

To whom it may concern,

The ability to jailbreak a device can be made easy enough for any user, however, use and maintenance require skills superior to those of the average user. Therefore, with the ethical principles typically associated with these atypical skill sets, an even smaller percentage of the user base would be inclined to use said skills for ill intent regardless of legal status. In the name of security for those who are not so quick to invest in the blind faith that iOS developers of all individual applications have every users best interests in mind; I support jailbreaking to gain root control of all intellectual properties interfacing with iOS software within copyright limitations. Further, the same should apply to control of any hardware used for multimedia or networked data devices including entertainment set-top devices and/or gaming consoles.

I am a network engineer by trade and interface with many varying hardware/software devices on a daily basis. Having over 15 years of experience in my trade, it has become obvious that the human element is a large contributor in system failures and security flaws. These can be found anywhere from hardware components and assembly, to system languages and integration, to IEEE standards. For those aware of these issues, control and auditing are imperative to the best practices and secure/trusted use and application of technologies.

The smartphone and tablet are fast becoming significant staples in the dissemination and sharing of information and multimedia; not forgetting communications in general. Were root access of such devices, though not without special knowledge, be limited by law; those with ill intent would still find ways to circumvent red-tape and legal bindings and those with knowledge will be forced to remain defenseless to attacks of their own person in order to comply.

To be sure, there have been many crooks fleecing customer pockets through app stores that customers blindly trust... and pay for. Each case could only exist where the theft was less than obvious to the subscriber.

Kevin Baker
Principal Network Engineer