Term Paper Proposal

By Sean Glover

CSC 300: Professional Responsibilities

Dr. Clark Turner

October 8, 2010

Abstract

The electronic devices we use are physical objects that we paid (potentially) exorbitant amounts of money for, and therefore they are our property. Traditionally, property that is owned by a person is subject to certain rules that protect it from being modified and used by non-owners. It is illegal, for example, for a person to break into somebody's car and modify the interior coloring or take the stereo out. Recently, however, with regards to electronic devices, this concept of ownership is being challenged.

In June 2010, some owners of Android-based cellular phones were greeted with a surprise as they discovered that two programs, which are unnamed, were deleted from their phone without their consent. [9] This "remote kill switch" similar to previously discovered functionality in Apple's iPhone. [11] The question becomes quite clear: Is it ethical for software developers, hardware manufacturers, and/or service carriers to remotely remove applications from devices *that we own* without our permission? Taking into special account the "Software Engineering Code of Ethics," which guides all software professionals in ethical matters, it becomes quite clear that tampering with a device without consent of the device's owner is unethical at best, and dangerous at worst.

1 Facts

1. The Android Market allows for Google to remotely remove applications from end users' mobile devices as per provision 2.4. [1]
2. Apple also has the capability to remotely remove applications at their discretion. [11]
3. Sony removed the ability for Playstation 3 systems to install alternative OSes (which resulted in a class action lawsuit). [10]
4. Google invoked their "kill switch" in June of 2010 when they removed two applications from the Android Market and the phones that the applications were installed on. [9]
5. Google's Android platform is touted as a free and open source platform. [2]

2 Research Question

Is it ethical for software developers, hardware manufacturers, and/or service carriers to remotely remove applications from devices *that we own* without our permission?

3 Extant arguments

It is ethical to allow others to modify our devices without our consent:

- Being able to remotely disable programs is critical to the security of end users. [9] [11]
- The ability to remotely disable functionality is important to company security. [7]

It is not ethical to allow others to modify our devices without our consent:

- Disabling functionality on devices is "unfair and deceptive business practice..." [3]
- Disabling "malicious" software is too broad; "malicious" is ill-defined and can be taken to mean many things. [11]
- Disabling software and/or functionality can hurt the advancement of certain scientific fields in some cases. [7]

4 Applicable analytic principles

- Professionals should "disclose to appropriate persons or authorities any actual or potential danger...associated with software or related documents." [6]
- They must also "be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, *methods* and tools." [6]
- It is ethical to "respect the privacy of those who will be affected by (the) software." [6]
- Professionals should "Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful." [6]
- People should act in a way where their actions are motivated by "good willed" intentions, according to Kant. [5]
- People should act such that it causes the greatest amount of "happiness" for the most people, according to Utilitarian principles. [8]

5 Abstract of Expected Analysis

1. Remotely disabling or removing software/functionality on a device that one does not own is ethically sound, based on the premise of security, but is not the best way to handle it.
   (a) If used for the sake of security, the intent is one which is good-willed.
   (b) There is a tradeoff, however, in that there are other ways to have good intent, but not be invasive (invasion of privacy violates the SE Code). [6]
   (c) For example, the company could follow the mentality of virus scanning software, which simply informs the user of a problem and asks the user what to do about it, rather than assume that the user wants it gone.
   (d) The tradeoff is that the public gains more freedom with their devices, while the manufacturer and developers lose a little bit of control over the software that interacts with "their" hardware and software.
2. The ability to remotely disable software is easily abused and, as such, could be detrimental to the "public good."

(a) If Google or Apple determines that a common program that enables a device to perform unadvertised functionality (Tethering, for example), those applications could be seen as "malicious" and "security threats" and, as such, be subject to deletion.

(b) Once again, the tradeoff is between the freedom of the consumer to do what he wants with the device that he owns vs. the freedom of the provider to control their products.

