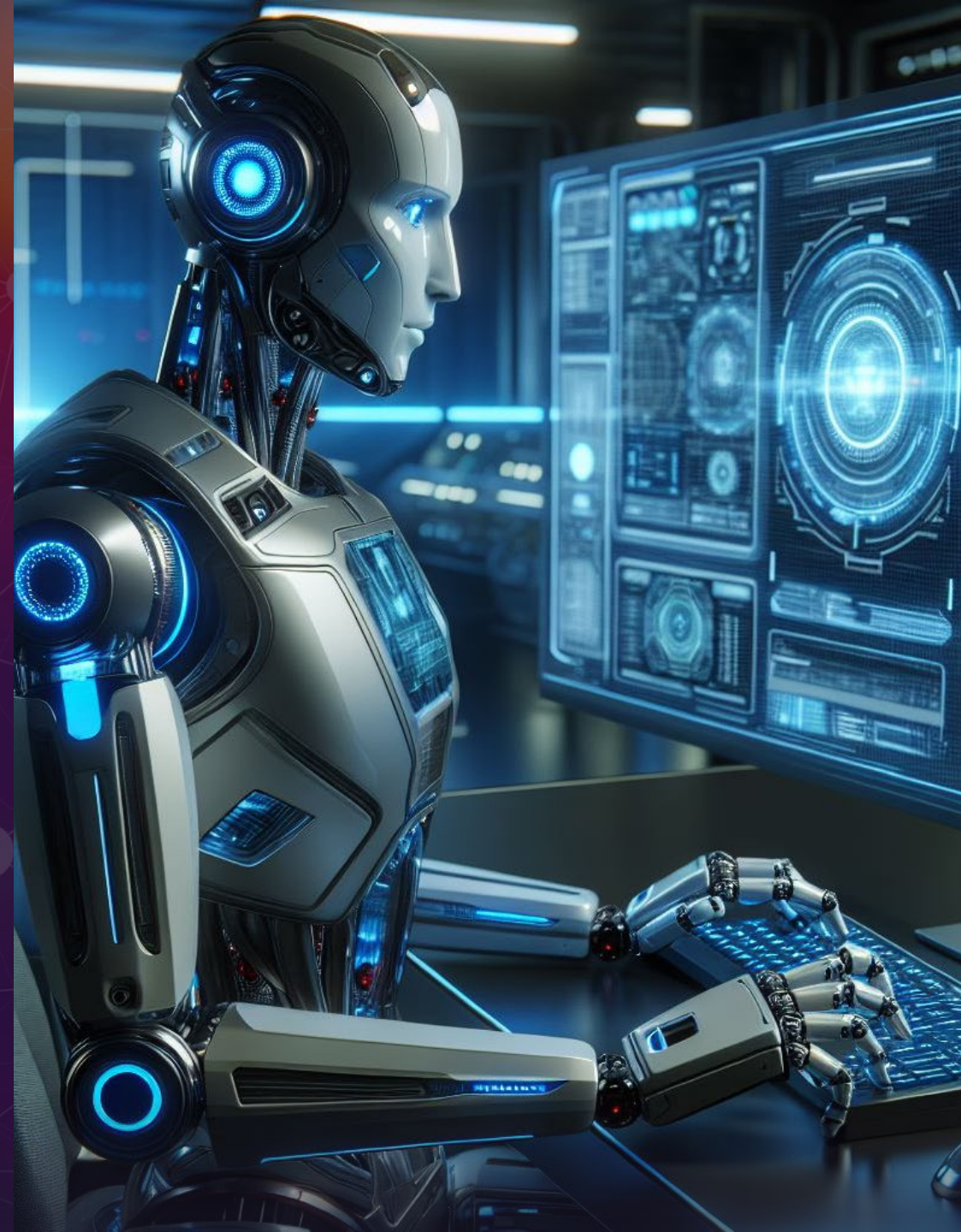


# Robots in Disguise

Marie Dilan

Senior Committee Administrator  
mdilan@uga.edu



# Disclaimer



The content of this presentation is from the PRIM&R Conference that I have attended in Seattle, WA (November 17-20, 2024). A written permission from the presenters has been sought for purposes of sharing this training session to the committee during education/training portion of the IRB Meeting.





## Definitions:

**Bot (short for “robot”)** – is an automated software program designed to perform tasks on the internet without human intervention. They can be good or bad actors and deciphering this label can pose challenges.

**Bot Incident** – refers to any event in which a bot disrupts the integrity of a research study.

e.g.,

- Unauthorized data collection
- Responses manipulation
- Other actions that can compromise research validity

# Background Information

Artificial intelligence (AI) development continues to make bots more sophisticated. It increases ability for bots to have human-like qualities/responses.

