This template MUST be used for new Social Behavioral studies submitted in eIRB+ on or after November 1, 2024.

This protocol must be completed for human participant research studies **unless your study will ONLY involve secondary data and/or specimen analysis** (use the **Data and Specimen Analysis Protocol (HRP-1704)** for secondary data analysis/specimen analysis studies). Use this protocol template whether your study will be determined to be exempt or approved via other IRB review procedures (investigators do not make their own determination as to whether a research study qualifies for an exemption -- the IRB issues exemption determinations). **If you are unsure whether your project is human research requiring IRB review**, complete and submit the **Human Research Determination Form (HRP-503)** instead of this document.

It will be helpful to your submission to understand the type of review you are requesting. Further resources can be found on the Northwestern IRB website: **Types of Review** OR **Department of Health and Human Services (DHHS) Decision Trees.** DHHS has provided numerous decision trees regarding whether an activity meets the definition of human subjects research; whether research is eligible for a Claim of Exemption, and whether research can be reviewed via expedited review.

NOTE: Your consent documents, data collection instruments (surveys, questionnaires, interview guides, etc.), and recruitment materials need to be uploaded in eIRB+ in the consent, recruitment, and supporting documents sections of the application and should NOT be attached or incorporated into this protocol document. For any supporting documents you upload, please use filenames for the documents that make clear what type of document you are uploading. If your study will include multiple phases, please make sure the filename is clear as to which phase of the study the document is related to.

TIPS ON COMPLETING THE PROTOCOL FORM:

- If any sections are not applicable to your research, mark that section as N/A (for not applicable). Do not delete the section(s) from the protocol.
- Keep an electronic copy of your protocol. If you submit modifications to your study at a later time, you will need to include tracked changes to all affected study documents, including the protocol.
- As you write this protocol, remove the text boxes and all instructional text contained inside the text boxes in each section. There should be no text boxes or instructional text (including these instructions) in the final version of your protocol.
- If you plan to access **HIPAA Protected Health Information (PHI) from medical records** for recruitment and eligibility screening purposes and/or to analyze as research data, you must fill out and upload **Social and Behavioral Protocol Template Appendix B (HRP-1724)** in addition to this protocol document.

STUDY TITLE:

Leveraging LLMs to protect users against target password guessing

PRINCIPAL INVESTIGATOR:

Name: N/A
Department sponsoring/supporting the study: N/A
Telephone Number: N/A
Email Address: N/A

NOTE: Per Northwestern University policy, undergraduate and graduate students are not allowed to be the Principal Investigator on a research study. Visiting faculty, visiting scholars, postdoctoral fellows, and medical residents are not eligible to serve as Principal Investigator on a research study unless they obtain special permission. For further information on who is eligible to serve as a Principal Investigator, see https://irb.northwestern.edu/submitting-to-the-irb/initial-studies/principal-investigator-eligibility-and-permissions.html

CO-INVESTIGATORS:

Name: N/A
Department: N/A

NOTE: students should **not** be listed as co-investigators

STUDENT INVESTIGATOR (complete this section only if the project is student-initiated):

Name: Manaswi Raj
Department: Computer Science and Engineering

Are you an:

- ☑ Undergraduate Student
- ☐ Graduate Student or Medical Student

Name: Harsh Sharma
Department: Computer Science and Engineering

Are you an:

- ☑ Undergraduate Student
- ☐ Graduate Student or Medical Student

Name: Vibhor Dave
Department: Electronics and Electrical Engineering

Are you an:

- ☑ Undergraduate Student
- ☐ Graduate Student or Medical Student

VERSION DATE:

10-11-2024

FEDERAL FUNDING:

(Complete the following matrix if this study will be supported by federal funds. Add additional matrices for each unique funding source. Remove this section if the study will not be supported by federal funds. Reminder: This information must match the information you provide on the funding page of the eIRB+ application.)

Funding Agency:	N/A	
Sponsored Research ID#:	N/A	
Does the grant indicate that covered activities will include Human Research? (Yes / No / Unknown)	N/A	
	Institution Name:	Human Research Assessment *** (e.g., Non-Exempt Human Research, Exempt Human Research, Not Human Research, etc.)
Prime Award Recipient*	N/A	
Sub-Award Recipients**	N/A	

* The prime award recipient is always engaged in Human Research and must have IRB oversight when one or more sub-award recipients conduct non-exempt Human Research.
Many federal agencies require that when more than one domestic site engages in non-exempt Human Research, all sites must rely on the review of one "Single IRB." If this applies to your study, you must obtain a Single IRB Letter of Support and IRB Fee Quote from the Northwestern University IRB Office before the Northwestern University IRB will review your study. Submit a Single IRB Consultation Intake Form to initiate this process.

