dub her digital disc off to analog tape. I imagine that everyone in this room is the front-line tech support for someone in her or his family: would it be great if all our non-geek friends and relatives were this clever and imaginative?

I also want to point out that this is the proverbial honest user. She's not making a copy for the next door neighbors. She's not making a copy and selling it on a blanket on Canal Street. She's not ripping it to her hard-drive, DivX encoding it and putting it in her Kazaa sharepoint. She's doing something **honest** — moving it from one format to another. She's home taping.

Except she fails. There's a DRM system called Macrovision embedded – by law – in every DVD player and VHS that messes with the vertical blanking interval in the signal and causes any tape made in this fashion to fail. Macrovision can be defeated for about $10 with a gadget readily available on eBay. But our infringer doesn't know that. She's "honest." Technically unsophisticated. Not stupid, mind you – just naive.

The Darknet paper addresses this possibility: it even predicts what this person will do in the long run: she'll find out about Kazaa and the next time she wants to get a movie for the kids, she'll download it from the net and burn it for them.

In order to delay that day for as long as possible, our lawmakers and big rights-holder interests have come up with a disastrous policy called anticircumvention.

Here's how anticircumvention works: if you put a lock – an access control – around a copyrighted work, it is illegal to break that lock. It's illegal to make a tool that breaks that lock. It's illegal to tell someone how to make that tool. It's illegal to tell someone where she can find out how to make that tool.

Remember Schneier's Law? Anyone can come up with a security system so clever that he can't see its flaws. The only way to find the flaws in security is to disclose the system's workings and invite public feedback. But now we live in a world where any cipher used to fence off a copyrighted work is off-limits to that kind of feedback. That's something that a Princeton engineering prof named Ed Felten discovered

when he submitted a paper to an academic conference on the failings in the Secure Digital Music Initiative, a watermarking scheme proposed by the recording industry. The RIAA responded by threatening to sue his ass if he tried it. We fought them because Ed is the kind of client that impact litigators love: unimpeachable and clean-cut and the RIAA folded. Lucky Ed. Maybe the next guy isn't so lucky.

Matter of fact, the next guy wasn't. Dmitry Skylarov is a Russian programmer who gave a talk at a hacker con in Vegas on the failings in Adobe's e-book locks. The FBI threw him in the slam for 30 days. He copped a plea, went home to Russia, and the Russian equivalent of the State Department issued a blanket warning to its researchers to stay away from American conferences, since we'd apparently turned into the kind of country where certain equations are illegal.

Anticircumvention is a powerful tool for people who want to exclude competitors. If you claim that your car engine firmware is a "copyrighted work," you can sue anyone who makes a tool for interfacing with it. That's not just bad news for mechanics—think of the hotrodders who want to chip their cars to tweak the performance settings. We have companies like Lexmark claiming that their printer cartridges contain copyrighted works—software that trips an "I am empty" flag when the toner runs out, and have sued a competitor who made a remanufactured cartridge that reset the flag. Even garage-door opener companies have gotten in on the act, claiming that their receivers' firmware are copyrighted works. Copyrighted cars, print carts and garage-door openers: what's next, copyrighted light-fixtures?

Even in the context of legitimate—excuse me, "traditional"—copyrighted works like movies on DVDs, anticircumvention is bad news. Copyright is a delicate balance. It gives creators and their assignees some rights, but it also reserves some rights to the public. For example, an author has no right to prohibit anyone from transcoding his books into assistive formats for the blind. More importantly, though, a creator has a very limited say over what you can do once you lawfully acquire her works. If I buy your book, your painting, or your DVD, it belongs to me. It's my property. Not my "intellectual property"—a whacky kind of pseudo-property that's swiss-cheesed with exceptions, easements and limitations—but real, no-fooling, actual tangible ***property***—the kind of thing that courts have been managing through tort law for centuries.