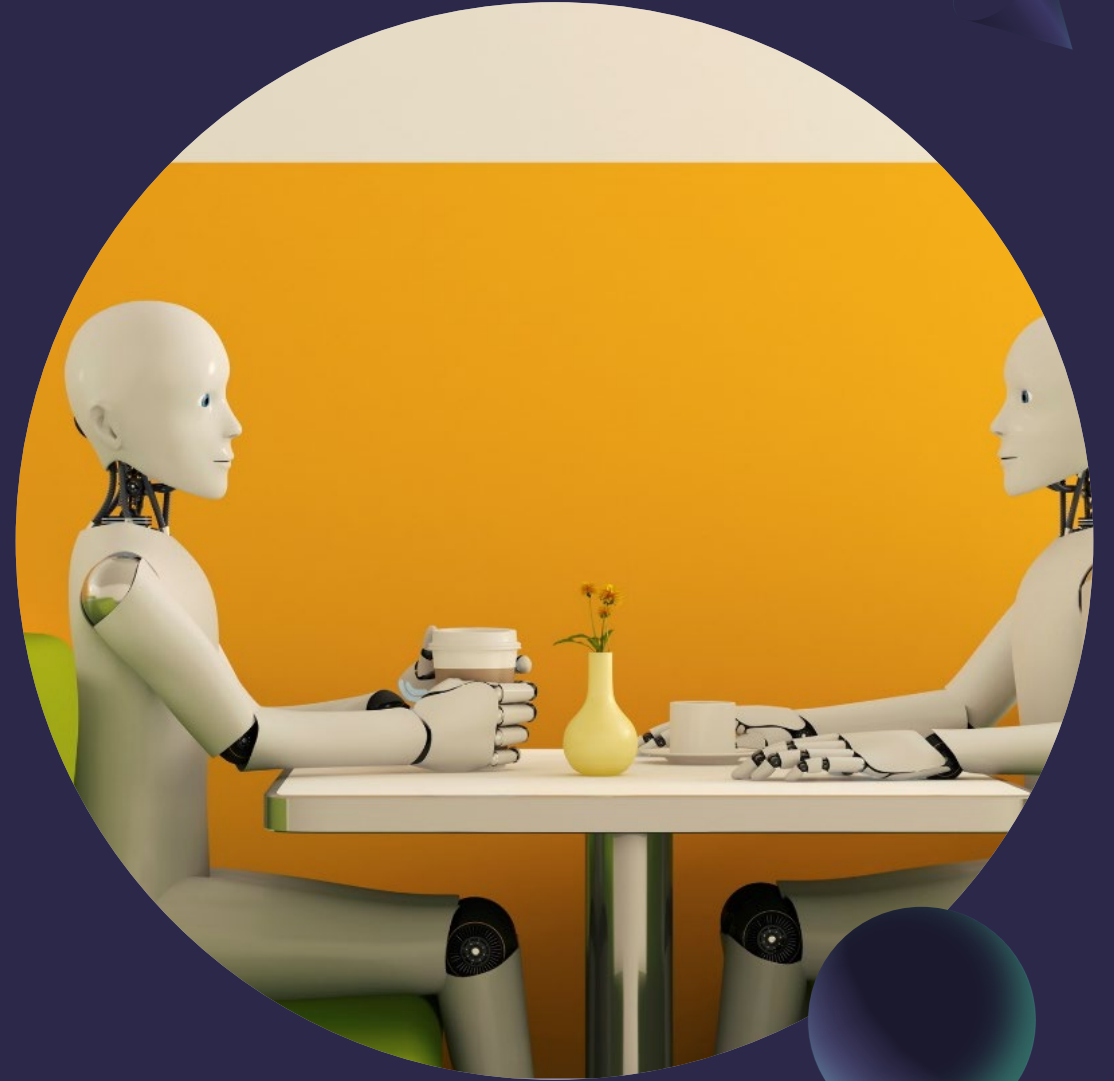
Online survey research design is more prone to this risk. Hence, researchers should be highly cautious when posting data online as this can impact study participants' eligibility, data integrity and overall research validity.

