Dec. 6, 2024

CRJS 310

Cybercrime as a Social Problem

“If the Person is Made Up, is it a Crime?”

Amiah Armstrong, Jasmyn Wilhelm and Louis Ferrara

Want to watch this online? Check out this Youtube video for more! https://youtu.be/1R7ZQpYMeHA

Contents

Introduction 03

Discussing Digital Deception's Impact 04

- Framing the Discussion 05
- Legal and Regulatory Gaps 06
- Statistics and Real-World Examples 07
- Slide 07 References 08
- Why This Social Issue? 09

Tackling Fake Personas in Cyberspace 10

- Enforcing Stronger Identity Verification 11
- Enhancing Cybercrime Legislation 12
- Encouraging Digital Education 13

Conclusion 14

References 15

Introduction

There is a new problem caused by advanced technology. A problem unforeseen, but unfortunately, one that carries significant ethical and societal challenges. The creation of fake online identities is haunting the web. Anonymity is an attractive enabler, granting both freedom and a shield for malicious intent. Individuals take advantage of it to manipulate others, commit crimes, or create obscene content. There are countless laws that target fraud and identity theft, but technology is advancing rapidly. It is difficult for lawmakers to keep up with the problems associated with deepfakes and artificial media. That begs the question: should creating a fraudulent online identity be illegal? Today's technology, in general, has made the line between protecting privacy rights and freedom of expression very slim. Ignoring this issue will have great consequences in the future, so reevaluating current and future reforms is a must.

Objectives

- Go over growing issue of fraudulent online identities
- Examine societal impact
- Discuss legal and regulatory gaps

Overview

Since the internet has made it harder to distinguish between fact and fiction, people are wondering if it is illegal to create a fraudulent online identity. Besides the impact on individuals, this brings up societal issues related to security, trust, and integrity in the digital realm.

Discussing Digital Deception's Impact

Impact on Lives and Safety

Catfishing and fraud are examples of fake personalities that can ruin a person's reputation, finances, and emotions. Because anonymity enables bad actors to target weaker people, undermine trust in digital communication, and jeopardize financial security, they also contribute to cyberbullying and harassment.

Social and Cultural Norms

Despite being essential for privacy and freedom of speech, the acceptance of online secrecy also increases the susceptibility of individuals to online fraud because of their digital connections.

Broader Societal Concerns

False identities threaten privacy and security and weaken public confidence in technology. As shown by Russia's use of fake profiles to influence the 2016 U.S. presidential election, they have the ability to alter public opinion. Identity theft is widespread and can have negative financial and legal effects for victims. Scams that target marginalized groups also use fake profiles to take advantage of their weaknesses.

Legal and Regulatory Gaps

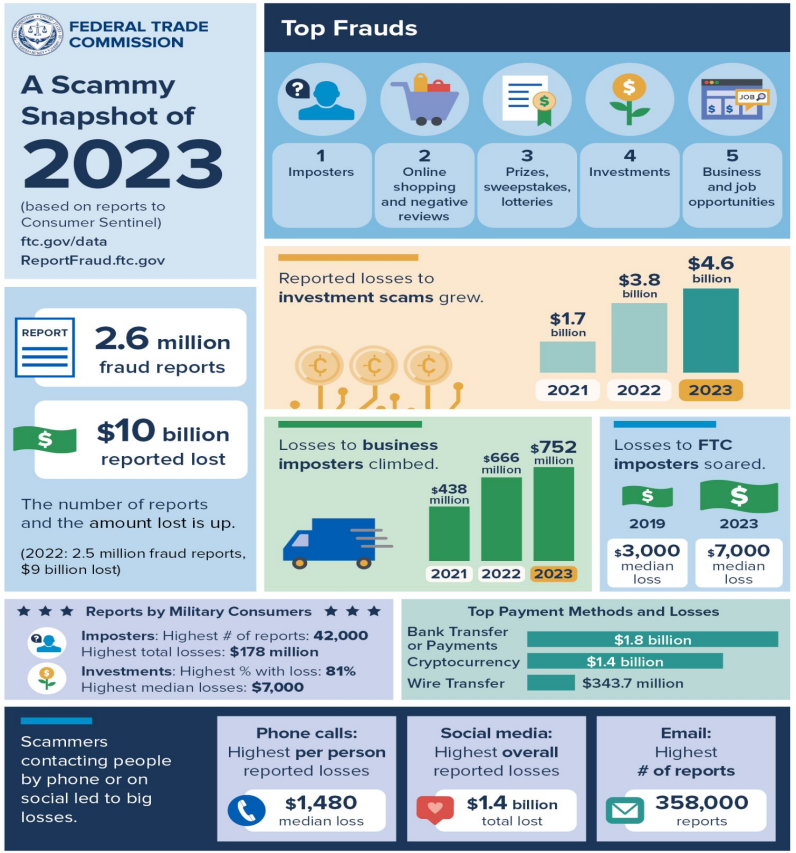
It is frequently difficult for current laws to handle the intricate details of bogus identities. For instance:

- **Jurisdiction Issues**: Since many cybercrimes using false identities cross national boundaries, enforcement is made more difficult.

