Commenter name: John William Harris
Classes of works: Game consoles, Personal computing device jailbreaks, Smartphones and tablets
Class numbers: 3, 4, 5

This argument applies to each of the above classes of works, but is particularly focused on smartphones and tablets, particularly those devices made by Apple that I call *iOS machines*.

At heart here, I feel, is a bit of terminology confusion. People talk about "computer security" as an unqualified good, but it depends on who is the computer protecting against. Against hackers from some random IP address on the internet? Fine. Against the person who actually owns the device? Terrible.

Any security measure on a device designed to restrict what someone who bought and paid for that device may do with it is bad in a fundamental sense, and should be exempt from anti-circumvention measures as a matter of course. Even if you make allowances for the prevention of privacy, the fact is that game console and mobile computing manufacturers use their control over their platforms for purposes far beyond prevention of privacy, specifically so they can sell extra entirely-software features at a later date. Sometimes these features are already present, in code form, on the device, and what is actually being sold is merely a key to "unlock" that functionality. If someone else should be willing to write a module for that device that provides that function for free they should not be prevented, but that's exactly what this "security" is being used to do.

There is no better example of what I'm talking about than the vibrant Windows and Linux software communities. Both provide many examples of software able to perform almost any feature a user could want, and often for free. Even on Windows, which is a far from open platform, one can find many useful utilities that people have chosen to make available for nothing, or merely in order to charge for support.

Contrast this with Apple's App Store, on which nearly everything one could hope to obtain costs either a nominal 99 cents (somes much more), or is loaded with obtrusive ads. This is because Apple charges developers $100 *a year* to provide development access to their device, and because of their role as gatekeeper over the platform, most people who write software for iOS machines have to pass along these charges in order to recoup those losses. If Apple loosened this restriction then people could either load their own software, or other's freely-distributed software, onto their devices for free (an act which needn't allow for piracy considering how iOS will refuse to run unsigned applications anyway). But that would harm Apple's stranglehold over iOS software, which is designed to allow them 1. to effectively charge a tax on what features users have available on their machines, and 2. to allow them to forbid access to features that consider inappropriate to the device. Features like WiFi tethering, installing scripting languages, anything that could possibly look like a development tool, and in some past cases even restricting political speech.

On game consoles the situation is even worse. This entire class of device consists of capable computing hardware to which the manufacturer demands sole and unending control. A Nintendo Wii can serve as an able media center or a passable file server, or at least it could if Nintendo allowed for it. The problem isn't just that Nintendo doesn't provide a golden path to developers for doing this, but they actively seek to prevent it. This has long been the story of console software development, since the days of the Nintendo Entertainment System's infamous "lockout chip," created entirely to attempt to limit purveyors of software for that console to Nintendo's approved list of developers. Every major game console since then has contained similar lockout measures, of escalating levels of complexity. Yet the right of Nintendo, or Sony, or Microsoft, or Apple for that matter, to decide what a user should do with a machine they have purchased is questionable, but difficult to prevent. Backing up their "security" measures with legal force, however, is doubly questionable. Their desire to maintain their profits by acting as gatekeeper over their devices, to prevent unlicensed third-party developers from having access to the systems they manufacture, that is the true purpose of these lockouts; piracy is but a smokescreen.

In short, the terrible grip that limited computing device manufacturers on their devices, even after they are sold to end users, tremendously stifles of innovation. Far from being the subject of an exemption, it shouldn't be allowed to begin with! But while the DMCA remains in effect, we shall have to make due with exemptions. That is why I am arguing in favor of jailbreaking exemptions for class 3, 4 and 5 devices under the DMCA.