***Include the activities of all non-Northwestern affiliated sites in the multi-site/collaborative research section of the protocol below.*

****The federal funding application should include plans for whether award recipients will engage in Human Research. Based on the funding application, provide an assessment of the activities at each site and update the table if the planned activities change or if another IRB reviews the activities and makes a different determination.*

RELATED STUDIES:
N/A

Check any **applicable** boxes in the table below – you will be asked for further detail on these topics later in the protocol form:

Indicate Vulnerable Populations to be enrolled: ☐ Children ☑ Adults with Impaired Decision-making Capacity ☐ Pregnant Persons(IF the research activities will affect the pregnancy or the fetus) ☐ Prisoners (or other detained/paroled individuals)
☑ International Research (check this box if you will collect data from individuals located outside the United States)
☐ Research involving external collaborators (some research activities will be carried out by individuals not employed by Northwestern or NU affiliates will carry out some research activities)
☐ Research has U.S. Federal government funding via one or more direct awards or a sub-award (e.g., NIH, NSF, other federal agencies or departments)
☐ HIPAA-protected data (please use Social and Behavioral Protocol Template Appendix B: HRP-1724) ☐ FERPA-protected data (guidance found on WORKSHEET - FERPA Compliance (HRP-331)

1.0 Purpose and rationale of the study:

The purpose of this study is to assess the effectiveness of passwords generated by Large Language Models (LLMs) compared to those created by users, specifically in terms of their resistance to targeted password guessing attacks. With the advent of increasingly sophisticated password guessing algorithms, such as those based on machine learning and user behavioral data, traditional password creation practices are becoming less effective at protecting users against unauthorized access.

In this study, we will investigate whether LLMs, particularly when fine-tuned to avoid common user tendencies (such as predictable patterns, frequently used words, or common substitutions), can produce passwords that are inherently more resistant to these targeted guessing attempts. This research seeks to contribute to the field of cybersecurity by evaluating whether LLMs can be used as a tool to generate robust passwords that offer enhanced protection for users.

The rationale behind this research is grounded in the growing need for stronger authentication mechanisms. With the expansion of online services, password-based

authentication remains a primary security measure, yet it is frequently compromised due to weak or predictable passwords. By leveraging LLMs in password creation, we hypothesize that it may be possible to produce passwords that strike a balance between complexity and memorability, without relying on patterns that attackers commonly exploit. If successful, this approach could offer practical guidelines for enhancing password security and safeguarding user accounts in an increasingly digital world.

2.0 Enrollment Criteria (who can be in your study and who would not be eligible to participate in your study):

In this study, we plan to include participants who meet the following inclusion criteria:

- **Age**: Adults aged 18 and above.
- **Language**: Participants must be fluent in English, as the study materials and instructions will be provided in English.
- **Computer and Internet Use**: Participants should be regular users of computers and the internet, with familiarity in creating and using passwords.

Exclusion Criteria:

- **Minors**: Individuals under the age of 18 will not be included in this study.
- **Vulnerable Populations**: We will exclude populations that may require additional protections or considerations, including:
- Adults unable to consent or with impaired decision-making capacity
- Pregnant persons, as this study does not pertain to pregnancy but may involve slight emotional stress due to security concerns
- Prisoners or detained individuals, due to the sensitive nature of password security
- Non-English-speaking participants, as language barriers may impact understanding of the study instructions.

No vulnerable populations, as defined by the IRB criteria, will be enrolled in this study. This study is designed to evaluate password security without involving populations who may be at greater risk or have difficulty providing informed consent.

3.0 Sample Size:

For this study, we plan to recruit a sample of 100–150 participants. This sample size is based on the following considerations:

- **Feasibility**: Recruiting 100–150 participants is feasible within our timeframe and resources.
- **Statistical Relevance**: This sample size is adequate to detect meaningful differences in password guessability between user-generated and LLM-generated passwords.
- **Attrition Allowance**: We expect that some participants may withdraw or not complete the study, so recruiting up to 150 participants allows for a small margin of attrition while ensuring that at least 100 participants' data are available for final analysis.

This sample size is designed to provide a balance between achieving statistically significant results and managing the study's logistical constraints.

4.0 Recruitment and Screening Methods:

We plan to recruit a sample of 100–150 participants. To ensure diversity and inclusivity, we aim to recruit individuals across various racial, ethnic, and socio-economic backgrounds to obtain a sample representative of the larger population.

- **Recruitment Platforms**: Recruitment will primarily occur through online platforms, including social media (such as Facebook and LinkedIn), university mailing lists, and forums related to cybersecurity, password security, and general technology interest groups. Prior to posting recruitment information, we will review and obtain any necessary approvals from platform administrators.
- **Diversity Focus**: To address diversity in our recruitment process, we will tailor our outreach to reach underrepresented racial and ethnic groups by targeting relevant online communities and forums. For example, we will post in groups that specifically focus on cybersecurity and tech for underrepresented groups, as well as general tech and student communities.

2. Steps to Locate and Contact Eligible Individuals:

- **Location and Eligibility Screening**: We will initially contact potential participants through recruitment postings on approved platforms and mailing lists. Each recruitment posting will include a link to a brief online screening survey. This screening survey will assess eligibility criteria, such as age (18 and over), language proficiency (English fluency), and familiarity with computer and internet use.
- **Contact Process**: When a user clicks on the recruitment link, they will be directed to an online eligibility questionnaire hosted on a secure survey platform.
- **Timing**: Recruitment materials will be posted on social media and relevant online platforms during specific periods to maximize engagement. Posts will remain active for approximately four weeks or until the target sample size is reached.

