DIFFERENTIAL PRIVACY

Data Exposure and Informational Security

Rimisha Ghorsaini | Professor Scott Johnson | Honors College UTA

ABSTRACT

This research is based on the current emerging technology, differential privacy. The research questions privacy issues in information systems, processing, handling, organizing, and retrieving data. The goal is to have the information and the uses of the differential privacy algorithm in the data privacy processes and unfolds the application of differential privacy on various fields including the field of internet technology. This study conducted a survey of 89 University of Texas at Arlington students to understand their perception of information security. The survey revealed that participants were less attentive towards their daily activities, such as shopping, online registration, and subscriptions, which could provide one explanation for data exposure. The study also revealed respondents are open to adopting differential privacy applications. Differential privacy has a wide scope and may be very helpful in providing security to data privacy in the future.

INTRODUCTION

Differential Privacy is a system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset. It provides the way to add modulated amount of randomness to the dataset . It prevents the individual dataset from being exposed. Consider a simple algorithm that examines a dataset and computes statistics . When a single individual joins or leaves a dataset, a differentially private algorithm guarantees that its behavior hardly changes. Whatever the algorithm outputs on a database containing some individual's information is almost as likely to have come from a database without that individual's information.

METHODOLOGY

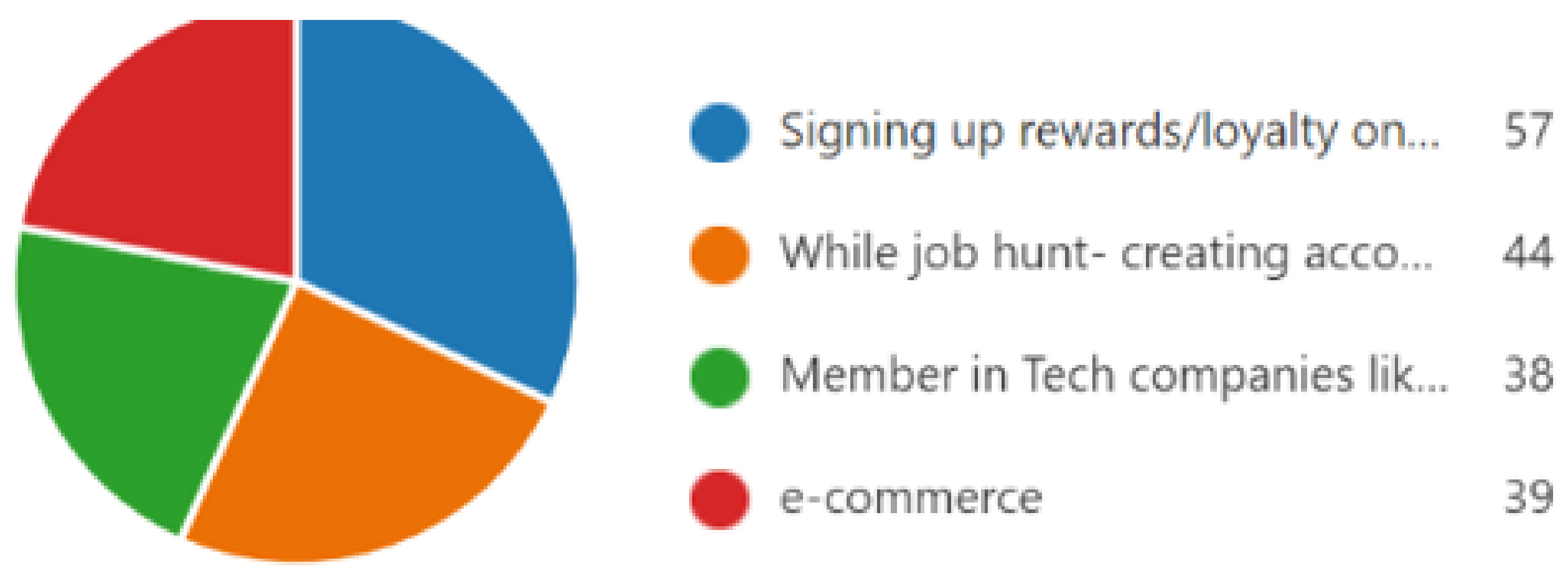
The research facilitates in two major ways.

