Does Privacy On Social Media Exist?

The Newest Threat of Deepfakes to Internet Privacy

Marist College
Honors Program
Nina Squicciarini
Dr. Wenjing Xie

Abstract

The newest threat to Internet privacy is the artificial intelligence (AI) program, Deepfakes. This program uses a collection of images to create fake videos of people. In this study, an online experiment was created with four conditions of varying proximity and efficacy involving the threat of Deepfakes. A total of 203 students at Marist College participated in it. The majority had never heard of this AI program. The participants plan to change their future behavior by restricting certain information they post on social media and limiting the people who follow their accounts. Many felt that Deepfakes are a distant threat and were unsure of how it could impact them. Currently, people value the instant gratification of social media over their own privacy on the Internet.

Literature Review

Deepfakes: This program has continued to develop in China and is being used for entertainment. All it takes is a few selfies with different facial expressions.

Social Cognitive Theory: This theory involves the influence that social support and information has on behavioral change. Self-efficacy impacted the changes people were willing to make in their lives.

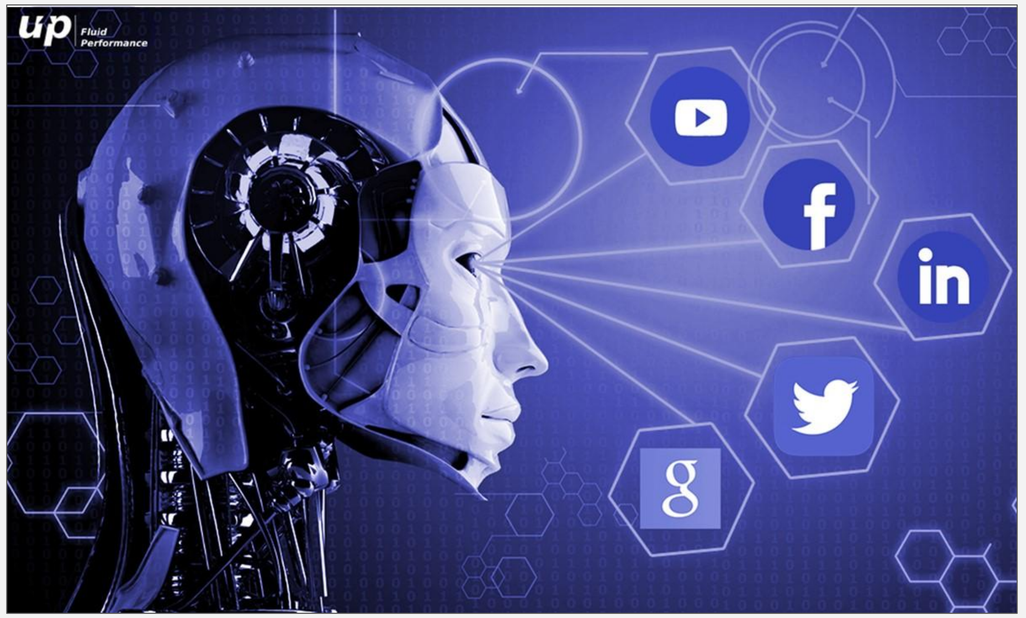
Construal Level Theory: This theory has been used in research about climate and other long term threats such as smoking. The impact that psychological distance has on people's action was analyzed in this study about the risks caused by Deepfakes.

Privacy Protection on Social Media: Social media user's do not have control over what other people post of them and this make it very difficult to truly be private on the Internet. Even if posts are deleted, that information remains on the Internet forever.

Research Questions

1. Do the benefits of social media outweigh the privacy risks?

2. Does proximity and efficacy influence how people view the threat of Deepfakes?



Method

Design
- ❏ An online experiment with four conditions
- ❏ Likert Scale

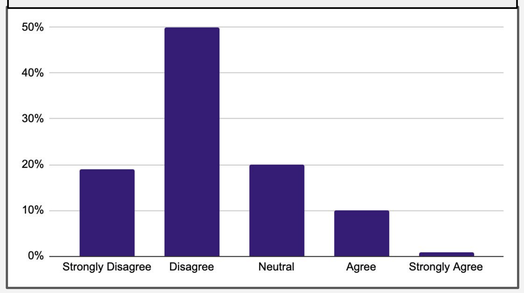
Condition 1: **High Proximity & High Efficacy**
Condition 2: **High Proximity & Low Efficacy**
Condition 3: **Low Proximity & High Efficacy**
Condition 4: **Low Proximity & Low Efficacy**

Sampling
- ❏ 203 respondents
- ❏ 50 per condition
- ❏ Marist Students (18-22)
- ❏ Systematic and Convenience Sampling

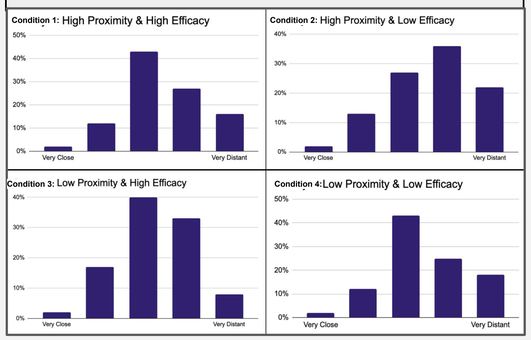
Procedure
- ❏ Online Survey
- ❏ 10 minutes in length
- ❏ Survey was divided into two pages
  - Page 1: General questions about social media usage (independent variables)
  - Page 2: Questions about Deepfakes and behavioral changes (dependent variables)

Results

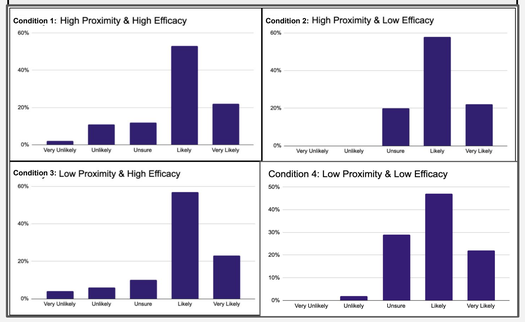
I can count on social media companies such as Facebook or Instagram to protect customers' personal information from unauthorized use.



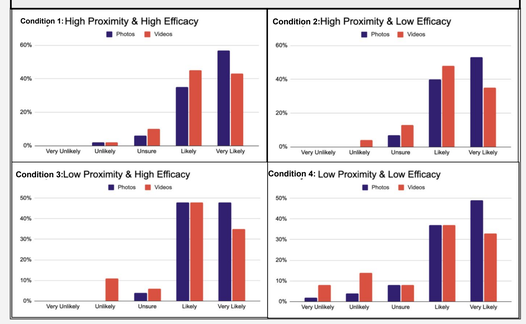
To me, the threat caused by Deepfakes feels...



Restrict the types of information that you share with apps on social media.



How likely are you to post photos/videos on social media in the future?



Discussion

No trust for social media - Respondents do not trust Facebook or Instagram to protect their information. Respondents are aware that their information is being sold to third party software programs.

Unaware of Deepfakes - The majority of respondents have never heard of the program Deepfakes. If college educated students were unaware of this new AI program, then it can be assumed that the general public is also unaware of this new threat.

Proximity & Efficacy - Proximity did not have a huge influence on respondents' decisions regarding Deepfakes. Respondents with the low efficacy condition were more unsure about how they felt towards this new AI threat.

Behavioral change - Respondents plan to unfollow/unfriend certain people from their social media pages and delete some of their existing post. Many agreed they would restrict types of information they share.

Benefits outweigh the risks - College students will continue to post photos and videos on social media.