But anticirumvention lets rightsholders invent new and exciting copyrights for themselves—to write private laws without accountability or deliberation—that expropriate your interest in your physical property to their favor. Region-coded DVDs are an example of this: there's no copyright here or in anywhere I know of that says that an author should be able to control where you enjoy her creative works, once you've paid for them. I can buy a book and throw it in my bag and take it anywhere from Toronto to Timbuktu, and read it wherever I am: I can even buy books in America and bring them to the UK, where the author may have an exclusive distribution deal with a local publisher who sells them for double the US shelf-price. When I'm done with it, I can sell it on or give it away in the UK. Copyright lawyers call this "First Sale," but it may be simpler to think of it as "Capitalism."

The keys to decrypt a DVD are controlled by an org called DVD-CCA, and they have a bunch of licensing requirements for anyone who gets a key from them. Among these is something called region-coding: if you buy a DVD in France, it'll have a flag set that says, "I am a French DVD." Bring that DVD to America and your DVD player will compare the flag to its list of permitted regions, and if they don't match, it will tell you that it's not allowed to play your disc.

Remember: there is no copyright that says that an author gets to do this. When we wrote the copyright statutes and granted authors the right to control display, performance, duplication, derivative works, and so forth, we didn't leave out "geography" by accident. That was on-purpose.

So when your French DVD won't play in America, that's not because it'd be illegal to do so: it's because the studios have invented a business-model and then invented a copyright law to prop it up. The DVD is your property and so is the DVD player, but if you break the region-coding on your disc, you're going to run afoul of anticircumvention.

That's what happened to Jon Johansen, a Norwegian teenager who wanted to watch French DVDs on his Norwegian DVD player. He and some pals wrote some code to break the CSS so that he could do so. He's a wanted man here in America; in Norway the studios put the local fuzz up to bringing him up on charges of ***unlawfully trespassing upon a computer system***. When his defense asked, "Which computer has Jon trespassed upon?" the answer was: "His own."

His no-fooling, real and physical property has been expropriated by the weird, notional, metaphorical intellectual property on his DVD: DRM only works if your record player becomes the property of whomever's records you're playing.

3. DRM systems are bad for biz

This is the worst of all the ideas embodied by DRM: that people who make record-players should be able to spec whose records you can listen to, and that people who make records should have a veto over the design of record-players.

We've never had this principle: in fact, we've always had just the reverse. Think about all the things that can be plugged into a parallel or serial interface, which were never envisioned by their inventors. Our strong economy and rapid innovation are byproducts of the ability of anyone to make anything that plugs into anything else: from the Flo-bee electric razor that snaps onto the end of your vacuum-hose to the octopus spilling out of your car's dashboard lighter socket, standard interfaces that anyone can build for are what makes billionaires out of nerds.

The courts affirm this again and again. It used to be illegal to plug anything that didn't come from AT&T into your phone-jack. They claimed that this was for the safety of the network, but really it was about propping up this little penny-ante racket that AT&T had in charging you a rental fee for your phone until you'd paid for it a thousand times over.

When that ban was struck down, it created the market for third-party phone equipment, from talking novelty phones to answering machines to cordless handsets to headsets — billions of dollars of economic activity that had been suppressed by the closed interface. Note that AT&T was one of the big beneficiaries of this: they *also* got into the business of making phone-kitsch.

DRM is the software equivalent of these closed hardware interfaces. Robert Scoble is a Softie who has an excellent blog, where he wrote an essay about the best way to protect your investment in the digital music you buy. Should you buy Apple iTunes music, or Microsoft DRM music? Scoble argued that Microsoft's music was a sounder investment, because Microsoft would have more downstream licensees for its proprietary format and therefore you'd have a richer ecosystem of devices to choose from when you were shopping for gizmos to play your virtual records on.

What a weird idea: that we should evaluate our record-purchases on the basis of which recording company will allow the greatest diversity of record-players to play its discs! That's like telling someone to buy the Betamax instead of the Edison Kinetoscope because Thomas Edison is a crank about licensing his patents; all the while ignoring the world's relentless march to the more open VHS format.

