

Hacking as a Form of “Self-Improvement”

Eric Clark
Department of Computing Sciences
Graduate School
Villanova University
Villanova, PA 19085
+01 610 721 9258
eric.clark@villanova.edu

ABSTRACT

When does hacking one’s own property pose an ethical problem?

Categories and Subject Descriptors

K.4.1 [Computers and Society]: Public Policy Issues - *Ethics*

General Terms: Legal Aspects

Keywords: Hacking, firmware, DVDs, cell phones, digital cameras

1. DISCUSSION

Hacking has long been a topic of great interest in the field of computer ethics, as attested by many references in the media as well as in the professional literature [1], [2], [3] [4]. These conventional notions can be summarized as illegally accessing someone else’s intellectual property and amount to a virtual “breaking and entering,” as well as stealing.

A far newer and much less debated aspect of hacking relates to “breaking into” one’s own personal property. The question arises, why would one “hack” into one’s own phone or camera? Recently, the most common reason is to gain access to features that, for monetary reasons, were locked by the manufacturer. A typical example of this is the camera/phone feature on the latest U.S. mobile phones. In order to increase revenue, most wireless carriers require phone manufacturers to install software to prevent the downloading of photos without using the cell phone’s fee-based transfer service. These same cell phones in Europe and Asia do not have the blocking software installed so there is no problem transferring photos via USB or serial cables. Websites such as www.cellphonehacks.com [5] are now emerging with “How to” instructions on the art of unlocking SIM cards on imported phones for use with US wireless plans.

Another good example of manufacturer installed blocking features is Canon’s Rebel 300D digital camera. It was released shortly after Canon’s more expensive and more feature filled 10D camera. Because of similarities between the cameras, curious developers (hackers) carefully examined each camera’s firmware. By slightly modifying the 300D firmware, many features of the 10D could be unlocked. This new firmware is known in the 300D community as the Wasia hack (named after the developer) [6]. This type of activity by Rebel camera buffs is becoming as common and as easy as installing an external flash or neck strap [7].

Copyright is held by the author/owner(s).

ITiCSE’05, June 27–29, 2005, Monte de Caparica, Portugal.

ACM 1-59593-024-8/05/0006.

This new type of hacking exists in a much grayer area than the traditional hacking. Here is the ethical “pull”. If a person legally owns something, shouldn’t they have the right to alter it in any way they deem appropriate for their needs? Most US mobile phone companies will only release SIM card information concerning their phones after several months into your plan. Now, most of the popular digital photography websites are banning people from posting links to “the hack”. But so far, no one has ever received an official warning from Canon, even though most of the webmasters fear that by providing direct links, they are assisting in the modification of proprietary software [8].

A highly publicized example of this type of “hacking” relates to ownership of DVDs. 321 Studios released DVDXCOPY, a product that allowed users to extract movies from DVDs and “back them up” onto a hard drive. The MPAA feared this would lead to the pirating of movies and launched a series of lawsuits against 321 Studios. While the lawsuits never really panned out, legal costs forced 321 Studios out of business. [9], [10].

What right do companies have to stop consumers from altering the devices they legally purchased? Manufacturers can, of course, refuse to honor warranties on products that have the additional features installed by unlocking blocking devices but where do they draw the line? Should Warner Brothers care if I edited Harry Potter 3 so that the deleted scenes are woven into a movie legally purchased from them? Does Ford sue aftermarket parts vendors because they can make a Mustang faster or more fuel-efficient? Ethical criteria separating legal from illegal “hacking” have yet to be determined by manufacturers, consumers or the government.

2. REFERENCES

- [1] Denning, D., “The U. S. vs. Craig Neidorf,” *Communications of the ACM*, volume 34, no. 3 (March 1991), pp. 23-32.
- [2] Kapur, M. “Civil Liberties in Cyberspace: When does hacking turn from an exercise of civil liberties into crime?” *Scientific American* (September 1991), pp. 158-162.
- [3] Levy, S. “Wisecrackers,” *Wired Magazine* (March 1996)
- [4] Spafford, E. “Are Computer Hacker Break-Ins Ethical?” *Journal of Systems Software*, volume 17 (1991), pp. 41-47.
- [5] <http://www.cellphonehacks.com>, last accessed 20-02-05.
- [6] <http://satinfo.narod.ru/en/>, last accessed 20-02-05.
- [7] <http://www.digit-life.com/articles2/canon300dfw2/>, last accessed 20-02-05.
- [8] <http://www4.law.cornell.edu/uscode/17/117.html>, last accessed 21-02-05.
- [9] <http://www.wired.com/news/digiwood/0,1412,64453,00.html>, last accessed 20-02-05.
- [10] <http://www.321studios.com/>, last accessed 20-02-2005.