3. Screening Process:

- **Screening Method**: Eligibility screening will be conducted via an online questionnaire. The questionnaire will include questions about the participant's age, language proficiency, and familiarity with computer and internet usage to confirm that they meet the inclusion criteria.
- **Privacy and Data Handling**: Only eligibility data will be collected in this survey, and we will inform participants that their responses will be kept confidential. Participants who meet the criteria and consent to participate will be contacted with further study details. For individuals who are ineligible or choose not to participate

after screening, their responses will not be used in any further analysis and will be securely deleted from our records.

- **Consent for Screening**: Since the screening questionnaire is used solely to assess eligibility, explicit consent to screen will be requested at the beginning of the survey.
- **Data Security**: Screening data for both eligible and ineligible individuals will be securely stored in compliance with university data protection policies, and any identifying information will be deleted promptly if the participant does not proceed to the main study.

Additional Information:

We will not include any vulnerable populations, as defined by the IRB, such as individuals under 18, pregnant individuals, prisoners, or adults with impaired decision-making capacity. Recruitment and eligibility screening processes are designed to ensure that only eligible adults participate while protecting the confidentiality and privacy of all responses.

5.0 Research Locations:

This study will be conducted **online**, allowing participants to complete all research activities remotely. We will use a secure, university-approved survey platform, such as **Qualtrics**, for data collection. This platform provides encryption and privacy features necessary to protect participant responses, and all data will be stored securely in accordance with institutional data protection standards.

Location and Access: Since the study is entirely online, participants can complete the study from any location with internet access. While our recruitment efforts will target U.S.-based platforms and mailing lists, there is a possibility that participants may reside outside the United States. However, we will clearly indicate that participation is limited to individuals within the U.S. through eligibility screening.

Approvals and Permissions: No in-person research locations are required for this study, and we do not require site permissions from institutions or organizations. Before implementing the study, we will ensure that all necessary university and IRB approvals are in place.

If future modifications involve collecting data from additional sources or at specific physical locations, we will obtain the required approvals from those sites before conducting any research activities.

6.0 Multi-Site or Collaborative Research:

This project is a non-collaborative study, conducted solely by the research team at Indian Institute of Technology Kharagpur. All research activities, including study design, recruitment, data collection, and analysis, will be carried out independently by the IITKGP research team without partnership or involvement from other institutions, organizations, or external collaborators. Since the project does not require resources, data access, or assistance from outside entities, no formal collaborations or agreements are needed. All necessary approvals and oversight will be managed internally, ensuring compliance with Indian IITKGP's research policies and IRB requirements.

7.0 International Research (where data collection will occur outside the United States and U.S. territories, including online activities)

This study is designed to be conducted worldwide, with data collection open to participants from various countries. Although recruitment and data collection will be conducted online, the study will specify in the eligibility criteria that participants must meet specific requirements (e.g., age, language proficiency, internet access) regardless of location.

IRB and Research Ethics Committee Review: Since the study is worldwide in scope, review by IRBs or ethics committees in each country where data is collected may not be feasible. However, we will ensure compliance with local ethical guidelines wherever possible. In cases where a country requires review by a local ethics committee, we will take the necessary steps to obtain approval or provide documentation showing our good-faith efforts to consult with local experts and secure cooperation. The study will also comply with the research ethics standards set by the Indian Institute of Technology Kharagpur (IIT Kharagpur), where the research is led.

Sociocultural Factors Affecting Consent: The consent process will be tailored to account for sociocultural factors in different regions. For example, literacy levels, language barriers, or customs requiring consent from community or family leaders may influence how consent is obtained. The consent form and recruitment materials will be available in multiple languages as needed, and the study team will be prepared to provide additional support to participants where necessary.

Data Protection Laws: Given the global scope of this study, we will ensure compliance with relevant data protection laws in each country where participants are located. This includes but is not limited to:

- General Data Protection Regulation (GDPR) for participants located in the European Economic Area (EEA).
- Personal Information Protection Law (PIPL) for participants located in the People's Republic of China.

- Other local data protection regulations, such as India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, will also be followed for participants in India.

The study will comply with all relevant international and local data protection laws, including obtaining informed consent and ensuring participant data is securely handled and stored.

Data Security: All data will be collected through a secure, encrypted platform (e.g., Qualtrics or a similar platform), which complies with international data security standards. Data will be stored on university-approved servers that adhere to IIT Kharagpur's data protection policies. Sensitive data will not be stored on mobile devices or laptops to minimize risk.

Export Control Compliance: We will ensure compliance with U.S. and international export control regulations, including the Office of Foreign Assets Control (OFAC) guidelines and any country-specific restrictions. The study will avoid the inclusion of participants from embargoed or military-end-use countries such as Cuba, Iran, North Korea, and others under U.S. sanctions.

This approach ensures the study's compliance with the highest international standards of research ethics, data protection, and security, while also considering the cultural and legal requirements of each participating country.

