Chapter 2
Hacking:
Legal and Ethical Aspects of an Ambiguous Activity

Gráinne Kirwan
Dun Laoghaire Institute of Art, Design and Technology, Ireland

Andrew Power
Dun Laoghaire Institute of Art, Design and Technology, Ireland

ABSTRACT

Hacking is an activity which has long been tied with ethical and legal complications. The term has evolved to have both ethical and unethical connotations, which can be confusing to the uninitiated. Hacker subculture has a myriad of terminology, sometimes with subtle variations, and this chapter identifies the main subcategories of hackers. The methods used by hackers to infiltrate systems will also be briefly examined, along with the motives for the activities. The question of whether or not hacking can be an ethical activity, and how it should be dealt with by the legal system is considered in this chapter. Consideration is also given to the international legal perspective. The evolving hacker ethic is described and examined, and the justifications provided by hackers are investigated.

INTRODUCTION

The hacking subculture has developed a specific hacker ethic, which has evolved over the course of its lifetime. However, this ethical system is critically flawed in many regards, and its nature tends to be more hedonistic than truly ethical. Even the nomenclature of hacking culture has significant basis on the ethical position of the hacker, with specific terms (such as 'white-hat'; 'black-hat' and 'grey-hat') assigned to individuals depending on the behaviours they exhibit both during and after the hacking activity. The ethical distinctions within hacking have evolved to such an extent that it is possible to complete Masters level courses in 'Ethical Hacking' (such as that offered by Abertay

DOI: 10.4018/978-1-61350-132-0.ch002

University in Scotland). Realistically, excepting the cases where it is completed by an employee or consultant to benefit their own company or organisation, there are few cases where hacking could truly be considered ethical.

This chapter will introduce several taxonomies of hackers, and illustrate the difficulties in assigning hackers to any one of these classifications. For example, few hackers will consider themselves to be 'black-hat' (or malicious), even though they may engage in illegal activities, or activities which damage websites or computer systems. Further confusion is added by a wide variety of other expressions which are used to describe individuals engaged in various types of hacking activities, such as 'cracker', 'script-kiddies' and 'cyber-punks', to name but a few. To aid in understanding the nature of hacking, a brief overview will be provided of the techniques frequently used by hackers, along with the suspected motives for these actions. The ethical standards of hackers will then be examined, with particular focus on how these principles are ultimately self-serving, with little consideration for others. Finally, an overview will be provided of how hacking is viewed in the legal system, and the types of punishments that can be administrated, along with an evaluation of the likelihood of the success of these. The aims of the chapter are to provide the reader with an understanding of the various types of hacker, both 'ethical' and otherwise, to evaluate the 'hacker ethic' and how it is justified by hackers, and to investigate the legal implications of hacking behavior.

BACKGROUND

There are numerous cases of famous hackers widely available. For example, Gary McKinnon, who hacked into 97 US government computers, including the US Navy and NASA, between 2001 and 2002 using the online name 'Solo'. His declared motive was "to prove US intelligence had found an alien craft run on clean fuel" (BBC News, 28th July 2009, para. 3). McKinnon's hacking became an obsession, and other aspects of his life began to suffer the consequences. He lost his job and girlfriend, stopped eating properly and neglected his personal hygiene. In hindsight he indicated that he "almost wanted to be caught, because it was ruining me" (Boyd, 2008).

Former hacker Kevin Mitnick in particular has made a career from advising on computer security and has authored a number of books on hacking, with a particular focus on social engineering methods (see for example Mitnick & Simon, 2002; Mitnick & Simon, 2005). Mitnick was involved in hacking behaviors from a young age, manipulating telephone systems in order to play pranks and later progressing to infiltrating computer systems. He was apprehended by the police several times, and served time in prison for his hacking. He has since founded a company aimed at improving organisations' IT security, and regularly gives guest lectures based on his hacking experience and security expertise.

Adrian Lamo has also experienced a lot of publicity due to his hacking activities. His 'white-hat' attempts to improve the security of firms led to mixed responses from the companies involved – some were highly appreciative of his efforts, while others filed lawsuits against him (Mitnick & Simon, 2005). He has allegedly hacked into some very high profile companies, including Microsoft, Yahoo!, and Cingular. On managing to hack into the New York Times, he utilized their subscription to *LexisNexis* for three months, before reporting the security hole to the newspaper, via a third party journalist. The New York Times reported the infiltration to the FBI.

Definition and History of Hacking

Hacking began in the late 1950s at a few US universities at a time when computers were rare (Levy, 1984). The original hackers were motivated to use and improve computer technology, and many hackers today indicate that their motives have not