

Chapter 6

Piracy and Intellectual Property Theft in the Internet Era

Shun-Yung Kevin Wang

University of South Florida – St. Petersburg, USA

Jeremy J McDaniel

Principal Financial Group, USA

ABSTRACT

Stealing ideas is not something new, but stealing and transporting ideas in a massive amount has become possible in the era of the internet. Based on the frameworks of criminological theory/thesis, this chapter intends to elaborate intellectual property theft and piracy in cyberspace. Contemporary cases of intellectual property theft and piracy are used to illustrate the blurred line between victims and offenders. The impacts of related information technology should be carefully appraised, as more and more intellectual properties are in digital format.

INTRODUCTION

Internet has quickly become an essential part of contemporary society across country borders for its capacity to offer a wide array of functions, ranging from information distribution, communications, financial and business management, to entertainments. Also, the Internet has evidenced itself as a unique medium with the fastest speed of diffusion in human history. With hundreds of thousand miles of optical fiber that connect servers and mega-storing devices together globally, several terabytes of digital information, as huge as those stored in the U.S. Congress Library, can be easily transferred from one end of the world to the other within minutes (Britz, 2013). In conjunction with widely available Wi-Fi and telecommunication (e.g., 3G, 4G, LTE) in many areas of the world, it is never this easy for an average user to transmit valuable information in digital format via mobile devices.

The information technology advances with incremental innovation, but business is the instrument that facilitates the widespread of the technology. The mechanism of business determines when to release certain technology, and the nature of business makes it user friendly for the purpose of obtaining a larger market share and a higher level of profit (Felson and Clarke, 1997). While legitimate opportunities are

DOI: 10.4018/978-1-5225-7492-7.ch006

created in the process, some offenders may take advantage. Like many innovations that have a tendency to crime (Merton, 1968), the growing capacity of Internet probably is too good to be true, as it has created new forms of intellectual property (IP). Before further discussing IP and elaborating the victimization of piracy, background of some theoretical frameworks of crime is necessary.

BACKGROUND

Basic Elements of Crime and Socio-Technical Gap

In their theory of crime, Cohen and Felson (1979) point out three elements of a crime incident: a suitable target, a motivated offender, and the absence of capable guardians. A suitable target is something valuable to potential offenders, and the target must be easy enough to be removed. Although crime rate is the highest among young males, motivated offenders can be anybody in the population, if an adequate opportunity is present. The guardians against crime do not necessarily refer to law enforcement. Instead, the owner of the targeted property, friends and neighbors of the property owners serve better roles of capable guardians that discourage potential offenders. In the scenario of burglary, potential perpetrators probably would less likely to choose houses that the owners are present or their friends/neighbors pay attention to. In the business settings, for another example, an office suite's receptionists who watch people entering the office can serve as the role of guardian. In sum, for a crime to occur, the above three elements have to emerge.

There is little doubt that industry has incentives to make their products lighter, more portable, more convenient, and more added functions and values, but this tendency naturally leads to some unwanted consequences of the products, such as suitable targets to theft. However, the social system (e.g., laws, justice agencies) usually simply reacts to the consequences of technological advancements pushed by industry and business. That is, technology proactively runs at the front, and the social system passively chases behind and (hopefully) fixes problems and challenges. In the era of Internet, the discrepancy between fast-growing Internet and information technology and the slow-reacting social system in the virtual space has created a cybergap in which crimes emerge (Huang and Wang, 2009). Explicitly, many more new digital IP are valuable targets with little to no meaningful guardians that trigger motivation of potential offenders in the cyberspace. The following section provides a description of IP theft and piracy. The discussion of IP and piracy in the present article is focused within the arena of those using digital technology, with an intention to compare and contrast several major incidents.

IP, IP Theft, and Piracy

The discussion of IP traditionally revolves copyrights, patents, trademarks, and trade secrets. Piracy has been generally defined as "the unauthorized use or reproduction of another's work," and it encompasses any individual or corporation that utilizes intellectual property in a digital form without the authorization of the originator (Business Software Alliance, n.d.; Filby, 2007). The nature of such behaviors is perceived as illegitimate, with some noticeable variation across different levels of civilization and cultures. For example, in some Asian societies with long histories, scholarly works are traditionally viewed as public goods contributing to the advancement of the entire society, and the scholars are informally "rewarded" with socially-recognized reputations and their social status. On the other hand, in the United States and

10 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/piracy-and-intellectual-property-theft-in-the-internet-era/213639

Related Content

A Study of Steganography Approach for Securing Data in a Confidential Communication Using Encryption

A. V. Senthil Kumar, Rahul Ramaswamy G., Ismail Bin Musirin, Indrarini Dyah Irawati, Abdelmalek Amine and Seddik Bri (2023). *Fraud Prevention, Confidentiality, and Data Security for Modern Businesses* (pp. 105-127).

www.irma-international.org/chapter/a-study-of-steganography-approach-for-securing-data-in-a-confidential-communication-using-encryption/317956

A Lightweight Authentication Protocol for Secure Communications between Resource-Limited Devices and Wireless Sensor Networks

Piotr Ksiak, William Farrelly and Kevin Curran (2014). *International Journal of Information Security and Privacy* (pp. 62-102).

www.irma-international.org/article/a-lightweight-authentication-protocol-for-secure-communications-between-resource-limited-devices-and-wireless-sensor-networks/140673

Design of Public-Key Algorithms Based on Partial Homomorphic Encryptions

Marwan Majeed Nayyef and Ali Makki Sagheer (2019). *International Journal of Information Security and Privacy* (pp. 67-85).

www.irma-international.org/article/design-of-public-key-algorithms-based-on-partial-homomorphic-encryptions/226950

Utilizing Sentence Embedding for Dangerous Permissions Detection in Android Apps' Privacy Policies

Rawan Baalous and Ronald Poet (2021). *International Journal of Information Security and Privacy* (pp. 173-189).

www.irma-international.org/article/utilizing-sentence-embedding-for-dangerous-permissions-detection-in-android-apps-privacy-policies/273597

Security Policies and Risk Analysis

Joseph Kizza and Florence Migga Kizza (2008). *Securing the Information Infrastructure* (pp. 137-160).

www.irma-international.org/chapter/security-policies-risk-analysis/28502