8.0 Procedures Involved:

Please check the boxes for all applicable data collection procedures you plan to use:

- ☐ One-on-one interviews
- ☐ Focus Groups
- ☑ Questionnaires/surveys
- ☐ Secondary Data Analysis (medical record data, educational records, government or private sector datasets, etc.)*
- ☐ Ethnographic observation
- ☐ Physiological measurements (e.g., EEG, EKG, MRI)
- ☐ Biospecimen collection (saliva samples, blood draws, hair samples, etc.)
- ☐ Mobile applications/data collection devices (e.g., Fitbits, actigraphs, etc.)
- ☐ Behavioral decision making tasks (e.g., puzzles, interactive games, etc.)
- ☐ Physical activities such as walking and other forms of exercise
- ☐ Other procedures (briefly list types of procedures here if not covered by the check-boxes above): _____

Overview of Data Collection Process: The study will utilize an online questionnaire and survey method for data collection. Participants will be recruited through online platforms, and the survey will be administered using a secure survey platform (e.g.,

Qualtrics). The data collection process will be carried out in a single phase, with participants completing the survey remotely at their convenience.

Procedures:

1. **Recruitment**: Participants will be recruited through online channels, including social media, university mailing lists, and crowdsourcing platforms. Recruitment materials will provide details about the study, including eligibility criteria and the link to the survey.
2. **Informed Consent**: Upon clicking the survey link, participants will first be presented with an informed consent form. They will need to read and agree to the terms before proceeding with the survey. If they do not agree to the consent, they will not be able to participate.
3. **Survey Completion**: The survey will consist of demographic questions, followed by questions about password usage, creation habits, and a set of passwords that the participants have used in the past. The survey will be self-administered and will take approximately **15-20 minutes** to complete. Participants will also be asked to create a set of passwords that they typically use and provide an additional one for comparison.
4. **Data Storage and Security**: All responses will be securely stored on the Qualtrics platform, which adheres to IIT Kharagpur's data protection policies. The survey data will be anonymous, with no identifiable personal information collected from participants.

Timeline:

- **Week 1-2**: Recruitment and distribution of the survey. This phase will involve posting recruitment materials, sharing the survey link, and collecting responses.
- **Week 3-4**: Data collection from participants. During this phase, we will track survey responses and send reminders to ensure a representative sample is collected.
- **Week 4**: Final data collection and closure of the survey.
- **Week 5**: Data cleaning and preliminary analysis.

Duration of Participation:

- **Informed Consent**: Approximately 2-3 minutes.
- **Survey Completion**: Approximately 15-17 minutes.
- **Total Estimated Time**: Each participant will spend approximately **17-20 minutes** to complete all activities.

Attention Checks and Incentives:

To ensure that participants are fully engaged with the survey, we will include a **brief attention check question** at regular intervals (e.g., "Please select 'Strongly Agree' for this

question to continue"). If participants fail the attention check or provide inconsistent answers, they will be flagged, and their responses may be excluded from the analysis to ensure data quality.

Participants who complete the survey will not receive any financial incentives; however, they will be thanked for their participation at the end of the survey.

Secondary Data:

There is no secondary data being used in this study; the data will only be collected directly from participants via the survey.

Supervision (for Student Researchers):

Since the study does not involve any physical risks or sensitive medical data, there will be no immediate need for frequent check-ins. However, as a student researcher, I will ensure ongoing supervision by my PI at the Indian Institute of Technology Kharagpur to ensure the research adheres to ethical guidelines and data protection standards. Regular consultations will occur as necessary throughout the data collection and analysis process.

9.0 Research with Vulnerable Populations

This study does not include vulnerable populations such as children, prisoners, adults with impaired decision-making capacity, pregnant individuals, or any other groups specifically susceptible to coercion or undue influence. The participants eligible for this study will be adult individuals (18 years and older) who voluntarily consent to participate in the online survey.

However, given that recruitment is done online and the survey will be self-administered, the study design ensures that participants are given full control over their participation, which minimizes the risk of undue influence. Below is a breakdown of how the study addresses issues of coercion and influence, particularly for certain demographics that may require additional safeguards:

Recruitment Process:

- Recruitment will be done through online platforms (such as social media, mailing lists, and crowdsourcing platforms like Amazon Mechanical Turk) where participants can opt into the study voluntarily. No direct interaction will be required between the researchers and the participants, reducing the possibility of undue influence.
- Participants will be fully informed of the voluntary nature of the study before they consent to participate. Recruitment materials will emphasize that

participants may withdraw from the study at any point without consequences, ensuring that no coercion is involved.

Assent/Permission Process:

- Since the study will only include adult participants (18 years and older), formal assent or parental permission is not required.
- Participants will be asked to provide informed consent electronically before beginning the survey. The informed consent form will detail the study's purpose, procedures, risks, and confidentiality measures.
- Given the adult population, this process will not involve interactions with parents, legal representatives (LAR), or guardians. The consent will be independent, ensuring participants are fully able to understand the study and make informed decisions.

Data Collection:

- The data collection method (online self-administered survey) is suitable for the adult population being recruited, as it allows participants to complete the survey in their own time and space, ensuring comfort and privacy.
- Since the survey is anonymous and participants are not required to provide any personally identifiable information, the risk of undue pressure is minimized.
- Participants will be informed at the beginning of the survey that they can choose not to participate or skip questions without any penalties.

