Chapter 9
Beyond Griefing: Virtual Crime

A. INTRODUCTION

Because there is so much money involved in virtual worlds these days, there has been an increase in criminal activity in these worlds as well. The gaming community calls people who promote conflict “griefers”. Griefers are people who like nothing better than to kill team-mates or obstruct the game’s objectives. Griefers scam, cheat and abuse. Recently, the have begun to set up Ponzi schemes. In games that attempt to encourage complex and enduring interactions among thousands of players, “griefing” has evolved from being an isolated nuisance to a social disease. Much in the same way crime has become the real world’s social disease. Grief is turning into crime.

DOI: 10.4018/978-1-61520-795-4.ch009

Some consider virtual worlds to be a game and therefore outside the realms of real law and merely subject to the rules of the game. However, some virtual worlds have become an increasingly important as a method of commerce and means of communication. In most circumstance the law is reluctant to intrude into the rules of the game, but it will do if necessary. (Lastowka & Hunter, 2004) Criminal law applies in virtual worlds as it does in the real world, but not necessarily in the manner that a player would expect or want. The law looks at the real consequences of actions, not the on-screen representations. (Kennedy, 2009)

According to one study, the majority of online crime is theft (73.3%) and fraud (20.2%). The average value of the online gaming loss is about $459 with 34.3% of the criminal loss between $100 and $300. (Chen, 2005) These figures come pre-
dominantly from Korea and Taiwan as there has been no study elsewhere. However a Newsweek commentator estimates that one million dollars in virtual goods are stolen every year. (Spring, 2006) In fact in the United States, police will not provide any assistance in recovering or investigating virtual theft. Final Fantasy XI player, Geoff Lurrs, brought his case before the Blaine, Minnesota police department after having $4,000 in virtual goods and currency stolen. He was refused any help. (Cavalli, 2008)

Although there are acceptable forms of theft in the rules of game play in most virtual worlds which have a questing theme, this is not not the sort of theft which is producing the statistics above. It is important to distinguish between in-game and out-of-game theft. There are ways which a character whose job is thief can steal from other characters within the game. He may ‘steal’ a valuable object while the owner’s attention is diverted. He may ‘kill’ or ‘harm’ the other player in battle and take his goods. If this is within the magic circle of game play, then there is no crime. This is part of the risks that a player takes within the game. The courts are unlikely to intervene unless there is actual cheating.

Such as, other in-game scams which may amount to theft or fraud. The most common include: (1) “Trade Window Switch” where the thief attempt to pass a valueless item as valuable only because it is graphically similar to a valuable item; (2) “Anni Scam (muling scam)” which occurs only when the items cannot be traded through a trade window, but instead must be dropped on the ground and left for anyone to pick up; (3) “Guess Who Scam” where the thief pretends to know the player only to ask for an item loan; and (4) “Item Switch Scam” where the player, after a trade, receives an item of less value than anticipated. (Darnoc, 2005)

Then there are out-of-game thefts when a player attempts to obtain access to another player’s virtual items through subterfuge, e.g., phishing and hacking. The Council of Europe’s Convention on Cybercrime is the leading international instrument defining computer-related criminal offences of this nature. There are four categories: (1) offences against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related offences; (3) content-related offences; and (4) offences related to infringement of copyrights and related rights. This is an excellent tool for conventional computer crime. But a distinction must be made between hacking and exploiting. Hacking is the equivalent of bending the laws of time and space to acquire someone else’s property. Exploiting is finding a flaw in the game and making the most of it. The ‘gold dupe’ is a classic example. The character finds the gold dupe flaw and duplicates currency to the point of devaluing the currency of the entire world. This is not quite counterfeiting but rather finding an ATM which endlessly provides £100 notes instead of £10 notes. (White, 2008) However, even within the scope of activities permitted in virtual worlds, transactions do go wrong. Some of these ‘bad’ transactions, in fact, are real world fraud pure and simple.

B. THEFT

Section 1 of the United Kingdom’s Theft Act 1968 defines theft: “A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it...” Section 15(4) of the Theft Act states: “For the purposes of this section ‘deception’ means any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person.” The U.S. Model Penal Code (MPC) 1962 §223.2(1) theft provisions are divided into an unlawful taking, theft by deception, and embezzlement. A person is guilty of theft by unlawful taking or disposition if “he unlawfully takes, or exercises unlawful control over, mov-