Chapter 1
Defining Online Aggression:
From Cyberbullying to Nonconsensual Pornography

ABSTRACT

The internet has become an inescapable part of our lives, and while it makes our lives easier, it also exposes us to online threats ranging from identity theft to denial of service to phony lottery/sweepstake scams. Among these online threats are those that are carried out with the direct intent of harming another person or group of individuals. This category of crimes is referred to as cyber aggression and includes cyberbullying, cyber-harassment, and cyberstalking. As technology expands, so does the opportunity for new forms of online aggression such as doxing and revenge porn. It is becoming difficult to keep up with new trends in acts of online aggression or distinguish between cybercrimes that appear to have similar definitions. This chapter acts as an introduction to online aggression by providing an overview of older and emerging forms of cyber aggression.

INTRODUCTION

Acts of cyber aggression, like other Internet crimes, have unique features making them more difficult to address. First, the Internet empowers perpetrators of cybercrimes by helping to mask their identity. Individuals who wish to remain anonymous can create multiple fake email accounts or use messaging

DOI: 10.4018/978-1-5225-5285-7.ch001

accounts such as Whisper, all of which conceal identity and make it more difficult for law enforcement to identify suspects and gather evidence. Even if law enforcement can determine the Internet protocol (IP) address of a computer from which a crime was committed, it can be difficult, if not impossible, to establish who used it (Jany, 2016). In addition, anonymity can increase the likelihood of someone committing a cybercrime by reducing inhibitions and individual restraint (D'Ovidio & Doyle, 2003). Second, since cybercrimes are not constrained by geographical boundaries, it becomes challenging to determine which level of government has jurisdiction. One example is the story of Canadian teen, Amanda Todd, who committed suicide in 2012. While in the 8th grade, a cybercrime perpetrator posted explicit pictures of Amanda online and sent them to her classmates. Although Amanda's family transferred her to different schools following the initial and subsequent incidents, the perpetrator continued to distribute pictures to classmates at each new school. After two years of being taunted and bullied by other students, Amanda committed suicide (Grenoble, 2012; Nobullying.com, 2017). Her tormentor, Aydin Coban, a 35-year-old Dutch male, was identified in 2014. Coban was found to have several victims in the United States., United Kingdom, Canada and the Netherlands. His modus operandi was to manipulate under-aged girls to pose seductively in front of a webcam and then use the images to extort, taunt and bully his victims (Nobullying.com, 2017).

Though Coban was arrested and sentenced in the Netherlands, jurisdictional issues can make obtaining justice more difficult. For example, who has jurisdiction when the victim lives in one jurisdiction and the offender lives in another? The answer is not always clear. The jurisdiction where a crime is tried can significantly influence legal relief for the victim. For example, the definition of a crime can and does vary among jurisdictions and in some instances what is a crime in one jurisdiction may not be a crime in another. Finally, if the cybercrime originates from a country where there is no extradition agreement with the country where the victim resides, there may be no legal resolution.

The differences in how cybercrimes are legally defined do not only vary between countries. In the United States the judicial response to cybercrimes has varied based on the level of government and the form of aggression (whether physical or cyber). For example, the federal government, all 50 states, the District of Columbia, and U.S. territories have enacted criminal