Students/Employees in Research:

- The study does not involve participants from specific groups like students or employees in any coercive or supervisory relationships. Participants will not be recruited from any specific workplace, academic course, or other environments where undue influence may arise.
- To further reduce any risk of undue influence, recruitment efforts will be spread across different platforms (e.g., social media, online forums) to ensure that participants are not part of any specific group that may feel pressured to participate due to the status of the researcher.

10.0 Sharing Results with Participants

In this study, participants will not receive individual results, as the data collected is not related to investigational diagnostic tests, genetic tests, or any clinical assessments. The study focuses on password usage patterns and the comparison of user-generated versus LLM-generated passwords, which do not generate any personal health or diagnostic

information that would require follow-up with participants or other stakeholders (such as a primary care physician).

Study Results Sharing:

1. **Aggregate Results**: Upon completion of the study, the overall results will be analyzed and published in a research paper or report. These findings will focus on the comparative effectiveness of LLM-generated passwords versus user-generated passwords in resisting targeted password guessing. If applicable, the results will be shared in peer-reviewed academic journals or conferences.
2. **Sharing Results with Participants**: Participants will be informed at the outset that they will not receive individual results. This is because the study does not involve personalized feedback or clinical outcomes. However, they will be provided with an opportunity to access the overall study findings upon request. This will be communicated through a summary report or website link after the study is completed and results are published.
3. **Justification for Not Sharing Individual Results**: The nature of the data does not involve personal diagnostic information or findings that would require individualized follow-up. Since participants are not providing personal health data or undergoing clinical testing, there is no ethical or practical need to share individual results with participants. The research will focus on aggregate trends and statistical outcomes related to password security, which does not affect the participants' personal security beyond the scope of this study.

11.0 Incomplete Disclosure or Deception:

This study does **not** involve incomplete disclosure or deception. The purpose of the study, the procedures involved, and any associated risks will be fully disclosed to the participants during the informed consent process. Participants will be clearly informed about the nature of the study, which involves the comparison of user-generated and LLM-generated passwords to evaluate their susceptibility to targeted password guessing attacks. The participants will not be misled or withheld any information that could affect their decision to participate.

Since the study does not involve deceptive practices, there is no need for a debriefing process or any alteration to the standard consent procedure. All participants will have the opportunity to ask questions before providing consent and will be informed that their participation is voluntary, with the ability to withdraw at any time without consequences.

12.0 Consent Process:

Consent Method: The study will obtain online informed consent from all participants. Participants will be required to read the consent form before completing the online survey. The consent process will include detailed information about the study, its purpose, procedures, potential risks, and benefits. Participants will also have the opportunity to ask questions before consenting.

Participants will be presented with the consent form at the beginning of the online survey. They will indicate their consent by selecting the "I agree to participate" option. This will be recorded electronically as their consent to participate in the study.

Process Details:

1. Pre-Survey Information: At the beginning of the online survey, participants will be provided with an introductory section that clearly outlines the study's purpose, procedures, risks, and benefits. This information will be written in clear and concise language to ensure that participants understand the study's goals and what participation entails.
2. Informed Consent: After reading the study information, participants will be asked to confirm that they understand the study details and agree to participate. By selecting "I agree to participate," they will be providing their consent.
3. Time for Decision: Participants will be given adequate time to review the consent form and ask questions before agreeing to participate. The form will explain that participation is voluntary, and they may withdraw from the study at any time without consequences.

For Non-English Speaking Participants: In the case of non-English speaking participants, the consent materials will be translated into the most relevant language(s) based on the target audience. The process will include:

- Translation of Materials: Any recruitment, consent, and study materials will be translated to the language(s) spoken by participants.
- Certified Translator: A professional translator will be employed to ensure accurate translation of consent documents and other materials.
- IRB Approval: The English-language versions of the materials will be submitted to the IRB for approval before proceeding with translations. The translated documents will also be submitted to the IRB with a Certificate of Translation.

Participants Who Lack the Capacity to Consent: This study does not involve participants who lack the capacity to consent. All participants will be required to confirm their ability to consent to the study prior to participation.

Enrolling Children (If Applicable): This study does not include children, as the target population will consist of adults over the age of 18.

Special Circumstances: Since this is an online survey, there are no face-to-face interactions. Therefore, there is no concern about undue influence or coercion in the consent process.

Consent Documentation: In the case of online consent, participants' consent will be documented automatically by the online platform. Their consent is captured by selecting the "I agree to participate" option, which will be recorded in the system for reference.

13.0 Waiver of Participant Signature on Consent Form:

In this study, **the participant's signature on the consent form will not be obtained**. This is due to the nature of the research being conducted **online** via a survey platform, where obtaining a physical or digital signature would be cumbersome and unnecessary. Instead, consent will be documented by the participant actively selecting the "I agree to participate" option at the beginning of the online survey, which will serve as the consent confirmation.