## Some risks:

- Suspicious-looking data can be bot generated
- Responses can be automated (click boxes or Likert scales)

Knowing the difference between an eligible human subject and the bot is important

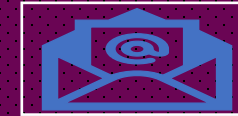
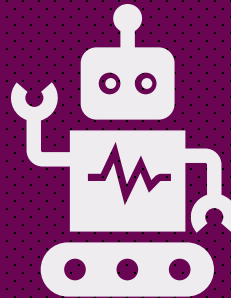
# Sample Cases



# Case #1: A Study on LGBTQ+ Mental Health & COVID-19-Related Issues

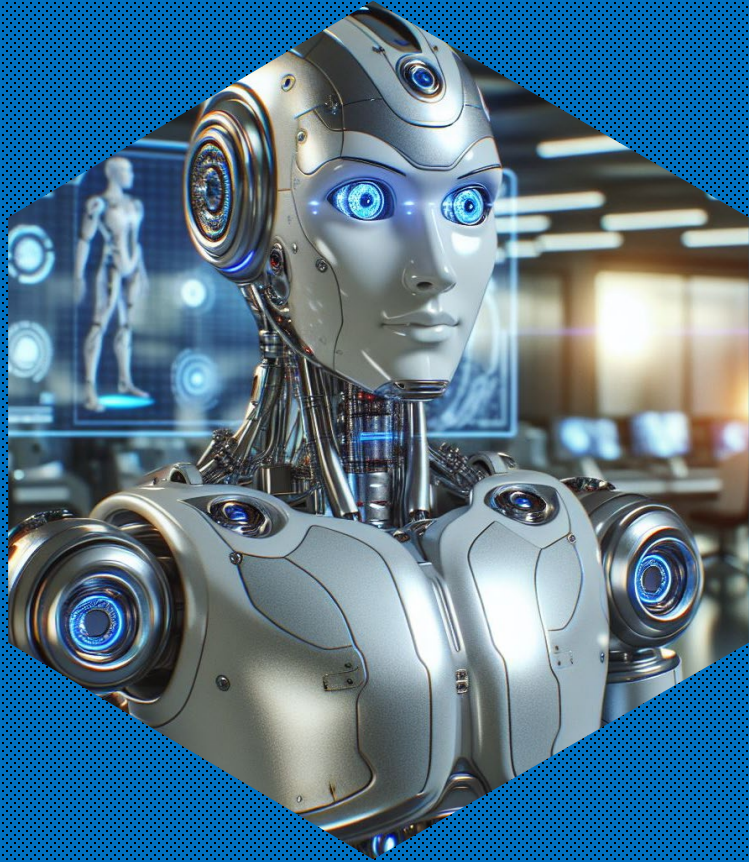


The researcher has described a situation in which bots infiltrated an online survey conducted as part of the study. The study was hosted on the Qualtrics platform and used a \$5 gift card incentive to attract participants. The survey was designed to collect data on various issues affecting the LGBTQ+ population, particularly in relation to COVID-19. To reduce direct human interaction, the survey was set up to allow for automated responses.



However, bots began to infiltrate the survey, filling out the form repeatedly using fake email addresses and completing the entire survey. This led to the expenditure of \$1,500 in gift cards overnight, as the bots systematically "claimed" the gift cards meant for actual eligible human participants. Once the infiltration was discovered, the researcher urgently communicated with the IRB, and a modification to the incentive model was made, replacing the gift card system with a raffle-based model to reduce the attraction for automated bots.

# Case #2:



Residences in a specific city were invited via mail to participate in an online survey and would receive a \$25 gift card. The letter provided a link to the survey along with a unique PIN for each recipient to access their survey. Once inside the survey, participants were prompted to create a password.

A respondent, likely motivated by the incentive, programmed a bot to replicate the PIN pattern and generate guesses to gain repeated access to the survey. This bot systematically bypassed the access controls, leading to significant financial losses, amounting to over \$10,000 due to repeated redemption of incentives. The bot also had the potential to access surveys for respondents who had already started taking the survey by phone and therefore not set up a password.

The study data was not live-monitored and there was not language in the consent form precluding collecting multiple incentives. The individual who created the bot subsequently reached out to the study team to inquire why they were no longer receiving incentives after completing the surveys.



## Case #3: An Online Survey Recruiting Postpartum Women

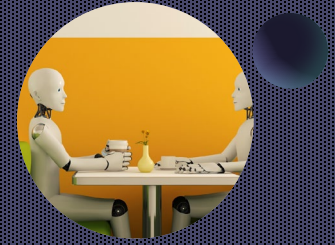
The study involved an online survey with compensation, and participants, who were postpartum mothers, completed the survey at various times. Some responses were flagged for suspicious activity.

The study was partially monitored live for issues like duplicate responses or inconsistent data patterns, leading to the rejection of certain responses due to suspected fraudulent activity, potentially involving bots or ineligible human respondents. Several rejected participants, whose emails suggested a coordinated effort, contacted the researcher to inquire about their ineligibility. The researcher was concerned about how much information to share with these individuals, fearing that bot creators might use this knowledge to enhance their algorithms and evade detection.