It's a bad business. DVD is a format where the guy who makes the records gets to design the record players. Ask yourself: how much innovation has there been over the past decade of DVD players? They've gotten cheaper and smaller, but where are the weird and amazing new markets for DVD that were opened up by the VCR? There's a company that's manufacturing the world's first HDD-based DVD jukebox, a thing that holds 30 movies, and they're charging *$30,000* for this thing. We're talking about a $300 hard drive and a $300 PC—all that other cost is the cost of anticompetition.

4. DRM systems are bad for artists

But what of the artist? The hardworking filmmaker, the ink-stained scribbler, the heroin-cured leathery rock-star? We poor slobs of the creative class are everyone's favorite poster-children here: the RIAA and MPAA hold us up and say, "Won't someone please think of the children?" File-sharers say, "Yeah, we're thinking about the artists, but the labels are The Man, who cares what happens to you?"

To understand what DRM does to artists, you need to understand how copyright and technology interact. Copyright is inherently technological, since the things it addresses—copying, transmitting, and so on—are inherently technological.

The piano roll was the first system for cheaply copying music. It was invented at a time when the dominant form of entertainment in America was getting a talented pianist to come into your living room and pound out some tunes while you sang along. The music industry consisted mostly of sheet-music publishers.

The player piano was a digital recording and playback system. Piano-roll companies bought sheet music and ripped the notes printed on it into 0s and 1s on a long roll of computer tape, which they sold by the thousands—the hundreds of thousands—the millions. They did this without a penny's compensation to the publishers. They were digital music pirates. Arrrr!

Predictably, the composers and music publishers went nutso. Sousa showed up in Congress to say that:

> These talking machines are going to ruin the artistic development of music in this country. When I was a boy ... in front of every house in the summer evenings, you would find young people together singing the songs of the day or old songs. Today you hear these infernal machines going night and day. We will not have a vocal chord left. The vocal chord will be eliminated by a process of evolution, as was the tail of man when he came from the ape.

The publishers asked Congress to ban the piano roll and to create a law that said that any new system for reproducing music should be subject to a veto from their industry association. Lucky for us, Congress realized what side of their bread had butter on it and decided not to criminalize the dominant form of entertainment in America.

But there was the problem of paying artists. The Constitution sets out the purpose of American copyright: to promote the useful arts and sciences. The composers had a credible story that they'd do less composing if they weren't paid for it, so Congress needed a fix. Here's what they came up with: anyone who paid a music publisher two cents would have the right to make one piano roll of any song that publisher published. The publisher couldn't say no, and no one had to hire a lawyer at $200 an hour to argue about whether the payment should be two cents or a nickel.

This compulsory license is still in place today: when Joe Cocker sings "With a Little Help from My Friends," he pays a fixed fee to the Beatles' publisher and away he goes—even if Ringo hates the idea. If you ever wondered how Sid Vicious talked Anka into letting him get a crack at "My Way," well, now you know.

That compulsory license created a world where a thousand times more money was made by a thousand times more creators who made a thousand times more music that reached a thousand times more people.

This story repeats itself throughout the technological century, every ten or fifteen years. Radio was enabled by a voluntary blanket license—the music companies got together and asked for an antitrust exemption so that they could offer all their music for a flat fee. Cable TV took a compulsory: the only way cable operators could get their hands on broadcasts was to pirate them and shove them down the wire, and Congress saw fit to legalize this practice rather than screw around with their constituents' TVs.

Sometimes, the courts and Congress decided to simply take away a copyright — that's what happened with the VCR. When Sony brought out the VCR in 1976, the studios had already decided what the experience of watching a movie in your living room would look like: they'd licensed out their programming for use on a machine called a Discovision, which played big LP-sized discs that disintegrated after a few plays. Proto-DRM.

