# Chapter 32

# The Internet Never Forgets: Image-Based Sexual Abuse and the Workplace

### Melody Lee Rood

University of North Carolina at Greensboro, USA

### **John Schriner**

https://orcid.org/0000-0001-5588-2432

City University of New York, USA

#### **ABSTRACT**

Image-based sexual abuse (IBSA), commonly known as revenge pornography, is a type of cyberharassment that often results in detrimental effects to an individual's career and livelihood. Although there exists valuable research concerning cyberharassment in the workplace generally, there is little written about specifically IBSA and the workplace. This chapter examines current academic research on IBSA, the issues with defining this type of abuse, victim blaming, workplace policy, and challenges to victim-survivors' redress. The authors explore monetary motivation for websites that host revenge pornography and unpack how the dark web presents new challenges to seeking justice. Additionally, this chapter presents recommendations from the literature focusing on shifting cultural attitudes, effective legislation, and increased education and training.

This chapter published as an Open Access Chapter distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

DOI: 10.4018/978-1-6684-5598-2.ch032

## INTRODUCTION

It is estimated that 1.2 trillion photos were taken in 2017; out of those images, 85% were from smartphones (Richter, 2017). In a 2015 survey that looked into "commonly regretted types of social media posts" among adults ages 18 and older in the United States, 14% shared pictures that could potentially impact their reputation at work; 10% sent intimate, sexual messages with a fear that their privacy could be breached (YouGov, 2015). While documentation culture becomes increasingly normalized with popular social media platforms like Instagram, Tik Tok, Twitter, and YouTube, a growing concern is how online presence can impact educational and/or professional prospects. It is commonplace to see social media accounts include prefacing statements in the account's bio section, declaring thoughts and opinions as one's own and not a reflection of the views of any institution in which that user is associated. Not only should people be cautious of their individual contributions to their online identities, but there is also the fear of what others can say or do without consent. Cyberbullying only exasperates this concern.

In a survey titled, "Online Hate and Harassment: The American Experience," 53% of internet users in the U.S. claimed to have experienced some form of harassment; 37% experienced severe harassment from sexual harassment to physical threats and stalking (ADL, 2019). Image-based sexual abuse (IBSA) or what's commonly known as "revenge pornography" is a type of non-consensual cyberharassment with effects that jeopardize reputation, job security, professional and educational aspirations, mental health, and in some cases, physical safety.

Revenge pornography can be defined as: "Sexually explicit images or videos of an individual, published online without their consent and with the intent to cause them distress" (Chandler & Munday, 2019). Revenge pornography is a type of cyberharassment that often directly impacts the workplace and one's job prospects. Once an image is uploaded to web platforms, it seems an insurmountable challenge to get it removed. The area of revenge pornography is akin to *doxxing*, that is, having one's personal information leaked to websites or forums—also deeply unsettling.

There is much written about cyberharassment and the workplace, although there is currently little to no academic research about specifically IBSA and the workplace. One's profession is very often the first target of abusers, as the authors explore in depth below. A major issue in dealing with IBSA is that private images can be uploaded by a single individual, but it is often shared so many times anonymously that it is difficult to find all the perpetrators. This type of mob mentality, or cyber mob, is typified by a phenomenon called *online disinhibition*. Online disinhibition, or more broadly *deindividuation* as social psychologists term it, is found when an individual experiences loss of self-awareness in a crowd: online disinhibition may be attributable to anonymity in a forum or a collective identity (Barlett & Helmstetter, 2018; Citron, 2016; Suler, 2004). Not all online disinhibition is harmful. The lack of being identified, as well as being physically separated, can help individuals with anxiety open up to strangers in online communities. That type of deindividuation is benign and can be described as the ease of communication online versus in-person, whereas *toxic deindividuation* is the ease of hurting others due to a perceived anonymity (Barlett & Helmstetter, 2018).

Toxic deindividuation can lead to less concern about social norms, and generally, the well-being of others. When individual accountability is not a concern, people may act differently than when they are identified. "It is these factors that desensitize people such that their social learning is altered to increase their willingness to engage in cyberbullying. Just as alcohol may disinhibit some people and consequently give them the courage (or stupidity) to pick a fight with a member of a biker gang at a bar, anonymity's

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/the-internet-never-forgets/301172

## Related Content

# Exploring the Link Between Cruelty to Animals and Violence Against People: Violence Against People and Animals – Evidence

Milica Boskovic, Nenad Putnikand Brankica Jankovic (2018). Social, Psychological, and Forensic Perspectives on Sexual Abuse (pp. 26-41).

www.irma-international.org/chapter/exploring-the-link-between-cruelty-to-animals-and-violence-against-people/197817

# New Forms of Victimization Linked to Video Games: A Multi-Level Proposal of a Categorization

Aiala Tejada García De Garayo, Mario Santisteban Galarza, Jesús C. Aguerriand Alba Diaz Ortega (2024). Modern Insights and Strategies in Victimology (pp. 56-75).

www.irma-international.org/chapter/new-forms-of-victimization-linked-to-video-games/342795

#### Tax Disclosures in Financial and CSR Reporting as a Deterrence for Evasion

Fábio Albuquerqueand Julija Cassiano Neves (2021). *Handbook of Research on Theory and Practice of Financial Crimes (pp. 397-427).* 

www.irma-international.org/chapter/tax-disclosures-in-financial-and-csr-reporting-as-a-deterrence-for-evasion/275472

### Dark Web: A Breeding Ground for ID Theft and Financial Crimes

Annamaria Szakonyi, Brian Leonardand Maurice Dawson (2021). Handbook of Research on Theory and Practice of Financial Crimes (pp. 506-524).

www.irma-international.org/chapter/dark-web/275477

# Combating the Exploitation of Children in Cyberspace: Technical Mechanisms to Protect Children From Sexual Content

Amar Yasser El-Bably (2021). Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities (pp. 42-67).

www.irma-international.org/chapter/combating-the-exploitation-of-children-in-cyberspace/270488