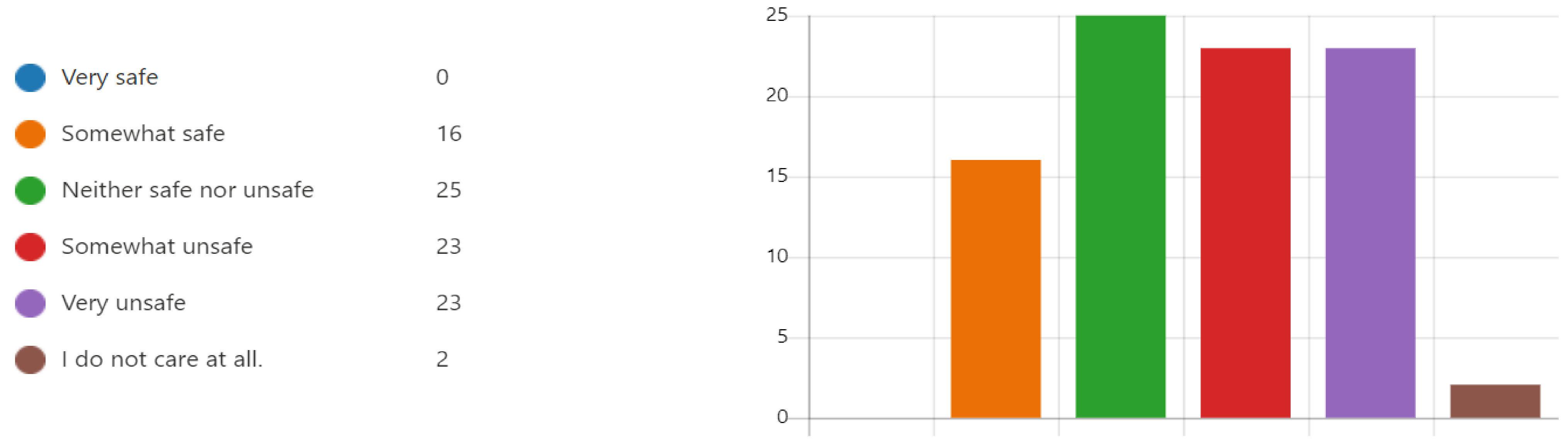
- □ Surveys
- □ Comparison/article studies

For survey, the 19-questionnaire form was distributed which collected total of 89 responses from UTA students and faculty. The survey used the differential privacy by keeping the respondent's privacy and not revealing their personal data.

SURVEY | ANALYSIS

- □ 66% of respondents were 18-24 yrs. old.
- □ Data Exposure of these 89 people through subscription, shopping, and services like utilities.
- □ View on Technological advancement and safety
- □ Differential Privacy awareness and acceptance





FINDINGS

- □ Differential Privacy was widely used in 2008, U.S. Census. In 2020, LinkedIn for advertiser queries.
- □ In iOS and macOS in emojis, health queries also showed differential privacy application.
- □ Differential Privacy has the capacity for preventing data breaches, safeguarding people's rights,
- □ and preventing attacks.
- □ On the other hand, differential privacy might not be helpful with big data due to low accuracy and the inability to analyze at the individual level.

The findings from survey revealed that people are open to differential privacy and aware of the causes of data exposure. The findings are also supported by various scholars and their research..

REFERENCES

Informational Privacy vs. Public Access to Governmental Records. Informational privacy. (n.d.). Retrieved March 19, 2022, from https://media.okstate.edu/faculty/jsenat/jb3163/infoprivacy.html

Aitsam, M. (2022, January 1). Differential Privacy Made Easy-Computer Science > Cryptography and Security. Sheffield Hallam University United Kingdom; Cornell University-Arxiv. https://arxiv.org/abs/2201.00099

Litman, J. (2000). Information Privacy/Information Property. *Stanford Law Review*, *52*(5), 1283–1313. https://doi.org/10.2307/1229515\

CONCLUSION

Many companies and businesses could focus on adopting algorithm in their services including large tech companies such as Apple and even government agencies. This research could bring awareness to the public about their information privacy, exposure, and consequences. Future research into differential privacy has the potential to protect privacy and optimize collected data.

ACKNOWLEDGEMENT

Thank you to the individuals who helped with the project and the students who responded to the survey.