The copyright scholars of the day didn't give the VCR very good odds. Sony argued that their box allowed for a fair use, which is defined as a use that a court rules is a defense against infringement based on four factors: whether the use transforms the work into something new, like a collage; whether it uses all or some of the work; whether the work is artistic or mainly factual; and whether the use undercuts the creator's business-model.

The Betamax failed on all four fronts: when you time-shifted or duplicated a Hollywood movie off the air, you made a non-transformative use of 100 percent of a creative work in a way that directly undercut the Discovision licensing stream.

Jack Valenti, the mouthpiece for the motion-picture industry, told Congress in 1982 that the VCR was to the American film industry "as the Boston Strangler is to a woman home alone."

But the Supreme Court ruled against Hollywood in 1984, when it determined that any device capable of a substantial non-infringing use was legal. In other words, "We don't buy this Boston Strangler business: if your business model can't survive the emergence of this general-purpose tool, it's time to get another business-model or go broke."

Hollywood found another business model, as the broadcasters had, as the Vaudeville artists had, as the music publishers had, and they made more art that paid more artists and reached a wider audience.

There's one thing that every new art business-model had in common: it embraced the medium it lived in.

This is the overweening characteristic of every single successful new medium: it is true to itself. The Luther Bible didn't succeed on the axes that made a hand-copied monk Bible valuable: they were ugly, they weren't in Church Latin, they weren't read aloud by someone who could interpret it for his lay audience, they didn't represent years of devoted-with-a-capital-D labor by someone who had given his life over to God. The thing that made the Luther Bible a success was its scalability: it was more popular because it was more proliferate: all success factors for a new medium pale beside its profligacy. The most successful organisms on earth are those that reproduce the most: bugs and bacteria, nematodes and virii. Reproduction is the best of all survival strategies.

Piano rolls didn't sound as good as the music of a skilled pianist: but they ***scaled better***. Radio lacked the social elements of live performance, but more people could build a crystal set and get it aimed correctly than could pack into even the largest Vaudeville house. MP3s don't come with liner notes, they aren't sold to you by a hipper-than-thou record store clerk who can help you make your choice, bad rips and truncated files abound: I once downloaded a twelve-second copy of "Hey Jude" from the original Napster. Yet MP3 is outcompeting the CD. I don't know what to do with CDs anymore: I get them, and they're like the especially nice garment bag they give you at the fancy suit shop: it's nice and you feel like a goof for throwing it out, but Christ, how many of these things can you usefully own? I can put ten thousand songs on my laptop, but a comparable pile of discs, with liner notes and so forth—that's a liability: it's a piece of my monthly storage-locker costs.

Here are the two most important things to know about computers and the Internet:

1. A computer is a machine for rearranging bits
2. The Internet is a machine for moving bits from one place to another very cheaply and quickly

Any new medium that takes hold on the Internet and with computers will embrace these two facts, not regret them. A newspaper press is a machine for spitting out cheap and smeary newsprint at speed: if you try to make it output fine art lithos, you'll get junk. If you try to make it output newspapers, you'll get the basis for a free society.

And so it is with the Internet. At the heyday of Napster, record execs used to show up at conferences and tell everyone that Napster was doomed because no one wanted lossily compressed MP3s with no liner notes and truncated files and misspelled metadata.

Today we hear ebook publishers tell each other and anyone who'll listen that the barrier to ebooks is screen resolution. It's bollocks, and so is the whole sermonette about how nice a book looks on your bookcase and how nice it smells and how easy it is to slip into the tub. These are obvious and untrue things, like the idea that radio will catch on once they figure out how to sell you hotdogs during the intermission, or that movies will really hit their stride when we can figure out how to bring the actors out for an encore when the film's run out. Or that what the Protestant Reformation really needs is Luther Bibles with facsimile illumination in the margin and a rent-a-priest to read aloud from your personal Word of God.

New media don't succeed because they're like the old media, only better: they succeed because they're worse than the old media at the stuff the old media is good at, and better at the stuff the old media are bad at. Books are good at being paperwhite, high-resolution, low-infrastructure, cheap and disposable. Ebooks are good at being everywhere in the world at the same time for free in a form that is so malleable that you can just pastebomb it into your IM session or turn it into a page-a-day mailing list.