The reasons for the waiver of the participant signature are as follows:

1. **Online Data Collection:** The study is conducted entirely online, and obtaining a participant's signature would complicate the process. The "I agree" selection within the survey platform serves as an appropriate and secure alternative to documenting consent.
2. **Confidentiality Considerations:** Since this study is focused on survey responses, the absence of a signature ensures that the data collected remains anonymous and reduces any potential risk related to identifying or linking participants to their responses. The use of an online platform ensures that no personal identifying information, other than what is required for study participation, is collected.
3. **Cultural Norms and Practices:** Given that this study may include participants from diverse regions around the world, the practice of obtaining signatures may not be a common or culturally appropriate method for documenting consent in all locations. Therefore, an electronic acknowledgment of consent ensures broad cultural and practical feasibility.

For these reasons, a waiver of participant signatures on consent forms is being requested, with the online "I agree to participate" mechanism serving as the valid consent process for the study.

14.0 Waivers and Alterations of Consent Information:

In this study, we are requesting a **waiver of consent** to facilitate the collection of survey data. The following points outline why this waiver is necessary and appropriate:

1. **Minimal Risk to Participants:** The study involves minimal risk to participants, as the survey collects general information related to their views and opinions. There are no physical interventions, sensitive topics, or risks of harm involved in participation, making the request for a waiver of consent reasonable under the **minimal risk** category.
2. **Practicability of the Research:** Obtaining written consent through signatures would not be feasible in an online survey context, especially for a study with potentially large-scale participation across various countries. Requiring a signature would introduce logistical and cultural barriers that would make it difficult to gather sufficient data to make the study successful. The study can only be effectively carried out if consent is obtained through a digital acknowledgment (i.e., the "I agree" option in the survey).
3. **Use of Identifiable Information:** The study will not collect any identifiable personal information, as responses are anonymous. This helps minimize any risks related to privacy concerns while allowing for a meaningful analysis of the data.
4. **No Adverse Impact on Participant Rights or Welfare:** The waiver of written consent will not adversely affect the rights and welfare of the participants. Participants will still be fully informed about the study purpose, procedures, and their voluntary participation through the consent information presented at the beginning of the survey. They will also have the option to withdraw at any time without penalty.
5. **Debriefing:** Since the study does not involve **deception** or **incomplete disclosure**, **debriefing does not apply to this study**. Participants will be given all relevant information about the study during the consent process and can contact the researcher for any further clarifications.

Thus, the requested waiver of written consent will ensure the study is conducted effectively, and the rights and welfare of the participants will be safeguarded throughout the process

15.0 Financial Compensation:

There is **no** requirement to compensate research participants.

16.0 Audio/Video Recording/Photography

In this study, we do **not** plan to use audio, video, or photography for data collection purposes. The study will be conducted through an anonymous online survey, which does not involve any audio or video recordings.

Rationale for Not Using Recordings:

- Since the research is focused on collecting survey data, the use of audio or video recordings is unnecessary and would not provide any additional value to the data collection process.
- The research aims to gather participants' opinions or responses, which can be effectively captured through text-based survey responses, and does not require visual or audio documentation.

17.0 Potential Benefits of this Research:

This study does **not** involve direct benefits to individual participants, as it focuses on collecting data to assess opinions or experiences related to the topic of internet voting. Participants are not expected to gain any personal advantages from participating in the study, as the primary aim is to contribute to academic knowledge and understanding of the subject.

However, **indirect benefits** include the potential for broader societal impact. By investigating the need and feasibility of internet voting, the research may:

- **Contribute to public policy development**: The findings could help policymakers understand public attitudes toward internet voting, potentially influencing decisions on the adoption or improvement of such systems in various jurisdictions.
- **Enhance understanding of voting systems**: The study could provide insights into the challenges and opportunities of internet voting, supporting efforts to make elections more accessible, secure, and efficient.
- **Advance academic research**: The research could add valuable data to the field of election security and internet-based decision-making, influencing future studies and technological developments in this area.

These potential societal benefits, such as informing better electoral systems, ensuring more inclusive and accessible voting processes, and improving public trust in voting technologies, are key outcomes of this research.

18.0 Potential Risks to Participants:

While the study does not involve significant physical risks, there are some **social and psychological risks** associated with participation:

1. **Breach of Confidentiality**:
    - **Risk**: There is a potential risk of breach of confidentiality, which could lead to personal information being disclosed without consent.
    - **Magnitude**: The risk is considered moderate, as personal data such as survey responses will be collected. However, measures to anonymize and securely store data will mitigate this risk.
    - **Mitigation**: To reduce this risk, all data will be anonymized, and participants' identities will not be linked to their responses. Data will be stored on encrypted servers, and access will be limited to the research team.
2. **Emotional Discomfort**:
    - **Risk**: Some participants may experience mild discomfort or frustration when answering questions related to internet voting, especially if they hold strong opinions on the matter.
    - **Magnitude**: The psychological impact is expected to be minimal, as the survey questions are not intended to provoke intense emotions.
    - **Mitigation**: Participants will be informed in advance that they can skip any questions they do not feel comfortable answering. A contact point for further questions or concerns will be provided at the end of the survey.
3. **Social or Political Stigma**:
    - **Risk**: If participants' opinions on internet voting differ significantly from the mainstream, they may feel social stigma or judgment, particularly in a public or community context.
    - **Magnitude**: The social risks are minimal since the survey responses are anonymous.
    - **Mitigation**: Anonymity of responses will ensure that no participant can be identified or publicly associated with any particular opinion or viewpoint, reducing the chance of social stigma.
4. **Time and Effort**:
    - **Risk**: Participation requires time and effort, as the survey may take 15–20 minutes to complete.
    - **Magnitude**: The risk is low, as this is a typical duration for surveys and is unlikely to cause significant inconvenience.
    - **Mitigation**: The time commitment required for participation will be clearly communicated to participants prior to their involvement, and they will have the option to withdraw at any time without penalty.

