I am a developer of games and applications for mobile phones. I support allowing owners of devices to "jailbreak" the devices – for the owner to be the final authority on what will and will not be allowed to run on the device.

A good example of why this needs to be allowed to continue is from my own experience:

I released a game for Android, and a common practice to promote a game is to release a video showing game play. The only way to capture video of the screen of a device is to "root" the device. There are no other ways possible. Not even if for extremely tech-savvy users like myself.

The fallback position is to use a camera to film the screen, but this is a pretty unacceptable result. The user's hand and fingers are constantly obscuring the action. In short, you can't film a game in action without "jailbreaking" or "rooting" the device. And this is a legitimate need of developers to create promotional and marketing materials for a product.

A secondary, but equally important aspect is security.

Cellular carriers and 3Rd party app developers have shown an increasing willingness to perform secret surveillance of their users through their mobile devices. While it is currently within their rights to do this, the rights of end users must be respected as well. Their right to not have their own devices secretly spying on their activities is protected by the ability of researchers to discover these operations.

Were it to be illegal to jailbreak devices, researchers would be forced to break the law to explore what information is being shared without the end users' consent. And furthermore, end users would have no options but to accept the unlicensed snooping, or to abandon the device's use.

The data generated from the surveillance is valuable to the companies that do this. But owners of devices are not compensated for the gathering of this data. And part of the reason is that many users would not consent to it if asked. Jailbreaking helps to even the tables, and to expose when companies providing software and devices are not being completely honest and transparent with the owners and users of those devices.

Remember that those being spied upon include our military, our police, our politicians, workers at nuclear plants, chemical plants, water treatment plants, and others security critical points. Do you want their whereabouts, habits and personal data shared with unknown third parties, and foreign corporations? I do not.

The device and software providers are not necessarily entities that have the same interests as the citizens of the United States for a safe, stable and secure country, governed by the rule of law, and characterized by fair business transactions.

The ability of device owners to have final and absolute authority to choose what software runs on their devices helps users not served by the mainstream market to use their devices to accomplish their work and goals. It also helps the country as a whole, by creating a more secure and trusted computing environment all of us.

Zachary Foley

Los Angeles, CA

2012-01-25

Comment number(s) of proposed classes of works to which you are responding: 5.