(Long) Comment Regarding a Proposed Exemption (Under 17 U.S.C. 1201)

Item 1. Commenter Information

Jay Freeman (saurik); +1 (805) 895-7209; saurik@saurik.com; SaurikIT, LLC (Member)
Mailing Only: 8605 Santa Monica Boulevard #21162; West Hollywood, CA 90069, USA

Item 2. Proposed Class Addressed

Proposed Class 17: Jailbreaking — all-purpose mobile computing devices

Item 3. Statement Regarding Proposed Exemption

In the comments from the Business Software Alliance, a fundamental misunderstanding seems to have taken place: they seem to believe that the ability to install any third-party app makes a device open, and constitutes an alternative to circumvention. As discussed in my earlier comments, the kind of software that users install on modified devices goes far beyond the notion of an "app": instead, the focus is on installing "new features to the platform", whether the modifications are simple in nature (a modified graphical theme or reorganized menu) to complex (changing the way notifications, or the interface, works).

Later in these comments, the Business Software Alliances quotes the comments of the Electronic Frontier Foundation out of context, generalizing a statement that two specific manufacturers of Android devices now offer ways of jailbreaking their devices to a wider "Android manufacturers". This rhetorical slight of hand hides the reality that due to the much more limited hardware options able to be offered by these two manufacturers, the vast majority of consumers are forced into an awkward tradeoff: buy a device that they can easily modify, or buy a device that actually contains hardware of reasonable quality.

The Business Software Alliance then tries to claim that maintaining closed systems via software access controls deserves "at least some credit" for the "golden age" of "mobile devices, device firmware, and mobile applications". They conveniently fail to mention, of course, that due to the security of these devices actually being pitifully weak, almost all devices, from both major and minor brands, everything from toys to flagship hardware, has been "de facto open" for almost the entire lifetimes of these products; obviously, the success of these platforms cannot be due to a security mechanism that never worked.

The most unique argument made by the BSA is in regards to the ability to use a laptop as an alternative to circumvention, and that a laptop could be included in the set of "all-purpose mobile computing devices". At this time, all laptops using the power-efficient ARM CPU design (which is almost exclusively used in the devices which are "mobile") are locked down and require "jailbreaking". The Microsoft Surface that is mentioned by the BSA uses this CPU, making an interesting choice for them to use in their example.

http://www.geek.com/microsoft/how-to-jailbreak-the-surface-rt-1538987/

http://www.makeuseof.com/tag/how-to-jailbreak-your-windows-rt-device-and-run-unapproved-desktop-software/

Finally, I will respond to the "call for evidence" related to the inability to install software that "expresses political commentary", as stated by the EFF: there have actually been many examples, but a quick search on Google turned up, in the first few results, a well-known example: MyShoe, an application which was rejected from the Apple App Store; this application used the device's accelerometer to simulate throwing a shoe at George W. Bush. While this application may or may not be "in good taste" or "in good form", it is a clear example of software that "expresses political commentary" users could not get.

The BSA ends their argument by bringing up the specter of piracy. They do this without either responding to or acknowledging that piracy on all of these devices (including on the iPhone, as demonstrated in my comment) does not require jailbreaking. This is an argument that has also been well worn previously; in 2012 the Copyright Office stated "While Joint Creators raised concerns about pirated applications that are able to run on jailbroken devices, the record did not demonstrate any significant relationship between jailbreaking and piracy.": the BSA neither acknowledges this nor attempts to refute it.

In response to General Motor's comments, their entire argument seems to come down to an attempt to rely on a law, the DMCA anti-tampering clause, to make their systems secure. They describe a scenario where malicious agents are somehow suddenly able to hack into and modify their vehicles, something that was somehow impossible before when this might be covered by the DMCA. (I say "might", as in MGE UPS Systems, Inc. v. GE Consumer and Indus, Inc., "mere access" to a copyrighted work has been stated to not be covered by the DMCA.) This is clearly an absurd implementation of "security".

Frankly, General Motors seems to fundamentally misunderstand the safety capabilities of their own vehicles: in the second half of their comment, they shift the argument from remote malicious agents to modifications by the owner, stating that their stock "ECUs are designed to be operated as built by the automobile manufacturers, and not to be modified by circumventing TPMs". However, the same can be said of the vehicle's tires and transmission, as well as for the vehicle's headlights and door locks; yet, all of these components are easily (and legally!) removed, modified, or replaced by the car's owner.

To look at this notion in more depth, one could make the same argument made by GM for TPMs about tires: that allowing consumers to modify the tires on the wheels of their vehicle, carefully designed to comply with federal regulation, and which is critical to the safety of the vehicle, or to simply remove the door locks on their car, which are clearly necessary to guarantee the safety and privacy of the user, that this will somehow "limit the availability of tires and wheels, or cars with doors that have locks, in the future and suppress innovation (such as remote door locks or self-healing tires...) in these sector".

It is thereby not just clear, but to be frank, "fundamentally obvious", that the TPMs GM has put in their vehicles simply cannot be argued to be serving a copyright purpose, per the argument they have made. They are not using this TPM to prevent users from illegal redistribution of their software or data: they are trying to claim this TPM has the purpose of guaranteeing the safety of their vehicles. This does not seem to be a control measure

that the DMCA even claims to protect from tampering, nor is it a use case that actually provides them or users any real security, making GM's arguments a waste of our time.

Further, it must be pointed out that GM seems to misunderstand the key terminology in place for "jailbreaking" and "unlocking". On page 8 of their comment, in footnote 15, GM claims that because of a new agreement via the FCC related to carrier unlocking (which is when a phone under contract with one cellular provider, such as AT&T, is modified for use on another, such as T-Mobile), this somehow means that "consumers can download applications of their choice on their smartphones or other handheld devices". This is, of course, unrelated. In fact, "other handheld devices" are why we ask for this exemption!

On page 9, GM makes an argument that tampering with their vehicles may lead to the user violating other federal laws by tampering with the emissions-oriented mechanisms of their vehicles. It is neither GM's responsibility nor the goal of the DMCA to prevent the consumer from violating other federal laws, nor is this a necessary layer of protection for anyone involved given that the activity is already illegal. (And again, their argument later comes back to the case of a malicious agent acting against the consumer by modifying their vehicle in a way they could not detect, something the DMCA simply can't prevent.)

On page 12, connected with some earlier comments on page 3, GM claims that we did not meet our statutory burden for our class. In fact, we provided numerous examples of not just simple modifications made by individual consumers, but complex modifications made by businesses and sold for profit, generating millions of dollars of income for the developers: a substantial amount of new copyrighted works that should not exist without these exemptions. GM has then most graciously demonstrated that their software has a UI that could be modified in similar ways on page 10, which works with our evidence.

That said, this was a confusing side argument, because they also claim that we did not anticipate a car might be subject to our class. This is true: the word "mobile" as used by most consumers, implies the device is something that one could carry on their person, which immediately and succinctly removes all of GM's vehicles from this class. It does not seem either complicated or circumspect to see that at no point were GM's vehicles subject to being exempted by the class of "all-purpose mobile computing devices", as defined by most proponents. Maybe they should be included? We'll look at this for 2018.