Chapter 5
Cyber Law, Cyber Ethics and Online Gambling

Lee Gillam
University of Surrey, UK

Anna Vartapetiance
University of Surrey, UK

ABSTRACT

Cyberspace offers up numerous possibilities for entertainment and leisure, and can be a rich source for information. Unfortunately, it can also be a dangerous place for the unwary or ill-informed. In this chapter, we discuss some of the legal and ethical issues that can arise in the interface between cyberspaces and real places for virtual tourists. We mention the difficulties posed by variations in laws in the physical world, and how these make for problems in the virtual world. We discuss how it is possible to create systems that embed adherence to laws and provide support for ethics in order to avoid harm to the unwary or ill-informed. We show how we have applied such principles in a machine ethics system for online gambling.

INTRODUCTION

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system…(Gibson, 1984, p.51)

DOI: 10.4018/978-1-61350-132-0.ch005

The advent of "cyberspace" has led to traditional geographical boundaries being transcended. Cyberspace also creates the illusion for people that most things are available cheaper or for free, and all actions undertaken are acceptable everywhere. Sitting in front of a computer, a person accessing the internet is virtually relocated to a "generalized elsewhere" of distant places and "non-local" people (Jewkes, 2003). While the person inhabits this generalized everywhere, they may be incorrectly extending the rules and social norms that are

applicable in their own physical location across the geographical boundaries, or believing there is a relaxation of regulations and restrictions. They may also be erroneously enlarging their personal security perimeter, acting under a false impression that the limit of communication is with the computer screen itself, or is restricted to specific intended set of interested people. In this generalized elsewhere, people can be whoever, whatever, and wherever they wish, presenting themselves and re-inventing themselves as they desire. Unfortunately, this also offers the opportunity for those with fewer scruples to pretend to be people who already exist, based on information they have managed to obtain from unsuspecting users who are under such illusions and who become susceptible to such problems.

A key difficulty for cyberspace users is in this rapid but undistinguished crossing of boundaries that include legal, ethical and religious, amongst others. For tourists in the physical world, there are often certain clear indications of when geographical boundaries have been crossed, and other symbols may identify such a difference. In cyberspace, one can rapidly move across boundaries of geography without ever being aware of the fact. This can create significant difficulties for software designers and internet users alike in understanding what applies, where it applies, when it applies, and, most difficult of all, why.

Over time, geographical entities have introduced, updated, replaced and even discarded laws that enforce or supplement societal and cultural norms. As technologies have emerged, lawmakers have attempted to keep pace. Unfortunately, reinterpreting through legal cases and through the crafting of new legislation where old was insufficiently encompassing can be awkward and appear ill-informed. During such processes, typically elongated if anything remotely useful is to emerge, the technology has usually moved on: the present pace of technological innovation is vastly outstripping the ability of the majority to keep up with new products, let alone for lawmakers to keep up with problems created by new products. If laws are found wanting, those developing such technologies have to make reference to ethics and professional standards while the gaps are closed, and must hope for the best outcomes when courts decide whether their use of new technologies is acceptable or not. The jurisdictional framing of laws introduces yet another issue: the illusion of the generalized everywhere is not reflected in any kind of generalized law. Cyberspace has no set of unified laws governing all actions, enabling the fight against the crimes, or for promoting the wellbeing of society and prevention of harm. There may be some degree of commonality in law, for example when European Union member states implement certain directives, but these can happen over varying time spans, and even the transfer to a national implementation may be considered incomplete (Ashford, 2010).

Cyberspace offers up many benefits, but many more substantial risks. It may be possible to trust in well-known brands, but there are many others attempting to deceive through masquerading as these trusted brands using, for example, phishing attacks. By compromising weakly secured systems, it is possible to construct botnets (Weber, 2007) that can coordinate attacks against yet other systems, act as spam generators to catch the unwary, deploy ransomware (Net-Security, 2010) or obtain and distribute personal data contained within such systems. By the time such systems are detected and blocked, yet further such botnets will have been spawned. Meanwhile, those who compose phishing emails or construct such systems are difficult to identify and bring to justice. Personal data obtained via such approaches can include credit card numbers, bank account details, and potentially even DNA profiles (Vartapetiance & Gillam, 2010). Such personal data is becoming increasingly valuable because it can be used fraudulently for purposes of identification. With such data, it becomes possible to obtain credit in another person's name, and consequently to impact on their credit records. The first that an affected, and innocent, party knows of this is when