

## User resistance and repurposing: a look at the iOS 'jailbreaking' scene in Brazil

Adriana Amaral  
Unisinos  
Brazil  
adriamaral@unisinos.br

Rosana Vieira de Souza  
Unisinos  
Brazil  
rovieira.unisinos@gmail.com

### Abstract

The paper aims to discuss the growth of mobile platforms and the emergence of user counter-power in these environments. In that respect, we intend to reflect upon 'jailbreaking' practices from the users' point of view. The study is based on a qualitative approach that examined both motivations to engage in jailbreaking and critical incidents and included interviews with *Cydia Store* users from Brazil, the primary jailbreak apps store available to users of iOS devices. We discuss how the users of jailbroken handsets articulate the tensions between jailbreaking practice and market constraints, as well as the trade-offs and paradoxes (e.g. stability *versus* freedom) the users have to deal with in the jailbreaking scene. Our findings suggest that even though jailbreaking practices reflect social counter-power, it emerges from a free culture logic that legitimates the freedom to access, distribute or modify content and creative work, and not from an explicit political motivation.

### Keywords

Resistance; mobile media; hacker community; jailbreaking practices

### Introduction

The internet is seen as an open space that creates a number of collaborative practices. In contrast, freedom produces a deep worry concerning security issues. As the internet is moving towards a more mobile environment, the understanding of the dynamic structures of control underpinning the decisions on its nature are critical for society.

Some scholars (Benkler, 2006; Galloway, 2006 and Zittrain, 2008) point out that users of mobile devices are being locked down in a new wave of closed environments. By accepting more controlled spaces, they give up freedom in exchange for improving both security and stability. This is the case of devices from companies like *Apple*. An increasing number of users are looking for an experience that goes beyond the scripts defined by the platform owner. The practice called 'jailbreaking' has emerged as an alternative to those restrictions with around 22.8 million jailbroken iOS devices running *Cydia Store*, the jailbreak apps store (Perez, 2013).

Our main goal is to discuss the emergence of the user counter-power in such environments. The methodological design comprised a qualitative approach and data were collected by (1) analysis of discussion forum; and (2) in-depth interviews with jailbreakers. The interviews were conducted through the examination of both motivations for jailbreaking and critical events perceived as highly significant for either success or failure of the practice (Critical Incident Technique, Flanagan, 1954). This preliminary phase was conducted from April to June 2013 (24 critical incidents from 12 interviewees).

### Resistance in the mobile environment and Jailbreaking

Lately, a "post-PC" era has been debated due to the unprecedented adoption of mobile devices. As a new computer-mediated platform, what is at play is the role of mobile operating systems (e.g. *iOS*, *Android*) in the mobile environment. Mobile digital devices designed by *Apple* such as the *iPhone*, *iPod*, and *iPad* are referred to as iOS devices once all of them run the iOS operating system. The release of the official *App Store*, in July 2008, set up the beginning of the app store market for native apps.

All of these "i-devices" bring together several features that constitute a very attractive business model for the handset manufacturer since it profits from the device-specific native apps sold

through the App store and the interoperability of the iOS devices. The fact that users cannot realize the full potential of these devices has been seen as one of the reasons for the expansion of jailbreaking practices in the hacking and user communities.

Jailbreaking could be investigated both from the hackers or the users' point of view. Even though the literature on the hacking scene has covered fundamental aspects such as ethics, politics, economic and technical practices of hacking (Wark, 2004; Coleman, 2013) less attention was paid to the user's experience with jailbreaking strategies.

Jailbreaking allows users to change a device's operating system to run a number of applications not approved by *Apple* or to open up additional features. The procedure includes the download of free computer software that installs a hack onto the device and the installation of an alternative store called *Cydia*, released in February 2008. *Cydia Store* was developed by Jay Freeman and is considered the primary jailbreak apps store. Its name is allusive to the *Cydia pomonella*, the scientific name for the "worm of the apple". Some analysts claim that the practice of jailbreaking iOS devices has evolved into a lucrative industry earning about \$10 million in annual revenue with 4.5 million active weekly users worldwide (Shapira, 2011).

Even though jailbreaking makes the installation of pirated apps easier, it is not the main goal of such a practice. For some of the biggest jailbreaking communities like the iPhone Dev-Team, jailbreaking benefits people who are willing to take back control over their iOS devices. Besides, jailbreaking is considered legal in the USA since the Library of Congress ruled that it does not violate *Apple's* copyright. In Brazil this is still a grey area since it has no legislation on the issue yet. Despite that, *Apple* claims that the practice voids the handset's warranties. The company actively improves the anti-hacking strategies in every upgrade of the mobile operating system, bringing more complexity to the task for the hacker communities (Greenberg, 2013).

