Spring 6-1-2018

Gender and Major Differences in Privacy Views of UConn Students

Shreya Varshney
shreya.varshney@uconn.edu

Gender and Major Differences in Privacy Views of UConn Students

By Shreya Varshney

Table of Contents

Abstract

Online privacy is a challenge that is steadily gaining importance. New information on privacy breaches occurs with alarming regularly. Studies are being done to help people become more aware of this topic[1]. This study researched the if and how gender, major, and class standing affect the views towards online privacy of students at the University of Connecticut. The research was performed by first asking students to fill out a quick ten question survey. The responses to these surveys were analyzed in order to reach conclusions. The primary conclusion of this thesis is that gender and major definitely affect the online privacy of individuals.

Background

Online privacy is how much control an individual has over the sharing of their information on the Internet. The primary factors that affect online privacy are what the individual does online and how they do it. For example, if the individual is using a weak password for an email account then a hacker can easily break into this account and use it to send malicious emails to their friends or read emails that contain personal information and use this as leverage for blackmail. Another example is an individual posting a number of private and personal information on their social media accounts where anyone can see because their privacy settings are not restrictive. I personally encountered an individual who posted a picture of their credit card without blocking out the number, and then posted the pin number when asked to. Not everyone is aware of what is actually private when they are online. Unfortunately, the answer is very little.

[1] Examples of this include "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study" by Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Aquisti, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences" by Bernhard Debatin, Jeanette P. Lovejoy, Anne-Kathrin Horn M.A., and Brittany N. Hughes, and "Beyond Concern: Understanding Net Users' Attitudes about Online Privacy" by Lorrie Faith Cranor, Joseph Reagle, and Mark S. Ackerman

Online presence is a current issue for everyone. Based on information from whistleblowers, it appears that the federal government also records online activity[2]. Companies are collecting information from your computers using cookies. This data is stored and used to improve their performance ability to advertise to you. For example, say you visit an online shopping website, like Amazon or Alibaba. Then afterwards you visit a site about the history of clocks. The next time that you go on the shopping site you will most likely see some clocks on the welcome page. How did the site do this? Well, when you first visited the online shopping site while you were unaware (or maybe even aware) the site implanted a cookie into your system. This cookie will not harm you or your computer in any way. There are no viruses involved. The cookie *only* keeps a record of all that you do afterwards. When you visit the history of clocks website, the cookie records the fact that you are interested in clocks. Now the cookie reports back to the shopping website and says that you are interested in clocks. Thus, when you open the shopping website again you are likely to see clocks: that is what you are interested in and are likely to buy. The intention behind the collecting of data is to improve what a customer sees when they are shopping to produce more revenue for the website and so that the customer is likely to come to that site again. However, if there is even a small vulnerability in the server storing this data a hacker can breach the server and gain access to all the data stored in that server. This data often includes personal data collected either knowingly or unknowingly.

A new idea was developed to make data collection safer. This idea is called differential privacy[3]. Differential privacy is a mathematical definition for privacy loss when comparing two similar data sets. The idea is that if two data sets are so similar that there is little difference that

[2] Read the book "No Place to Hide; Edward Snowden, the NSA, and the U.S. Surveillance State" by Glenn Greenwald for more details

[3] Read "Calibrating Noise to Sensitivity in Private Data Analysis" by Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith for more info

can be discernible by an adversary, then a data set is private because it does not depend on any individual's contribution to the data set. An example of this would be when a person takes a survey. The data that they generate will not change the outcome of all the data collected. Therefore, the personal privacy of the survey-taker will not be affected.

The main mechanism for achieving differential privacy is to add random noise to the data. The idea is that the data the adversary sees could be real or randomly generated and they would not know. An example of this is the coin flipping protocol. In this protocol the surveyed individual flips a coin. If the coin lands on heads the individual sends their true answer. Otherwise the surveyed flips the coin again and sends a random response based on that coin flip. For example, say the survey question was what is your favorite color apple, and the options were green and red. Before answering, the individual will flip a coin. If it lands on heads the individual sends their real answer. Otherwise the coin is flipped once more. If the result of this coin flip is heads then the response is green, if the result is tails then the response is red. The intuition between why this protocol is private is that for an individual's response it is entirely possible that the choice is made by a random generator, the surveyor has no clue if this is the real response for that individual without knowing about the coin flips. However, overall statistics such as average and median are preserved on the collected dataset. Differential privacy is used by companies like Apple and Google to collect data on how to improve their services[4]. However, adoption is still relatively sparse, with companies planning future adoption[5].

[4] To read about Apple's use of Differential Privacy go to the following webpage: https://www.apple.com/privacy/ To learn more about Google's use of Differential Privacy go to the following webpage: https://research.google.com/pubs/pub42852.html

[5] An example of this is in the research paper "On the Connection between Differential Privacy and Adversarial Robustness in Machine Learning" by Mathias Lecuyer, Vaggelis Atlidakis, Roxana Geambasu, Daniel Hsu, and Suman Jana

One way for a person to understand their online privacy is searching for themselves. Search algorithms have five steps they go through in the few milliseconds that it takes for a search to be processed. The first step is to analyze the search query itself. This step involves determining the type of query, based on analysis of the natural language as it is spoken today, and checking for spelling mistakes. The next step is to search for web pages that match the search query. After that, each web page is ranked based on freshness, frequency of the query terms on the page, the trustworthiness of the page, and how often that site is referenced in other search results. In searching algorithms like Google's search algorithm, the location of the query and the user, if there is an account linked to the search query, are taken into account to make the results more relevant to the individual. In other searching algorithms, like DuckDuckGo's search algorithm these factors are ignored to enhance the searcher's privacy. The search occurs without using these factors. Finally, the search results are given a second evaluation on which results best fit the query before the searcher gets to see the results. In this thesis, we analysis search ranks to gain information about persons' online privacy.