19.0 Provisions to Protect Participant Privacy and Data Confidentiality:

1. Participant Privacy:

- **Privacy Measures**: To protect participants' privacy, all surveys and questionnaires will be administered online. They will be able to complete the survey at their convenience in a private space where they feel comfortable, ensuring no one else overhears their responses. If in-person interactions are necessary, such as a focus group or interview, these will take place in a private setting where others cannot overhear the discussion.
- **Anonymity**: The study will be designed to ensure that no personally identifiable information is collected. Data such as names, contact information, and IP addresses will not be recorded to preserve privacy.

2. Confidentiality of Data:

- **Data Collection and Initial Handling**: During data collection, all participant responses will be stored without any personally identifiable information (PII). For instance, survey responses will be collected through platforms such as Qualtrics or Google Forms that automatically anonymize the data (e.g., by excluding IP addresses or other direct identifiers). If any personally identifiable information is necessary for follow-up or for the study's integrity, participants will be explicitly informed and their consent will be obtained.
- **Data Security during Transfer**:
    - All data will be encrypted when transferred between collection platforms and the storage system. Secure data transmission protocols (such as HTTPS) will be used for web-based data collection.
    - Any transfer of data between team members will occur using secure channels such as encrypted email or a secure file sharing platform, like OneDrive or Dropbox, with password protection.
- **Data Storage**:
    - Data will be stored on password-protected, encrypted servers. Only authorized research team members will have access to the data. Access will be granted through a secure login system with multifactor authentication to ensure that only individuals with the necessary permissions can access the data.
    - For surveys or questionnaires that collect sensitive data, all responses will be anonymized by stripping any identifying information at the earliest stage of data processing, ensuring that individuals cannot be linked to their responses.
    - If audio or video data is collected, all recordings will be stored in a secure, password-protected location. The recordings will only be accessible by the research team members who are authorized to handle

such data. Audio recordings will be deleted once they have been transcribed.

3. Data Handling and Retention:

- **Coding System and Data Anonymization**:
  - If any personally identifiable information is collected, a coding system will be used to replace identifiable information with unique codes. The key linking the codes to the identities will be stored separately in a secure, password-protected location, and access to it will be restricted to the principal investigator (PI) and designated study staff.
  - The key will be stored on a different server or encrypted folder to prevent unauthorized access.
- **Transcription of Audio Recordings**:
  - If audio recordings are made, they will be transcribed by authorized personnel. Once transcription is complete, the audio files will be deleted from the storage system to minimize the risk of unauthorized access to sensitive data.
- **Data Storage Duration**:
  - Data will be stored securely for at least 3 years following the completion of the study, in accordance with institutional policies. If there are any legal or regulatory requirements that demand a longer retention period, the data will be kept for the required duration. After the retention period has passed, the data will be securely destroyed using data-wiping software to ensure that no recoverable information remains.

4. Additional Safeguards for International Data Collection:

- If the data is being collected internationally, steps will be taken to comply with relevant local data privacy laws. Data encryption will be implemented, and secure data transfer methods will be used. Additionally, any international travel for data collection will follow the necessary protocols set out by the institution's IT and export control offices to ensure compliance with international data security requirements.

20.0 Data Monitoring Plan to Ensure the Safety of Participants:

Although this study does not involve clinical trials or the direct assessment of risks that could immediately indicate harm to participants, we will monitor the data to ensure participant safety, particularly in the case of sensitive or distressing responses. Below is the plan to monitor and address potential risks:

1. Monitoring of Sensitive Data:

- Survey/Interview Responses: During the study, participants may provide answers that reflect distress or sensitive issues. For example, if participants disclose information suggesting harm to themselves or others, or if there are indications of abuse, the research team will follow appropriate procedures.
- Triggers for Action: Specifically, if any responses suggest suicidality, self-harm, intent to harm others, or any form of abuse (e.g., child, spousal, elder abuse), the research team will be prepared to take immediate action.

2. Response Protocol:

- Qualified Assessment: For any responses indicating potential harm, a qualified mental health professional or researcher trained in crisis management will review the situation and assess the level of risk. If necessary, the participant will be referred to appropriate resources such as emergency support services, mental health hotlines, or a local crisis center.
- Confidentiality and Reporting: In accordance with institutional and legal obligations, if a participant discloses intent to harm themselves or others, or if abuse is suspected, the research team will follow mandated reporting procedures. In these cases, the confidentiality of the participant will be balanced with the obligation to ensure safety.
- Immediate Contact: In the case of emergency or if the participant expresses intent to harm themselves or others, the research team will immediately offer to provide resources for support, such as the contact information for suicide prevention helplines or local emergency services. If the participant is in immediate danger, the research team will contact appropriate authorities (e.g., emergency services or the participant's emergency contact) in accordance with legal obligations.