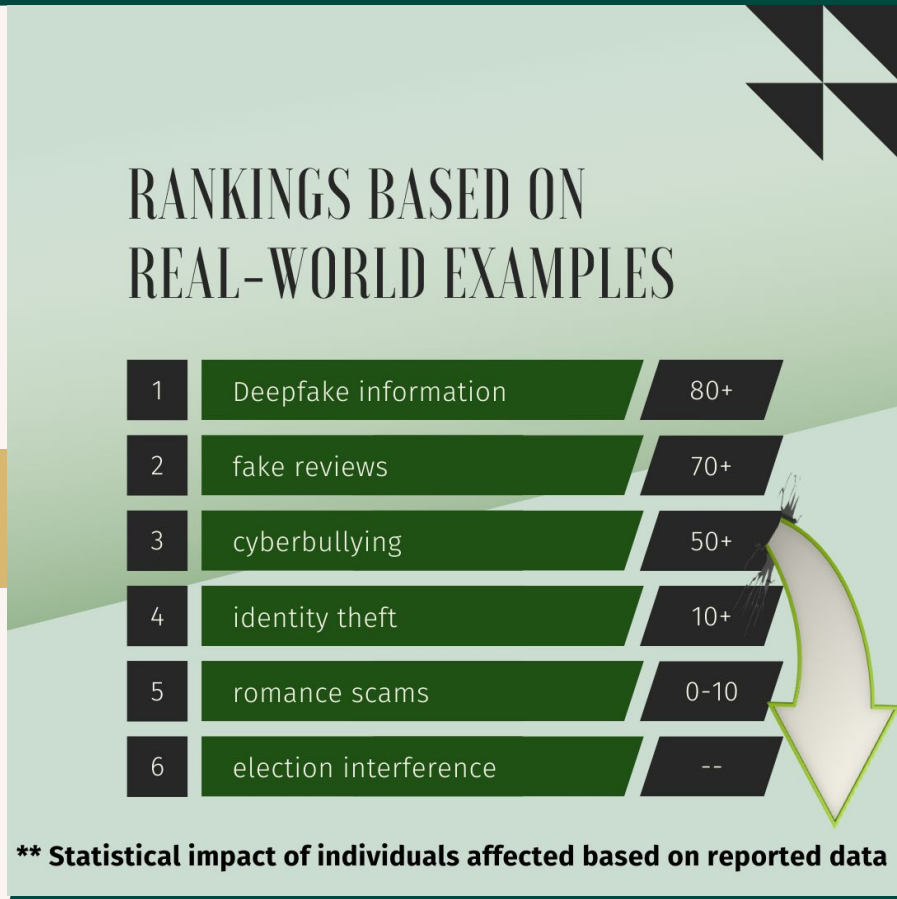
- **Outdated Law**: New technologies like deepfakes and artificial media may not be completely covered by current laws.

- **Lack of Standardization**: Cybercriminals take advantage of gaps created by the absence of consistent international regulations.

For example, although the United States has laws against fraud and identity theft, they are frequently reactive rather than proactive. Due to the relative anonymity with which malicious individuals might operate, inadequate regulation complicates the issue. The attached image has been pulled from the FTC Reports on fraud and identity incidents throughout 2023.



Statistics and Real-World Examples



References (Slide 7 Only)

Atske, S., & Atske, S. (2024, August 12). *Teens and Cyberbullying 2022*. Pew Research Center. https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

Consumer Sentinel Network Data Book 2022. (2024, February 13). Federal Trade Commission. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022

Paget, S. (2024, July 12). *Local Consumer Review Survey 2024: Trends, Behaviors, and platforms Explored*. BrightLocal. https://www.brightlocal.com/research/local-consumer-review-survey/

Publications | Intelligence Committee. (n.d.). https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

Shao, G. (2020, January 17). *Fake videos could be the next big problem in the 2020 elections*. CNBC. https://www.cnbc.com/2019/10/15/deepfakes-could-be-problem-for-the-2020-election.html?&qsearchterm=deepfake%20politics

Why This is a Social Issue

Beyond individual victims, this problem affects society as a whole by destroying trust, increasing inequality, and making it difficult for people to tell fact from fiction. This represents deeper worries about the ethical implementation of technology, the balance between privacy and responsibility, and the purpose of regulation in a quickly changing digital environment. The subject will require a team effort to solve the issue, including improved technological protections, updated legislation, and public education on digital literacy and awareness.