The only really successful epublishing—I mean, hundreds of thousands, millions of copies distributed and read—is the bookwarez scene, where scanned-and-OCR'd books are distributed on the darknet. The only legit publishers with any success at epublishing are the ones whose books cross the Internet without technological fetter: publishers like Baen Books and my own, Tor, who are making some or all of their catalogs available in ASCII and HTML and PDF.

The hardware-dependent ebooks, the DRM use-and-copy-restricted ebooks, they're cratering. Sales measured in the tens, sometimes the hundreds. Science fiction is a niche business, but when you're selling copies by the tens, that's not even a business, it's a hobby.

Every one of you has been riding a curve where you read more and more words off of more and more screens every day through most of your professional careers. It's zero-sum: you've also been reading fewer words off of fewer pages as time went by: the dinosauric executive who prints his email and dictates a reply to his secretary is info-roadkill.

Today, at this very second, people read words off of screens for every hour that they can find. Your kids stare at their Game Boys until their eyes fall out. Euroteens ring doorbells with their hypertrophied, SMS-twitching thumbs instead of their index fingers.

Paper books are the packaging that books come in. Cheap printer-binderies like the Internet Bookmobile that can produce a full bleed, four color, glossy cover, printed spine, perfect-bound book in ten minutes for a dollar are the future of paper books: when you need an instance of a paper book, you generate one, or part of one, and pitch it out when you're done. I landed at SEA-TAC on Monday and burned a couple CDs from my music collection to listen to in the rental car. When I drop the car off, I'll leave them behind. Who needs 'em?

Whenever a new technology has disrupted copyright, we've changed copyright. Copyright isn't an ethical proposition, it's a utilitarian one. There's nothing ***moral*** about paying a composer tuppence for the piano-roll rights, there's nothing ***immoral*** about not paying Hollywood for the right to videotape a movie off your TV. They're just the best way of balancing out so that people's physical property rights in their VCRs and

phonographs are respected and so that creators get enough of a dangling carrot to go on making shows and music and books and paintings.

Technology that disrupts copyright does so because it simplifies and cheapens creation, reproduction and distribution. The existing copyright businesses exploit inefficiencies in the old production, reproduction and distribution system, and they'll be weakened by the new technology. But new technology always gives us more art with a wider reach: that's what tech is ***for***.

Tech gives us bigger pies that more artists can get a bite out of. That's been tacitly acknowledged at every stage of the copyfight since the piano roll. When copyright and technology collide, it's copyright that changes.

Which means that today's copyright—the thing that DRM nominally props up—didn't come down off the mountain on two stone tablets. It was created in living memory to accommodate the technical reality created by the inventors of the previous generation. To abandon invention now robs tomorrow's artists of the new businesses and new reach and new audiences that the Internet and the PC can give them.

5. DRM is a bad business-move for MSFT

When Sony brought out the VCR, it made a record player that could play Hollywood's records, even if Hollywood didn't like the idea. The industries that grew up on the back of the VCR—movie rentals, home taping, camcorders, even Bar Mitzvah videographers—made billions for Sony and its cohort.

That was good business—even if Sony lost the Betamax-VHS format wars, the money on the world-with-VCRs table was enough to make up for it.

But then Sony acquired a relatively tiny entertainment company and it started to massively screw up. When MP3 rolled around and Sony's walkman customers were clamoring for a solid-state MP3 player, Sony let its music business-unit run its show: instead of making a high-capacity MP3 walkman, Sony shipped its Music Clips, low-capacity devices that played brain-damaged DRM formats like Real and OpenAG. They spent good money engineering "features" into these devices that kept their customers from freely moving their music back and forth between their devices. Customers stayed away in droves.