The General Counsel also highlighted potential vulnerabilities in the study design, including the risk of bots accessing the survey and the robustness of participant selection methods to prevent such infiltration. Furthermore, concerns were raised about the design and effectiveness of attention checks (e.g., photo-based CAPTCHA tests), as bots can sometimes bypass these measures.



# Key Issues and Questions



- Who is responsible for bot infiltration? Is it the researcher, the IRB, the institution or the platform (e.g., Qualtrics) or any survey plugins used (e.g., Tango)?
- How can the IRB improve its review processes for online studies?
- How will one address participant concerns and disputes? Could one provide general reasons for rejection (e.g., “inconsistent data” or “possible fraud detection”) without disclosing too much information that might help a bot operator refine their algorithms?
- What safeguards should be put in place to ensure that the rejection of responses based on suspicious activity does not unfairly impact participants?
- What tools does an online survey platform offer to detect bot activity?
- Were there any platform terms of service or guidelines that discussed bot? Was these violated by the bot activity? How did the platform respond to this?
- What measures were implemented to mitigate bot responses? (e.g., CAPTCHA, IP filtering, or other bot prevention tools)
- How was the incentive distribution tracked? Were there any fraud detection mechanisms to monitor for suspicious patterns? (e.g., multiple redemptions from the same IP address or unusual access attempts)
- How were participants notified about the incentive program? What procedures were in place to ensure that only eligible participants received incentives?

# Ethical and Practical Considerations

## Review and Enhance Security Protocols:

- Consent form - clearly state that compensation might be withheld in the event of suspected fraudulent activity.
- What level of liability does the institution hold if platform allow security lapses that compromise the integrity of the study?

## Compensation and Fairness:

- IRB should consider ethical guidelines when designing compensation policies for studies with potential for fraudulent data
- Ensure that compensation is withheld fairly and transparently, especially when bots are involved

# Ethical and Practical Considerations (cont.)

## Collaboration with Researchers and Other Stakeholders:

- IRBs may consider compassionate communication to encourage fearless engagement from study teams. Instances of bot infiltration can be unsettling and may disturb researchers (or the research community).
- Engage with institutional offices:
  - a) Office of Sponsored Research – for grants and funding
  - b) IT Office – for system security
  - c) Experts in data analysis, AI, and behavioral science – for refining methods for detecting and preventing fraudulent responses and ensure that validation metrics are effective

## Training and Awareness:

- Researchers may need to undergo additional training on data security and fraud prevention, particularly as it relates to online studies with incentive structures. This could be part of a broader effort to integrate cybersecurity best practices within the IRB's review process.