3. It is ethical for companies to avoid deception in statements regarding their software, and hiding these "kill switches" in the depths of terms of service agreements is a shady practice. [6]

   (a) It is not obvious and clear when a person buys a phone or other device that Google, Apple, etc. have the ability to remotely disable applications.

   (b) In the case of Apple's iPhone, the terms of service do not even explicitly mention that Apple has this remote "kill switch" functionality. [4]

   (c) In the case of Sony's Playstation 3, the company repeatedly said that it would continue supporting the "Other OS" feature. That they went back on their word is very deceptive. [3]

4. The ability to remotely disable software can be considered dangerous in the case where a company such as Google or Apple is compromised and a malicious person gains the ability to remotely disable software on consumers' devices.

   (a) This becomes the responsibility of the engineer, who, at some point, must have revealed to other workers and the companies in question the dangers of the software and its capabilities (in this case, the ability to remotely disable functionality). [6]

   (b) In an admittedly rare case such as this, it is extraordinarily dangerous to have such functionality available, even if it was intended for "good."

References

[1] "Android market terms of service." [Online]. Available: http://www.google.com/mobile/android/market-tos.html

The Android Market Terms of Service shows the provisions that every user agrees to when using the Android Market on Android smartphones. There is a provision (2.4) that explicitly states that Google may remove applications remotely if an application violates various policies and/or laws.

[2] "Android overview." [Online]. Available: http://www.openhandsetalliance.com/android_overview.html

The Open Handset Alliance's explanation of the Android platform, emphasizing its free and open source nature.

[3] "Anthony ventura et al v. sony computer entertainment america inc." [Online]. Available: http://www.wired.com/images_blogs/threatlevel/2010/04/sonysuit.pdf

The Sony lawsuit itself. Has arguments against remote disabling of functionality on devices.

[4] "itunes store terms and conditions." [Online]. Available: http://www.apple.com/legal/itunes/us/terms.html

The iTunes terms of service. These are what every user of the iTunes store must agree to. They do not explicitly say that Apple may remotely remove software.

[5] "Kant's moral philosophy." [Online]. Available: http://plato.stanford.edu/entries/kant-moral/

A good guide to Kant's moral philosophy, explaining the principles therein.

[6] "Software engineering code of ethics." [Online]. Available: http://www.acm.org/about/se-code

The Software Engineering Code of Ethics is the basis upon which this paper is written.

[7] "Sony's ps3 update could affect supercomputer users." [Online]. Available: http://www.wired.com/gadgetlab/2010/03/sonys-ps3-update-supercomputer-users/

Explanation of the situation regarding the Playstation 3 and how it affects science.

[8] "Utilitarianism." [Online]. Available: http://www.qcc.cuny.edu/socialsciences/ppecorino/intro_text/Chapter%208%20Ethics/Utilitarianism.htm

An explanation of Utilitarian ethics. Useful in analysing problems like the one this paper deals with.

[9] R. Cannings, "Android developers: Exercising our remote application removal feature," June 2010. [Online]. Available: http://android-developers.blogspot.com/2010/06/exercising-our-remote-application.html

The blog post where the Android Security Lead Rich Cannings explains that applications were removed from the Android Market as well as from users' phones remotely.

[10] D. Kravets, "Dropping ps3 linux support lands sony in court," April 2010. [Online]. Available: http://www.wired.com/threatlevel/2010/04/playstation-linux/

Wired article explaining Sony dropping the "Other OS" feature from the PS3, meaning that updating a PS3 would remove a feature that it previously had. Also mentions the lawsuit that resulted.

[11] C. Sorrel, "Apple sells 60 million iphone apps, jobs confirms kill switch," August 2008. [Online]. Available: http://www.wired.com/gadgetlab/2008/08/apple-sells-60/

Wired article explaining that Steve Jobs, CEO of Apple, confirms the existence of a "kill switch" that allows Apple to remotely disable applications on end users' iPhones.