

Chapter 46

College Students, Piracy, and Ethics: Is there a Teachable Moment?

Jeffrey Reiss

University of Central Florida, USA

Rosa Cintrón

University of Central Florida, USA

ABSTRACT

This study explores the nature of piracy prevention tools used by IT departments in the Florida State University System to determine their relative effectiveness. The study also examines the opinions of the Information Security Officer in terms of alternative piracy prevention techniques that do not involve legal action and monitoring. It was found that most institutions do not use a formal piece of software that monitors for infringing data. Furthermore, institutions agreed that students lack proper ethics and concern over the matter of copyright, but were not fully convinced that other prevention methods would be effective. The authors conclude that monitoring techniques are a short-term solution and more research must put into finding long-term solutions.

INTRODUCTION

With pressure from the Recording Industry of America (RIAA) and federal policies introduced in 2008, post-secondary institutions must implement software to monitor network activity to keep students off P2P software, dorm servers, and

any other online method of transferring media illegally (Joachim, 2004; Worona, 2008). Though some larger universities, such as the University of Florida, had already implemented software prior to the 2008 revision of the Higher Education Act, the remaining community colleges and smaller institutions were required to follow suit. Furthermore, as the new rules currently stand, institutions will not, at the present time, suffer any

DOI: 10.4018/978-1-4666-2136-7.ch046

penalties for failing to follow the procedures. After the appropriate committees interpret the rules, it is likely, however, that institutions will lose federal financial compensation for implementation failure, making the process burdensome for smaller, financially starved institutions (Worona, 2008). Though software will always play an important role, an expensive software solution becomes useless if students find an alternate route around the software. As a result, an institution may ultimately waste money on an ineffective solution only to replace it with another solution with a limited life-span due to technology's constant evolution.

The P2P blocking software, however, is only one part of the problem. With most institutions also blocking dorm servers and other potential piracy outlets, students feel that their personal freedoms are hindered. Despite the plethora of legal uses for P2P, its adoption was stifled due to the focus on illegal use. The dorm server ban is also problematic in a historical sense. The popular search engines Yahoo! and Google, two companies that made major contributions to the overall state of the Internet, began as dorm servers. By preventing students from utilizing these resources, institutions could easily and unknowingly prevent the next major Internet innovation satisfying a large private interest (Joachim, 2004). Thus, by exploring solutions that rely on more than software and legal threats, a university could potentially eliminate digital piracy without denying freedoms to students.

The following research question guiding the present study, focused on ethics, is part of a larger study investigating the multifaceted challenges of piracy in higher education: What alternatives are being considered to discourage piracy by college students at a lower cost than monitoring software? Although throughout this paper the term 'ethics' is used, the reader should understand that we are making particular emphasis on the field of study and research of technoethics. For the purpose of this paper we have aligned our definition of technoethics with that of this journal. That is,

technoethics is concerned with the "technological relationships of humans with a focus on ethical implications for human life, social norms and values, education, work, politics, law, and ecological impact" (Miah, 2010). Similar perspectives have been posited in the past by Bunge (1977) and more recently by Luppigini (2010).

REVIEW OF THE LITERATURE

According to Forester and Morrison (1994), software piracy first occurred in 1964 when Texaco was offered \$5 million in stolen software. Other cases occurred over the years but were solely private corporate programs such as air-traffic control programs and CAD software. Although these instances of software piracy were a different form of stealing trade secrets, mass software piracy only surfaced with the advent of the desktop computer and Microsoft. Bill Gates created the software programming language, BASIC, as part of a package with the desktop computer kit, the Altair. While the computer was poorly constructed, the software proved more useful, and some people made copies of the program to prevent others from purchasing the entire package (Forester & Morrison, 1994).

This view combined with the more powerful viewpoint of a software package being too expensive helped fuel consumers' justification to pirate or sell counterfeit copies. With the help of the early form of the Internet, counterfeit software became easier to distribute. In 1992, a major crackdown occurred on an Internet bulletin board known as Davy Jones Locker that sold pirated versions of expensive programs such as AutoCAD, and a number of Lotus and IBM products. Considering the pirated software from this site crossed national boundaries into nations such as Iraq (Forester & Morrison, 1994), the notion of a hostile nation obtaining software that could lead to the creation of a weapon to be used against the United States or its allies could prove dangerous. Another crack-

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/college-students-piracy-ethics/71013

Related Content

War 2.0: Drones, Distance and Death

Jai Galliot (2016). *International Journal of Technoethics* (pp. 61-76).

www.irma-international.org/article/war-20/152805

A Study on the Prevention of Cyberbullying in Workplaces

Youngkeun Choi (2018). *International Journal of Technoethics* (pp. 18-26).

www.irma-international.org/article/a-study-on-the-prevention-of-cyberbullying-in-workplaces/198980

Globalization in Benedict XVI's Caritas in Veritate

Patrick Flanagan (2012). *Ethical Models and Applications of Globalization: Cultural, Socio-Political and Economic Perspectives* (pp. 62-77).

www.irma-international.org/chapter/globalization-benedict-xvi-caritas-veritate/60420

Which Rights for Which Subjects? Genetic Confidentiality and Privacy in the Post-Genomic Era

Antoinette Rouvroy (2009). *Handbook of Research on Technoethics* (pp. 454-473).

www.irma-international.org/chapter/rights-subjects-genetic-confidentiality-privacy/21597

Health Ethics in a Global Context

Win Phillips and Cheryl Rathert (2012). *Ethical Models and Applications of Globalization: Cultural, Socio-Political and Economic Perspectives* (pp. 100-118).

www.irma-international.org/chapter/health-ethics-global-context/60423