From Britta Gustafson (britta@saurikit.com), June 2, 2015

I would like to respectfully respond to the letter about Class 21 from the National Network to End Domestic Violence. First, I acknowledge the root of their concerns: abusive use of spyware by intimate partners is a problem that happens right now on devices including general-purpose computers and both non-jailbroken and jailbroken smartphones.

But I support Class 21 because my experience indicates to me that lawful independent security research on vehicle software will help prevent abusive surveillance from spreading to vehicles. Independent experts need to be able to do legal security research on vehicle software in order to find and report vulnerabilities that could lead to the development and covert installation of malware, and to detect and understand any future malware in vehicles.

I have been working as a community manager for Cydia for jailbroken iOS devices for the past four years. The record for smartphones shows that security research has made those devices more secure over time, not less: iOS jailbreakers and other researchers who have reported and published vulnerabilities have contributed to strengthening iOS to be one of the most secure operating systems available to consumers.[1] Even though Apple is a sophisticated and powerful software company that can attract and hire some of the best software security experts, public investigation of iPhones for the past several years has still found a broad variety of serious vulnerabilities. Apple has fixed these in subsequent iOS versions and device models[2] — and even then, sometimes similar exploits are re-used in new jailbreaks because Apple's initial fix did not fully resolve the problem, requiring further fixes.[3] Software security is hard, and we cannot trust car companies to get it right. To protect people vulnerable to surveillance, we need robust and legal independent research. Often the way the public has found out about potential vectors for malware has been through independent security researchers; vehicle companies have an incentive to avoid publicly discussing scary problems with their software.

Stalkers and abusers likely are not especially concerned about violating DMCA §1201. The ban on vehicle software modification likely only deters those who are concerned about obeying the law more generally. Actual criminals (and people selling software to criminals) can make and use malware without consideration for copyright laws, and the proposed exemption only applies to lawful purposes, so continuing to criminalize legitimate security research is not likely to prevent abusive use.

[1] http://www.infoworld.com/article/2621796/mobile-security/apple-ios--why-it-s-the-most-secure-os--period.html "The security features in iOS were adopted by necessity, not by design. When it initially arrived in 2007, the iPhone immediately became a target of security researchers, who found vulnerabilities quite quickly." This article had a followup a month later after a new jailbreak was released, explaining that despite the jailbreak revealing a serious vulnerability, iOS was still overall a "very secure operating system": https://threatpost.com/new-iphone-jailbreak-makes-short-work-worlds-most-secure-os-070611/75401. An article from three years later: http://www.cnet.com/news/ios-scores-as-most-secure-mobile-os-in-new-report/

[2] Examples of Apple security update notes where they credit iOS jailbreak authors for exploits that Apple has fixed: http://thenextweb.com/apple/2013/03/19/apple-credits-evad3rs-jailbreak-team-with-4-of-6-software-bugs-fixed-in-ios-6-1-3/ and http://www.cnet.com/news/apple-credits-jailbreakers-for-ios-7-1-security-fixes/

[3] http://www.slideshare.net/i0n1c/syscan-2015-esserios678securityastudyinfail covers some examples of Apple not fully fixing vulnerabilities that then get re-used in subsequent jailbreaks, for example slides 22-27.

Declining an exemption for security research would also not prevent surveillance by abusers because owner-installed software and factory-installed legal tools can be repurposed by abusers. Victims using popular apps such as Facebook can accidentally leak information.[4] On iOS, built-in features such as "Find My iPhone" and "Find My Friends" can be misused by abusers, especially if they find out their victim's passwords.[5] Spyware tools such as MSpy do not require a smartphone to be jailbroken/rooted to provide a frightening amount of information.[6] If car software continues to grow more sophisticated and provide more tools for legitimate use by consumers, it will likely follow a similar pattern of being able to be misused. Digital stalking and abuse needs to be covered under the appropriate laws; using the Digital Millennium Copyright Act for this purpose is overbroad, with negative side effects on legitimate research, and it may also be redundant with the appropriate laws. The FBI has gone after at least one smartphone spyware provider under wiretapping laws.[7]

Another problem is that not all cars, especially older cars, may have ways to get official ECU software upgrades. If exploits get released for those cars, unofficial lawful software modification to preemptively fix the exploitable software bugs may be important and useful for many people, including vulnerable people. This kind of pattern has happened on smartphones — for older Android devices, rooting is sometimes the only way to get a newer version of the operating system with security patches. [8]

iOS has a very important feature for people concerned that they may be being stalked via malware or built-in tools: a novice user can wipe an iPhone's data and restore the operating system to default factory settings with a few clicks in iTunes. All cars need to have this important feature as well. As with most car maintenance, it may not be suitable to have this feature in the form of a one-click button for the owner, but it needs to be easy for a mechanic or dealer. If I am concerned that my car has been tampered with by a malicious partner, such as airbags removed or spyware installed, I will bring it to a service provider to check for problems. The service provider needs to have an easy and inexpensive way to first detect whether the ECU has been modified, and to reflash it back to stock as part of ensuring my safety.

Intimate partner surveillance is part of a societal pattern of surveillance technology being used against women — journalist Sarah Jeong has written about domestic use of spyware in a pattern with NSA officers abusing work tools to spy on loved ones and police officers using work databases to stalk women.[9] In that article she says "Privacy is about power, and undermining privacy serves the powerful at the cost of the powerless, even at home." It is very important for vehicle software to be subject to legal analysis by independent researchers.

[4] http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

[5] http://arstechnica.com/apple/2012/05/how-to-harden-your-smartphone-against-stalkers-iphone-edition/

[6] http://www.mspy.com/compatibility.html#tab-ios and http://www.mspy.com/compatibility.html#tab-android

[7] http://www.forbes.com/sites/kashmirhill/2014/09/30/stealthgenie-ugly-marketing-of-spyware/

[8] http://www.infoworld.com/article/2622494/mobile-technology/jailbreak--upgrading-a-non-upgradable-android.html

[9] http://www.forbes.com/sites/sarahjeong/2014/10/28/surveillance-begins-at-home/