

# Chapter 5

## Policing of Movie and Music Piracy: The Utility of a Nodal Governance Security Framework

**Johnny Nhan**

*Texas Christian University, USA*

**Alesandra Garbagnati**

*University of California Hastings College of Law, USA*

### ABSTRACT

*Ongoing skirmishes between mainstream Hollywood entertainment conglomerates and Peer-to-Peer (P2P) file-sharing networks recently reached a crescendo when a Swedish court convicted members of the world's largest BitTorrent, The Pirate Bay, and handed out the stiffest sentence to date.<sup>1</sup> Four operators of The Pirate Bay received one year imprisonments and fines totaling \$30 million, including confiscation of equipment. While this verdict sent shockwaves amongst P2P networks, piracy remains rampant, and this incident further exacerbated relations between file sharers and Hollywood. In retaliation, supporters of P2P file-sharing attacked websites of the law firms representing the Hollywood studios (Johnson, 2009). This victory by Hollywood studios may be a Pyrrhic defeat in the long run if the studios do not soften their antagonistic relations with the public. This chapter explores structural and cultural conflicts amongst security actors that make fighting piracy extremely difficult. In addition, it considers the role of law enforcement, government, industries, and the general public in creating long-term security models.*

### INTRODUCTION

#### The Problem

The rapid digitization of film and music and their distribution via the Internet is reflective of a changing business model. Hollywood's delay

in adapting to and securing this new medium has resulted in unauthorized alternative sources supplying digital music and movies. Advanced covert illegal distribution networks known as "Darknets" have emerged (Biddle, England, Peinado & Bryan, 2002; Lasica, 2003). Darknets mask malefactors' identities and counter enforcement efforts by employing sophisticated technical measures within

DOI: 10.4018/978-1-61692-805-6.ch005

a closed hierarchical social structure resembling that of organized crime. In some instances, the lucrative operation of illegal file-sharing has drawn in traditional organized crime groups (Treverton, Matthies, Cunningham, Goulka, Ridgeway, & Wong, 2009).

The Motion Picture Association (MPA) estimated worldwide film industry losses from Internet piracy five years ago to be at \$2.3 billion, with 80% of downloads originating from overseas (Siwek, 2006). On an annual basis, the recording industry estimates losses to be at \$3.7 billion annually (Siwek, 2007). Rampant Peer-to-Peer (P2P)<sup>2</sup> file-sharing has been blamed for the decline of the music industry (Rupp & Smith, 2004). While these figures are debatable (Cheng, 2009), they do suggest that illegal file-sharing is a large and expensive problem. Large losses are, in part, indicative of a security deficit from industry's inadequacy to self-police.

To close the security gap, industry has collaborated with law enforcement in recent years. The Pirate Bay's recent conviction in Sweden may be attributed, in part, to the creation of an FB- and MPAA-trained elite "P2P hit squad" consisting of Swedish police.<sup>3</sup> Despite this recent success, law enforcement, in general, has been a reluctant partner in policing corporate victimization matters. This reluctance may result from a number of cultural and structural factors that prioritize street crimes. Historically, law enforcement has lacked the legal and jurisdictional flexibility to enforce complex crimes requiring inter-organizational relationships (Schlegel, 2000). Instead, it is a "slow-moving institution," rooted in social norms (Rowland, 2004) and fortified by a strong subculture resistant to change (Skolnick & Fyfe, 1993). Nevertheless, high-tech crimes in the past few decades have forced police to change their orientation from strictly crime control to embracing new policing models based on information and risk management (Ericson & Haggerty, 1997).

## **The Nodal Governance Model**

Security in the new policing model is co-produced by both police and non-state institutions (Bayley & Shearing, 1996). Maintaining security in this "plural" model is achieved by a decentralized network of public, private, and "hybrid" security actors (Dupont, 2006). In this new "Nodal Governance" model, institutional actors, or "nodes," actively participate in security by sharing capital in various forms, such as technology, resources, and expertise (Johnston & Shearing, 2003; Shearing & Wood, 2004; Burris, Drahos, & Shearing, 2005). Bayley and Shearing (1996) draw a distinction between *police* and *policing*, stressing the latter is performed by other non-state security stakeholders, such as private security and corporations.

We employ the nodal governance conceptual framework to analyze policing piracy efforts in cyberspace. We examine four aggregate nodal sets determined to be relevant to cyber security: (i) state law enforcement/government, (ii) the motion picture industry, (iii) the recording industry, and (iv) the general public. We draw distinctions between the enforcement of music and film piracy by empirically "mapping" the security network in California. This "mapping exercise" identifies formal and informal key actors, their security assets, and their relationships to each other in the security field (Wood & Font, 2004; Wood, 2006). An examination of relationship "gaps" will draw out conflicting cultural and structural variables among nodes and the overall capacity of the security network (Burris, 2004). We use these variables to explore policing effectiveness of Internet piracy.

In our chapter, we first discuss the study completed, starting with the methods of inquiry. Next, we review literature on nodal governance in greater depth. We also examine the Internet geography in situating nodal governance networks. In addition, we map each security actor: Law enforcement/government, the film industry, the music industry, and the general public. An analysis

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:  
[www.igi-global.com/chapter/policing-movie-music-piracy/46421?camid=4v1](http://www.igi-global.com/chapter/policing-movie-music-piracy/46421?camid=4v1)

This title is available in InfoSci-Books, InfoSci-Security Technologies, Information Warfare and Homeland Security, Science, Engineering, and Information Technology, InfoSci-Security and Forensics. Recommend this product to your librarian:

[www.igi-global.com/e-resources/library-recommendation/?id=1](http://www.igi-global.com/e-resources/library-recommendation/?id=1)

## Related Content

---

**Watermark-Only Security Attack on DM-QIM Watermarking: Vulnerability to Guided Key Guessing**

B. R. Matam and David Lowe (2010). *International Journal of Digital Crime and Forensics* (pp. 64-87).

[www.igi-global.com/article/watermark-only-security-attack-qim/43555?camid=4v1a](http://www.igi-global.com/article/watermark-only-security-attack-qim/43555?camid=4v1a)

**Bitstream-Based JPEG Encryption in Real-time**

Stefan Auer, Alexander Bliem, Dominik Engel, Andreas Uhl and Andreas Unterweger (2013). *International Journal of Digital Crime and Forensics* (pp. 1-14).

[www.igi-global.com/article/bitstream-based-jpeg-encryption-in-real-time/84133?camid=4v1a](http://www.igi-global.com/article/bitstream-based-jpeg-encryption-in-real-time/84133?camid=4v1a)

**Telephone Handset Identification by Collaborative Representations**

Yannis Panagakis and Constantine Kotropoulos (2013). *International Journal of Digital Crime and Forensics* (pp. 1-14).

[www.igi-global.com/article/telephone-handset-identification-by-collaborative-representations/103934?camid=4v1a](http://www.igi-global.com/article/telephone-handset-identification-by-collaborative-representations/103934?camid=4v1a)

**Digital Camera Source Identification Through JPEG Quantisation**

Matthew James Sorrell (2009). *Multimedia Forensics and Security* (pp. 291-313).

[www.igi-global.com/chapter/digital-camera-source-identification-through/26998?camid=4v1a](http://www.igi-global.com/chapter/digital-camera-source-identification-through/26998?camid=4v1a)