Without an Open Internet and without holding media companies accountable (which should include requiring enhanced online disclosure of broadcaster's political files) stories like these (see below this paragraph) being published online could be censored by an ISP by limiting or discouraging user's access to such articles by blocking or slowing down the connection speeds of user's accessing websites with such stories. Using the Open Internet everyday regular Americans can comment on proposed transactions being reviewed by the FCC, complain to the FCC about companies they have authority over for misconduct to the consumer, or contact other government agencies like the U.S. Copyright Office to discuss why DMCA exemptions should be afforded to DVDs, Blu Ray Discs, video game consoles, smart-phones and tablets with DRM. They can use the Open Internet to communicate with their members of Congress etc. The Open Internet enabled users to comment on the AT&T T-Mobile merger, for environmentalists to report why Keystone XL Pipeline is bad for the environment and how whether the pipeline is built or not the tar sand oil would still go to China. Political activism by everyday Americans would suffer and minority, independent voices as well who could not afford to pay the special tolls ISPs want paid to them to make websites load faster.

Here's that article:

DRM gives companies security -- from competition

Cory Doctorow at 9:10AM Friday February 17th

Last night, Rob posted a very good piece on Apple's new "Gatekeeper" technology, which defaults to warning users of Apple's new Mountain Lion OS that software from companies that haven't been officially recognized by Apple should not be installed (though users can still choose to override it, or turn it off).

But I have one rather large quibble with Rob's piece. He wrote:
The truth is that Macs don't currently suffer much from malicious software, and DRM-esque lockouts are always circumvented. So what's the point of a DRM-esque system for malware prevention?

I agree that DRM is always circumvented, and it is especially circumvented by copyright infringers and malware creators. But I think that Rob has misunderstood the primary value of DRM to technology companies: because many countries' laws prohibit breaking DRM even if you're not doing anything illegal, DRM gives

companies the right to sue competitors who make compatible products and services.

The law has always recognized that interoperability is good for competition, markets, and the public. From generic windshield wiper blades and hubcaps to third-party hard-drives and keyboards and inkjet toner, and software like Pages and Keynote, the law recognizes that there is a legitimate reason to reverse engineer a competitor's products and make new products that replace, expand and augment them.

Companies don't like this. It interferes with the "razor blade" business model of subsidizing one part of a product and charging high margins on some other part. It undermines efforts to corner markets and freeze out disruptive innovation. It lowers prices and forces you to spend more money on R&D to get the next product out because the profits have started to fall on the old products.

But these are not bugs, they're features. High prices on inkjet cartridges and proprietary cables and other consumables and accessories hold us back from realizing the full utility of our property. Allowing carriers to lock handsets to prevent the introduction of VoIP and tethering software to preserve high tariffs is good for telco investors, but bad for those of us who buy their products, and it removes the incentive to improve voice-call quality to compete with VoIP. Artificially prolonging the profitability of last year's invention means that this year's invention doesn't get made as quickly -- or at all.

Locking devices to only accept software that has been blessed by the vendor has been a profitable anticompetitive strategy. It's allowed the iOS App Store to command high commissions on sales, and to expand those commissions to cover transactions after the initial sale (if you spend money within an iOS App, Apple takes 30% of that transaction as well -- like a cash-register manufacturer demanding a slice of each transaction after you've bought the register). It allows the company to freeze out apps it doesn't like, even if customers want them. It undermines copyright by making it illegal for someone to create and sell their copyrighted software to willing buyers without the approval

of the company that made the hardware the software will run on -- because the unblessed software won't run without breaking the DRM, and breaking DRM is illegal.

Legitimate, lawful transactions are different from copyright infringement or disseminating malicious software. Malware writers aren't worried that they'll get sued for breaking DRM -- they're already breaking the law. Copyright infringers don't need to raise capital to produce software, and they don't need to have easy-to-track merchant accounts for their services, because they offer those services for free, by and large.

So while Rob is right to note that DRM-esque mechanisms have no effect on piracy and malware, they do effectively prevent legitimate businesses from raising capital, making products, advertising products and selling products. No one will invest in a company that will get shut down by the courts for breaking DRM. You can't maintain a low, anonymous profile and also advertise your products and take money for them.

I don't know whether Apple will expand its iOS platform-locks to the Mac OS. But if they do, it won't be because they don't see any benefit from DRM-like measures. They assuredly do. That's why they asked the Copyright Office not to grant a jail breaking exemption for iPhones three years ago, and it's why they're objecting to renewing and expanding that exemption to cover iPads now.

And these exemptions are far more narrow than the freedom that the law, absent rules protecting DRM, would give to competitors.
When the Copyright Office grants a three-year jail breaking exemption, it doesn't make it legal to make, describe, sell or give away tools to jailbreak. Effectively, they only make it legal to figure out how to jailbreak your *own* phone or tablet, but not to tell anyone else how to do it, and certainly not to create a jail breaking service. This is very different from, for example, making a commercial offering like Apple's Keynote (which reverse-engineers and provides interoperability with Microsoft's PowerPoint), producing an advertising campaign for it, and selling it in boxes at the Apple Store.

Instead, this impoverished permission to interoperate dooms the public to shop in still-illegal black markets for jail breaking tools, with no recourse if the software breaks their phone or installs spyware on it. Even when the Copyright Office creates exemptions to the protections for DRM, they still leave an anticompetitive landscape intact.