Today, Sony is dead in the water when it comes to walkmen. The market leaders are poky Singaporean outfits like Creative Labs—the kind of company that Sony used to crush like a bug, back before it got borged by its entertainment unit—and PC companies like Apple.

That's because Sony shipped a product that there was no market demand for. No Sony customer woke up one morning and said, "Damn, I wish Sony would devote some expensive engineering effort in order that I may do less with my music." Presented with an alternative, Sony's customers enthusiastically jumped ship.

The same thing happened to a lot of people I know who used to rip their CDs to WMA. You guys sold them software that produced smaller, better-sounding rips that the MP3 rippers, but you also fixed it so that the songs you ripped were device-locked to their PCs. What that meant is that when they backed up their music to another hard-drive and reinstalled their OS (something that the spyware and malware wars has made more common than ever), they discovered that after they restored their music that they could no longer play it. The player saw the new OS as a different machine, and locked them out of their own music.

There is no market demand for this "feature." None of your customers want you to make expensive modifications to your products that make backing up and restoring even harder. And there is no moment when your customers will be less forgiving than the moment that they are recovering from catastrophic technology failures.

I speak from experience. Because I buy a new Powerbook every ten months, and because I always order the new models the day they're announced, I get a lot of lemons from Apple. That means that I hit Apple's three-iTunes-authorized-computers limit pretty early on and found myself unable to play the hundreds of dollars' worth of iTunes songs I'd bought because one of my authorized machines was a lemon that Apple had broken up for parts, one was in the shop getting fixed by Apple, and one was my mom's computer, 3,000 miles away in Toronto.

If I had been a less good customer for Apple's hardware, I would have been fine. If I had been a less enthusiastic evangelist for Apple's products—if I hadn't shown my mom how iTunes Music Store worked—I would have been fine. If I hadn't bought so much iTunes music that burning it to CD and re-ripping it and re-keying all my metadata was too daunting a task to consider, I would have been fine.

As it was Apple rewarded my trust, evangelism and out-of-control spending by treating me like a crook and locking me out of my own music, at a time when my Powerbook was in the shop—i.e., at a time when I was hardly disposed to feel charitable to Apple.

I'm an edge case here, but I'm a *leading edge* case. If Apple succeeds in its business plans, it will only be a matter of time until even average customers have upgraded enough hardware and bought enough music to end up where I am.

You know what I would totally buy? A record player that let me play everybody's records. Right now, the closest I can come to that is an open source app called VLC, but it's clunky and buggy and it didn't come pre-installed on my computer.

Sony didn't make a Betamax that only played the movies that Hollywood was willing to permit—Hollywood asked them to do it, they proposed an early, analog broadcast flag that VCRs could hunt for and respond to by disabling recording. Sony ignored them and made the product they thought their customers wanted.

I'm a Microsoft customer. Like millions of other Microsoft customers, I want a player that plays anything I throw at it, and I think that you are just the company to give it to me.

Yes, this would violate copyright law as it stands, but Microsoft has been making tools of piracy that change copyright law for decades now. Outlook, Exchange and MSN are tools that abet widescale digital infringement.

More significantly, IIS and your caching proxies all make and serve copies of documents without their authors' consent, something that, if it is legal today, is only legal because companies like Microsoft went ahead and did it and dared lawmakers to prosecute.

Microsoft stood up for its customers and for progress, and won so decisively that most people never even realized that there was a fight.

Do it again! This is a company that looks the world's roughest, toughest anti-trust regulators in the eye and laughs. Compared to anti-trust people, copyright lawmakers are pantywaists. You can take them with your arms behind your back.

In Siva Vaidhyanathan's book *The Anarchist in the Library*, he talks about why the studios are so blind to their customers' desires. It's because people like you and me spent the 80s and the 90s telling them bad science fiction stories about impossible DRM technology that would let them charge a small sum of money every time someone looked at a movie — want to fast-forward? That feature costs another penny. Pausing is two cents an hour. The mute button will cost you a quarter.

