1. INTRODUCTION

What if information on the website of a company in country A, is considered defamatory, an infringement of copyright, or an interference with a business relationship, by a company in country B? What if the allegedly wronged party sues for one of the foregoing causes of action in country A? Would the company in country B have to undergo the trauma, expense, and inconvenience of defending itself in country A? Cases such as these highlight the importance of jurisdiction, the authority of the defendant over the subject matter that has led to the prosecution, the authority of the prosecuting court over the defendant, despite their geographical location and the locations in which the crimes were committed. Jurisdiction generally describes any authority over a certain area or certain persons. In the law, jurisdiction sometimes refers to a particular geographic area containing a defined legal authority. Determining jurisdiction in a case of internet crime has proved
to be near impossible in many cases and in some cases it has appeared that the determining of jurisdiction has relied on opinion rather than fact (Whitehead & Spikes, 2006).

With the recent passing of the Digital Economy Act (passed in UK parliament on 7th of April 2010) the debate over internet jurisdiction has become highly public, with many people, including those the act claims to benefit, fiercely opposing its law, protesting that it is too severe and close minded. It has also in recent times exploded as a topic of conversation where a married footballer was named on Twitter as having an injunction over an alleged affair with a reality TV star. This particular footballer was eventually identified in Parliament as Ryan Giggs by Liberal Democrat MP John Hemming during a Commons question on privacy orders. The MP using parliamentary privilege to break the court order, said it would not be practical to imprison the 75,000 Twitter users who had named the player (Letts, 2011). This again was a problem of jurisdiction in that UK authorities simply knew that they could not ultimately defend against the ‘chatter’ on the Internet. This paper discusses the problems associated with jurisdiction on the internet, presenting well known cases which have influenced the current laws and have fuelled a long term debate that continues to get more heated.

2. COUNTRY SPECIFIC LAWS GOVERNING INTERNET JURISDICTION

Since the boom of domestic internet usage in the mid to late 1990’s, new laws have been created to help dictate what should be considered as correct and legal use of the internet. This section of the paper will document and explain some of the most significant laws to have been passed in an attempt to govern the internet. The first real act governing the use of data in the UK in response to the introduction of computerised systems and networks in an industrial capacity was the Data Protection Act (DPA), first introduced in 1983 and amended in both 1987 and 1998. The DPA does not have much jurisdiction over internet usage as it mainly governs the holding of data on computerised systems and can only be applied if data has been transferred over the internet in a way that does not comply with the DPA, for example if it has been sent from a company’s system that has the right to hold the data to a company’s system that has no right to hold the data. The majority of laws that have come into force governing the use of the internet have been aimed at child protection, a major issue on the internet. In the UK it is illegal both online and offline to:

- Entice or coerce a child under 16 to engage in sexually explicit conduct
- Import or transport obscenity using telecommunications public networks
- Knowingly receive child pornography or advertise child pornography
- Depict minors (or appear to be minor) engaged in sexually explicit conduct (even in pseudo-form)
- Advertise sexually explicit conduct by giving the impression that minors are engaged in sexually explicit conduct

However the law does not govern explicit material that is transported into the UK, a problem of geographical jurisdiction. In cases like this, courts will rely on the country which has jurisdiction over the material to prosecute using their laws. In a child protection case this is rarely a major problem as, although there are not many laws governing the internet, many countries have laws governing child protection on the internet as this is publicly acknowledged to be one of the largest risks posed by the internet.

The US Congress has passed 3 major laws to govern child protection online. The Communications Decency Act, or CDA (1996), was Congress’s first law to govern child protection. It made it