Knowing how fake identities affect society helps us to see how urgent it is to address this problem in a world that is becoming more interconnected by the day.

Overview

These three proposed solutions, along with their advantages, disadvantages, and practical considerations, aim to address the societal problem of fake online personas.

Possible Solutions to the Problem of Fake Personas in Cyberspace

Implementing Stricter Identity Verification on Platforms

Strengths:

- **Profile Integrity:** By requiring identity verification, attackers would be stopped from making various or fake profiles.
- **Transparency:** Since users are less motivated to commit crimes when they can be tracked down, real identities deter negative actions.
- **Increased Trust:** Users who have their identities verified feel more dependable and secure.

Weaknesses:

- **Privacy Worries:** Storage of PI or PII may result in abuse or poor safeguards that risk user privacy.
- **Withholding:** Those in remote areas that may not have access to major networks might inadvertently be left out of this answer.
- **Execution cost:** Setting up and running safe verification methods might call for companies to pay higher operating fees.

Challenges:

Experts stress that balancing user privacy and security is crucial, but global standardization of fake personas is difficult because of laws and regulations and various legal frameworks.

Strengthening Cybercrime Legislation and Enforcement

COMPARE & CONTRAST

Enhancing Cybercrime Legislation

STRENGTHS

- **JUDICIAL PREVENTION:** CYBERCRIMINALS ARE STRONGLY INTIMIDATED BY STRONGER REGULATIONS AND PROSECUTION.
- **INTERNATIONAL COORDINATION:** COOPERATION CAN BE IMPROVED AND TERRITORIAL DISPUTES CAN BE RESOLVED BY ALIGNING NATIONAL LAWS.
- **ADAPTABILITY:** LAWS CAN KEEP UP WITH CHANGING TECHNOLOGY IF REVISED REGULARLY.

CHALLENGES

EXPERTS RECOGNIZE THE IMPORTANCE OF INTERNATIONAL COLLABORATION BUT CRITICIZE MEASURES THAT MIGHT LIMIT FREE SPEECH OR TARGET ACTIVISTS AND WHISTLEBLOWERS BASED ON DIFFERENT RESOURCES AND GOALS.

WEAKNESSES

- **DIFFICULT ENFORCEMENT:** CYBERCRIMINALS ARE STRONGLY INTIMIDATED BY STRONGER REGULATIONS AND PROSECUTION.
- **OVERREACHING:** INCONSISTENT POLICIES MAY INSTEAD HARM THOSE WHO ONLY TRY TO MAINTAIN THEIR PRIVACY OR MAKE LIGHTHEARTED JOKES.
- **DELAYED LEGAL ACTS:** GAPS OCCUR WHEN LEGISLATION OFTEN FALLS BEHIND TECHNOLOGICAL ADVANCES.

Promoting Digital Literacy and Public Awareness

Strengths:

Initiatives for public awareness are adaptable and affordable, allowing customers to stay ahead of fraud and account misuse. In addition, they offer flexibility, enabling quick responses to new threats.

Weaknesses:

The difficulties in raising public awareness include a narrow audience reach, behavioral issues, and the lengthy process, which can be difficult for some demographics, such as senior citizens and people without reliable internet access.

Challenges:

Campaigns for public awareness should be accessible and engaging with the goal to have a big impact; this calls for engagement with private businesses, nonprofit organizations, and schools.

Conclusion

The rise of fake online personalities in the form of bots, catfishing and other forms poses a serious and multifaceted problem to individuals and to society overall. From personal impacts such as harm to a person's reputation, finances and emotional health to more broad impacts such as loss of trust in government institutions and weakened public confidence in technology, the dangers of fraudulent online personalities are very real and far reaching. While anonymity promotes individual privacy and fosters freedom of speech it also allows an entry point for bad actors looking to exploit vulnerabilities for monetary and ideological motives. As we have seen with the 2016, 2020 and 2024 U.S presidential elections and many other elections worldwide in the last several decades the ability to alter public opinion is now possible by malicious bad actors which puts democracy itself under threat. It will take a collective effort from all stakeholders worldwide to combine technology, law and policy and education to ensure that we all do our best to combat fake online personalities, hold those criminals who commit these crimes accountable and restore trust in the modern hyper connected digital world.

References

As nationwide fraud losses top $10 billion in 2023, FTC steps up efforts to protect the public. (2024, August 20). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

Greenberg, A. (2017, June 9). How Russia hacks elections in the US and around the world. *WIRED*. https://www.wired.com/story/russia-election-hacking-playbook/

Home - Canva. (n.d.). Canva. https://www.canva.com/

**Additional References listed on Slide 8

Thank You

Class Name

Student Name