Chapter 9
Legislative Response to Cyber Aggression:
Federal and State-Local Policy Reform

Ramona S. McNeal
University of Northern Iowa, USA

Susan M. Kunkle
Kent State University, USA

Mary Schmeida
Kent State University, USA

ABSTRACT

This chapter presents the federal and state-local legislative response to cyber aggression: stalking, harassment, and bullying. Along with other federal efforts, the federal Violence Against Women Act and its reauthorizations is identified as a cornerstone law in protecting the public on stalking and harassment. State-local laws have advanced in scope; yet, there are laggard states not yet entirely on board in passing legislation aligned with the advancement of technology used in cyber aggression. All three branches of government to some extent have had a voice in today's cyber policy. Judicial court cases have shaped policy decisions and several key cases are presented.

DOI: 10.4018/978-1-7998-1684-3.ch009

INTRODUCTION

Cyber aggression takes on varying forms including stalking, harassment, bullying, and nonconsensual pornography. See Table 1 of Chapter 1. These are behaviors restricted by laws and court rulings. Federal and state regulatory and administrative legislation fighting these dysfunctional behaviors have been incremental in the making. On the federal level, the 1994 Violence against Women Act (Public Law 103-322) is a cornerstone law to supporting stalking victims such as women and children. It authorized grants to states and tribal government to fight the aggression on the domestic level. With cyberbullying, there is no chief federal law that governs over the behavior. Instead, the federal government has devolved authority to states and school districts, and judicial decisions have had an impact on school discipline policy. In the fight against cyber aggression, states know the protective needs of their local best, but not all are on board. While the majority has some type of law protecting residents from "physical" aggression crimes, not all have updated to include the "cyber" of aggression. This chapter discusses government action or inaction on enacting regulatory and administrative cyber aggression laws on stalking, harassment, bullying, and nonconsensual pornography.

BACKGROUND

With nearly half (49%) of the world online (Pew Research Center, 2017) more people are susceptible to cyber aggression as criminals use technology to cyber stalk, harass, and bully. This is not surprising since obtaining electronics for criminal intent is easy. Most anyone can purchase a computer, multifunctional cell phone device and supporting software; and access to the World Wide Web is becoming less costly and free in some places. The traditional "physical" stalking, harassment, and bullying behaviors now have a digital counterpart. The U.S. Department of Health and Human Services (2015) reports cyber aggression as an "emergent concern," and not limited to "sending threatening texts, posting or distributing defamatory or harassing messages, and uploading or distributing hateful or demeaning images or videos intended to harm another" (USDHHS, 2015). Concerned about cybercrime, some Americans are taking counter measures to confront the unfriendly digital climate. A 2013 Pew Internet & American Life Project survey found as many as 55% of respondents reported avoiding online observation by people, employers, government, organizations, and other; while 86% of adult Internet users have taken measures to promote anonymity, privacy, and security online. To avoid surveillance, online safety behaviors range from masking personal information, clearing search histories, to using a public computer instead of personal home computer (Pew Internet & American Life Project, 2013).