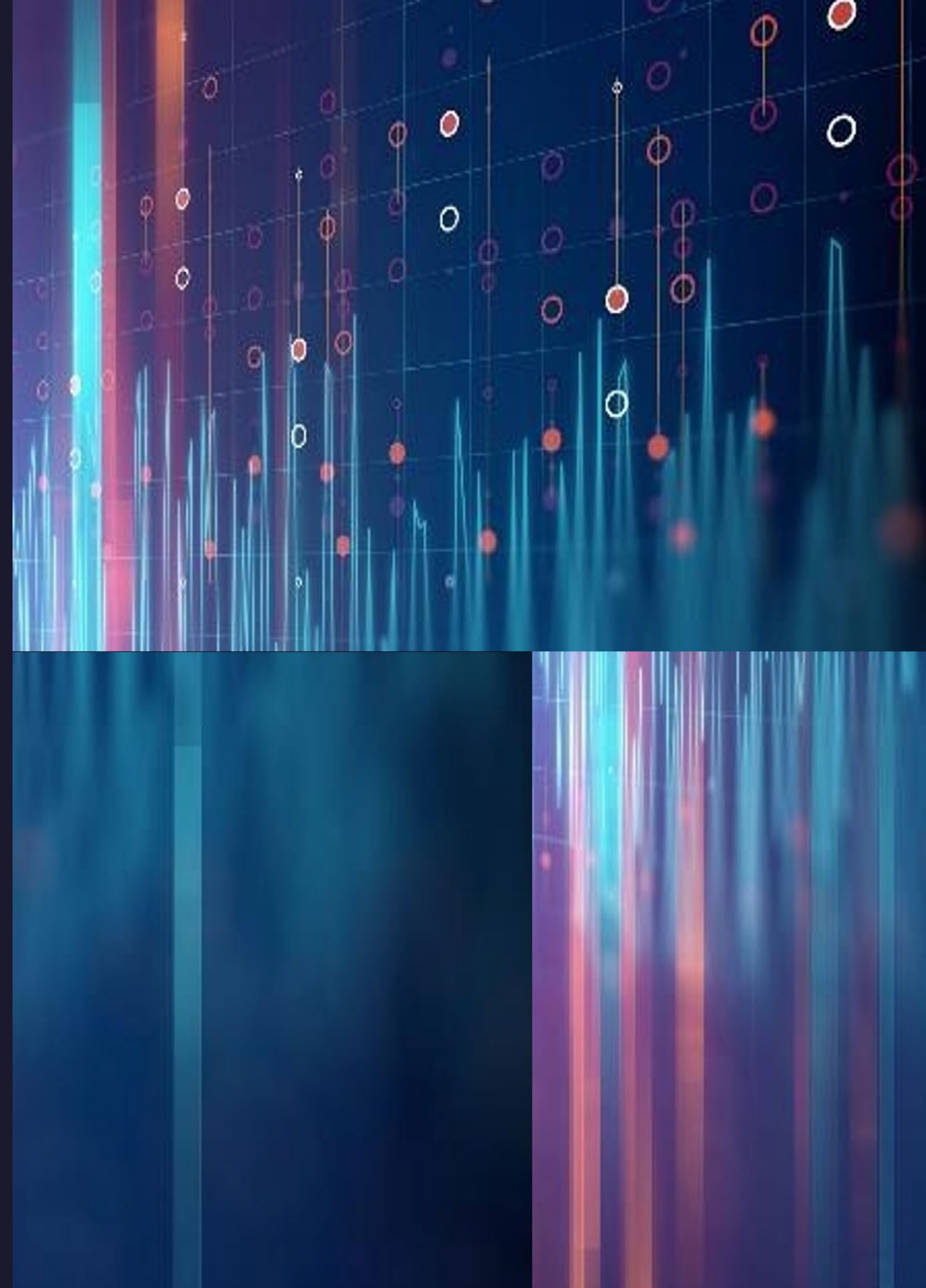
# Communication & Reporting

## IRB & the Institution:

- Establish a clearer communication channel for urgent modifications like this in future studies. Challenge: IRB may not know how to respond to a bot infiltration or compliance scope is outside of its purview.

## General Counsel:

- Review any contractual or legal implications on participant's data security and research integrity.
- Consider the legal implications and the need for transparency when rejecting participants.
- Provide guidance on liability issues and advise on how much information can be shared with rejected participants without compromising the integrity of the study.
- Help confirm whether legal action can be pursued against the bot creator.



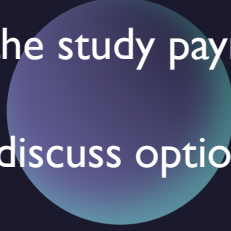
# Communication & Reporting



## IT Department/Data Security:

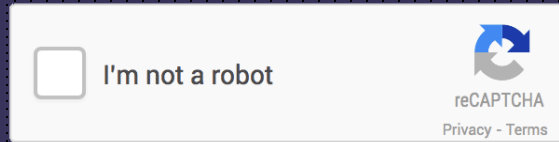
- Determine if there are any platform vulnerabilities that need to be addressed.
- Assess if sensitive participant data (e.g., email addresses) was compromised in any way by the bots.
- Review of the researchers' procedures and safeguards against bots should be conducted promptly, particularly if the study is open to respondents.

## Finance Office:

- Explore the financial impact of the bot infiltration and the effectiveness of the study payment or raffle model as a replacement.
  - To discuss options for halting payment or recouping funds, if possible.
- 



# Proactive Measures



Utilizing CAPTCHA (challenge-response test) and other verification tools to prevent automated submission



Data validation procedures



Data security training and best practices for preventing bot interference

In the initial IRB submission and Consent Form, Potential Risk –

- Researchers can acknowledge the possibility of bot interference.
- Outline how bots could impact the study (e.g., skewing data, generating false responses, influencing recruitment processes) and how this might harm the research integrity.



"Given the increasing sophistication of automated agents, this study will employ methods to detect and mitigate bot responses, though we acknowledge that the effectiveness of these methods is not absolute."





# Acknowledgment of PRIM&R Presenters

- Dr. Karen Stein, Principal Methodologist, Abt Global
- Dr. Myra Luna Lucero, Research Compliance Director, Teachers College, Columbia University
- Dr. Kristen D. Krause, Assistant Professor, School of Public Health, Rutgers University

**Thank you!**