When Mako Analysis issued their report last month advising phone companies to stop supporting Symbian phones, they were just writing the latest installment in this story. Mako says that phones like my P900, which can play MP3s as ringtones, are bad for the cellphone economy, because it'll put the extortionate ringtone sellers out of business. What Mako is saying is that just because you bought the CD doesn't mean that you should expect to have the ability to listen to it on your MP3 player, and just because it plays on your MP3 player is no reason to expect it to run as a ringtone. I wonder how they feel about alarm clocks that will play a CD to wake you up in the morning? Is that strangling the nascent "alarm tone" market?

The phone companies' customers want Symbian phones and for now, at least, the phone companies understand that if they don't sell them, someone else will.

The market opportunity for a truly capable devices is enormous. There's a company out there charging *$30,000* for a $600 DVD jukebox — go and eat their lunch! Steve Jobs isn't going to do it: he's off at the D conference telling studio execs not to release hi-def movies until they're sure no one will make a hi-def DVD burner that works with a PC.

Maybe they won't buy into his BS, but they're also not much interested in what you have to sell. At the Broadcast Protection Discussion Group meetings where the Broadcast Flag was hammered out, the studios' position was, "We'll take anyone's DRM except Microsoft's and Philips'." When I met with UK broadcast wonks about the European version of the Broadcast Flag underway at the Digital Video Broadcasters' forum, they told me, "Well, it's different in Europe: mostly they're worried that some American company like Microsoft will get their claws into European television."

American film studios didn't want the Japanese electronics companies to get a piece of the movie pie, so they fought the VCR. Today, everyone who makes movies agrees that they don't want to let you guys get between them and their customers.

Sony didn't get permission. Neither should you. Go build the record player that can play everyone's records.

Because if you don't do it, someone else will.

The talk was all about DRM (Digital Rights Management). Full text here. It's a great readâ€¦Â Ya know, Microsoft Research is like the uber cool kids at Microsoft that are always doing things but all the people we know at Microsoft rarely have any idea what they're up to. Maybe they'd do a blog, getting someone like Cory in front of a lot of MS peeps sounds like a good idea to us. All products recommended by Engadget are selected by our editorial team, independent of our parent company. Some of our stories include affiliate links. Digital rights management (DRM) tools or technological protection measures (TPM) are a set of access control technologies for restricting the use of proprietary hardware and copyrighted works. DRM technologies try to control the use, modification, and distribution of copyrighted works (such as software and multimedia content), as well as systems within devices that enforce these policies. The talk was not delivered verbatim, nevertheless, this is a good feel for what I said that day. For the text of an earlier talk on this subject delivered to Microsoft Research, see http://craphound.com/msftdrm.txt. The canonical version of this talk live at http://craphound.com/hpdrm.txt.Â The threat model for DRM is that an unscrupulous user will be able to download an asset for free from the Internet instead of going through a conditional access billing gateway. Additionally, DRM seeks to give rightsholders the ability to restrict the use of assets after receipt to enforce restrictions that are not related to copyright (e.g. remote viewing, region-control). Multi-DRM technology allows content to be protected by platform-native DRM without browser plugins. Many online content services use multi-DRM for better usability of browser users. But there are still some problems that the multi-DRM technology couldnâ€™t solve yet. The screen recording issue of Chrome and FireFox browser. Chrome and Firefox are the most popular browsers that occupy 75% of the desktop and laptop browser share. (As of May 2019, Chrome has 66% and Firefox has 9.6% of the market. â€” ref. #4). However, Widevine DRM embedded in these browsers has software level security (Widevine Lev Digital rights management (DRM) tools or technological protection measures (TPM)[1] are a set of access control technologies for restricting the use of proprietary hardware and copyrighted works.[2] DRM technologies try to control the use, modification, and distribution of copyrighted works (such as software and multimedia content), as well as systems within devices that enforce these policies.[3].Â What is digital rights management (DRM)? Enabling DRM for Kindle Publishing. Digital rights management - #kominfopedia.