## Results and Discussion

The jailbreakers expect an experience that resembles the flexibility provided by the internet. Therefore, they intend to extend the device capabilities in order to keep it more personalized (Fig. 1) or to escape from purchase requirement before the experience with the app. These motivations are legitimated by the perceived high costs of the iOS devices in the Brazilian market, as stated by Camila, an undergraduate Fashion student: "*You stop and think that you pay a lot for something that is not what you expected, and since Apple do now allow you to perform a 'test drive' for apps then it is complicated*".



**Figure 1:** Screenshot of jailbroken iPhone home screen with personalization apps.

The possibility of being creative through flexible and open environments and, on the other hand, the security of closed and stable devices provided are typical trade-offs the jailbreakers have to deal with. This decision, though, does not always happen with full comprehension of both the upside and downside of this practice, since it is not clear for the users the risks with which the device is involved. Even though the jailbreaking itself is seen as a user resistance mechanism, the users need to cope with the “not controllable” side of the practice. James, an undergraduate student of Geography, described the practice of downloading cracked apps as risky if the user depends on the app for working: “When I know that the app is very important for my presentations, I need to buy it ‘cause I cannot take the risk of having an unstable app”.

On the other hand, a positive event for jailbreakers is when they get rid of the restrictions they perceive as framing their use of mobile devices when the jailbreak process works well. As Laila, a 15 years old girl who reported how important it was for her to have the apps her friends have because they use another operating system and her parents don’t let her pay for apps.

## Conclusion

Since the results point out the paradoxical nature of this relationship (users-technology) (Mick e Fournier, 1998), some tensions might not be easily solved in the jailbreaking scene (Straw, 2006).

The results of this preliminary data indicate that jailbreaking could be seen as a social counter-power that reflects the weakening of the manufacturers’ hegemonic positions. The findings suggested that although jailbreaking indicates some kind of resistance to the market, it doesn’t emerge from an explicit political motivation, but instead, from a free culture logic that legitimates the freedom to access, distribute or modify content and creative work.

These situations are especially significant for those who believe they pursue interests that are outside of the intended by the company. They believe that there is an iOS that are for “medium users” for whom the official functionalities and apps will work well. However, if the user seeks personalization and the right to download whatever they want to an expensive device (in Brazil), the jailbreak is an alternative despite some risks involved in the practice.

## Acknowledgments

We would like to thank *Ford Foundation* and the Brazilian funding agency *CNPq* for financial support.

## References

- Benkler, Y. (2006). *The wealth of networks: how social production transforms markets and freedom*. New Haven: Yale University Press.
- Coleman, G. (2013). *Coding Freedom*. The ethic and aesthetics of hacking. New Jersey: Princeton University Press.
- Flanagan, J.C. (1954). The critical incident technique. *Psychological Bulletin* 5, 327–358.
- Galloway, A. (2006). *Protocol: how control exists after decentralization*. Cambridge: MIT Press.
- Greenberg, Andy (2013). Evasi0n is the most popular jailbreak ever: nearly seven million iOS devices hacked in four days. *Forbes*, February 8. Retrieved from <http://www.forbes.com/sites/andygreenberg/2013/02/08/evasi0n-is-the-most-popular-jailbreak-ever-nearly-seven-million-ios-devices-hacked-in-four-days/>
- Mick, David Glenn; Fournier, Susan (1998). Paradoxes of technology: consumer cognizance, emotions and coping strategies. *Journal of Consumer Research*, 25, 123-47.
- Perez, S. (2013). “Evasi0n” overloads servers as over 270,000 people download the new jailbreak for iOS 6.0/6.1 devices, including iPhone 5. *TechCrunch*, February 4. Retrieved from <http://techcrunch.com/2013/02/04/jailbreaking-is-back-new-evasi0n-software-works-on-most-ios-6-06-1-devices-including-iphone-5/>

Shapira, I. (2011). Once the hobby of tech geeks, iPhone jailbreaking now a lucrative industry. *The Washington Post*, April 6. Retrieved from [http://www.washingtonpost.com/business/economy/once-the-hobby-of-tech-geeks-iphone-jailbreaking-now-a-lucrative-industry/2011/04/01/AFBJ0VpC\\_story.html](http://www.washingtonpost.com/business/economy/once-the-hobby-of-tech-geeks-iphone-jailbreaking-now-a-lucrative-industry/2011/04/01/AFBJ0VpC_story.html)

Straw, W. (2006). Scenes and sensibilities. In: *Revista Ecompós*, Brasília, Ed. 06,. Retrieved from <http://www.compos.org.br/e-compos>

Wark, M. (2004). *A hacker manifesto*. Cambridge: Harvard University Press.

Zittrain, J. (2008). *The future of the internet: and how to stop it*. New Haven: Yale University Press.