3. Frequency and Type of Monitoring:

- Real-Time Monitoring: The research team will monitor the responses in real-time, especially in interviews or surveys where participants may disclose sensitive information. A team member trained to handle sensitive data will be available during data collection to assess any potentially harmful responses.
- Regular Evaluation: Data will be evaluated periodically to ensure there are no emerging patterns that suggest potential risks. The frequency of this evaluation will depend on the nature of the data collection. For surveys, monitoring will occur once data is submitted and processed, while for interviews, the team member responsible will assess any immediate issues raised by the participant.

4. Training and Qualified Team Members:

- The research team will be trained in identifying signs of distress and handling sensitive situations. This will include training on how to address disclosures of self-harm, abuse, or intent to harm others. A mental health professional will be available for consultation if needed.

5. Addressing Risk from Disclosures of Sexual Misconduct:

- Sexual Misconduct Reporting: If the study involves any disclosures regarding sexual harassment or assault, participants will be informed in the consent form that the research team must report such disclosures in accordance with Northwestern University's policies. This includes a requirement to report to the Office of Equity any instances where sexual misconduct is disclosed by a participant who is affiliated with the Northwestern community.
- Participants will also be informed about the resources available for sexual misconduct survivors, including the Office of Equity and counseling services. If a disclosure occurs, the research team will follow the necessary reporting procedures as outlined by the university and state laws.

6. General Safety Measures:

- The research team will prioritize participant well-being throughout the study. Participants will be given resources at the beginning of the study, such as emergency contact numbers and hotlines for mental health support, in case they feel distressed during or after participating.

21.0 Long-term Data and Specimen Storage and Sharing:

1. Data Storage Plan:

- The data collected during this study will be stored securely for a minimum of **3 years** after the completion of the study, as per Northwestern University's policy. This includes both any survey or interview data collected and any transcriptions of audio recordings.
- **Storage Locations**: The data will be stored in encrypted, password-protected folders on Northwestern University's secure servers or other approved institutional platforms, such as **Qualtrics**, **REDCap**, or other designated data management systems.
- **Data Anonymization**: Identifiers will be removed from the data as soon as they are no longer needed. If identifiers are kept for any reason (e.g., for longitudinal studies), they will be stored separately from the research data, with strict access controls in place.

2. Data Sharing Plan:

- **Sharing for Future Research**: If the data is to be used for future research, the data will be made available to other researchers through a **data repository**. The primary repository for this study will be a **public or institutional repository** such as **OpenICPSR** or **Harvard Dataverse**, depending on the nature of the data and the preference of funding bodies or publication requirements.
- **Data Sharing Requirements**: If this research is funded by an external agency, the funder may require data sharing in accordance with their policies. Additionally, if the research results are published in a journal, the data may be made available for review by others. The data will be shared in a way that complies with the data sharing policies of the funder or publisher.
- **Identifiers and Anonymization**: In line with best practices for data sharing, **personal identifiers will not be included** in the shared datasets. Instead, any shared data will be **de-identified**. If identifiers are necessary for the research, they will be stored in a separate, secure location with restricted access.

3. Plans for Storing Data in a Repository:

- The data will be uploaded to the chosen repository once it has been cleaned, de-identified, and the consent form stipulations are met. The repository will serve as a secure long-term storage solution, ensuring the data remains accessible for future research but also protected from unauthorized access.
- **Repository Selection**: The repository selected will be chosen based on the type of data and the discipline. For example, **OpenICPSR** is often used for social science data, while **Harvard Dataverse** is a general-purpose repository that can house a variety of data types. If the data involves sensitive materials (such as health information), it may be stored in a restricted-access repository, following relevant ethical and legal guidelines.

4. Special Considerations for Data Sharing:

- **Consent for Data Sharing**: Participants will be informed in the consent form that their data may be shared for future research purposes, but only after de-identifying or anonymizing the data. They will also be informed of the data repositories where their data might be deposited.
- **Access to Data**: Only authorized researchers with appropriate clearance will have access to the de-identified datasets. Access will be granted according to the terms specified in the data sharing agreement and in compliance with institutional policies.

5. Identifiers and Future Data Sharing:

- **Identifiers**: If identifiers are retained for any purpose (e.g., for longitudinal studies or matching datasets), the data will be linked to these identifiers in a

separate, secure system and not shared with the dataset. Access to this linked information will be restricted to specific researchers as necessary.

- **Future Use of Identifiable Data**: If identifiable data is needed for future research, separate consent for such use will be obtained from participants, or the data will only be shared with explicit permission and in accordance with institutional guidelines for data privacy and protection.

22.0 Qualifications of Research Team to Conduct the Research:

The research team is highly qualified to conduct the proposed study, with expertise spanning relevant fields of study, research methodologies, and ethical considerations. Each team member brings valuable experience, certifications, and cultural competence to ensure the study is conducted safely and ethically. The team is committed to protecting the rights and welfare of participants throughout the research process.