My interest in privacy came from a class that I took in my third semester at UConn. The class was called Privacy in the Information Age. It talked about how privacy affects us in the current age, also known as the Information Age. This age is called the Information Age because there is so much information out there and everyone is expected to share it. Privacy in this age is different than in other ages because everyone wants privacy, but they also want attention from their peers as approval. This creates a paradox: because we want privacy but we also want to tell others about ourselves. A societal goal is to create some protocols that allow people to share information while still controlling their privacy. I wanted to research this phenomenon further; I decided to study how citizens beliefs and knowledge affect their online privacy.

Design

The purpose of this study is to analyze the online presence and privacy of University of Connecticut Students. We are living in the Information Age where everyone is expected to provide some personal information to everyone else. This leads to an increase in our individual online presence and a decrease in our personal privacy. This study will examine the usage of UConn students on popular shopping and social media sites. The study will attempt to identify underlying variables controlling such usage including major and class year.

The survey was designed to see if education level, type of education, and gender affect the online privacy and presence of the UConn students. One stereotype being investigated is gender differences. The stereotype is that people who identify with the female gender will spend more time shopping and on social media. Therefore, the students that are female should have a higher online presence than males. Another common belief is that students' major will affect their online presence as well. Those students with computer related majors may know more about privacy and the affect it has on online presence, as they learn this information in classes. In addition, they have more technical expertise on how to modify and control privacy settings. The final common belief is that education level and age will affect online presence. As students learn and progress, they learn more about their environment including the online world. It is natural to assume that as students learn, this would affect their online presence.

Based on these previously mentioned beliefs and stereotypes, I hypothesize that gender, major, and education level will affect a student's online presence and awareness of privacy. More specifically: men, students with computer related majors, and students with a higher education level will be more aware of privacy and therefore less present online.

The study was designed in a survey format that would be sent to specified groups. The members of those groups would fill out a quick 5-10 minute survey. I used an online survey platform called SurveyMonkey. This platform was used because SurveyMonkey allows for me to anonymize the data so that I do not receive any information about the student and the computer that the student used. The online platform also allows for the students to fill out the surveys from the comfort of their home rather than fill them out in the cold winter weather of Connecticut.

I picked three groups to ask to fill out this survey. I asked the UConn Cybersecurity Club for two reasons: 1) they have an interest in the results 2) they may have a smaller online presence than an average student. I also asked the UConn Marching Band and UConn's Honors Community as these are organizations that I am a part of and they have people from a variety of majors. The Cybersecurity Club and the Marching Band accepted but unfortunately the Honors Community was unable to participate. I expected less than a 10% response rate from this population. My goal was to receive approximately 100 responses overall. The study required a variety of students from many majors to participate in the survey. I asked the above groups to participate as they provided a variety in the intended demographics. Since I expected a low response rate a large number of individuals were solicited. I asked the following questions:

1. What gender are you most associated to?
2. What is your major?
3. What is your class standing?
4. Which of the following social media do you use?
5. What is the security setting for these social media accounts?
6. Where do you shop online?
7. Do you think these shopping sites value your privacy?

8. Go to google.com.

   Make sure that you are signed out of all accounts.

   Type in your whole name into the search bar.

   Look at the results.

   Enter the number of the search result that is actually about you (i.e. 1, 2, 3), or indicate that you do not show up on the results of the first page.

9. Now sign into your Google account, and repeat the previous step. (Your school email @uconn.edu is a Google account)
10. Sign out of Google and proceed to another search engine called DuckDuckGo (found at www.duckduckgo.com). Repeat the steps of question 8.

Each question was chosen for a specific intended purpose.

Questions 1, 2, and 3

These three questions were chosen to determine which demographic cross-section the student taking the survey is in. Each question outright asks for the specified demographic. There are three questions one for each demographic that was studied.

Questions 4 and 5

I chose these questions to see how aware you are of yourself online. The hypothesis is that those aware of their presence would have fewer social media accounts and more private security settings. The more social media accounts that you have the less private you are on the Internet. Also, social media sites use the less private settings as their default setting. A student has to be consciously aware of privacy and the settings in order to have a more private account.

Questions 6 and 7

These two questions were chosen to determine if the student was aware about the online companies' data collection. If the student was then they would know that the online shopping sites do not value privacy of their customer and thus would answer no to the second question. Answering yes shows that the student is not aware of the privacy consequences of online shopping sites.

Questions 8, 9, and 10

These three questions are designed to measure students' online presence. It uses the search algorithms to measure a student's online presence. There are three questions. The first simply checked what the rank are from the Google search engine without entering a Google account or linking to a specific student. The second question asks if there was a change if an account linked to the student was used for the search. The final question was to see if locations, linked accounts, and other secondary factors used by Google affect the results. The higher the rank of the result (meaning the number is smaller) the more present the student's online presence is and so they are likely to be less private online.

The above questions helped in analyzing the results and demographics to reach a conclusion on how these demographics affect online privacy.

Analysis

***Figure 1**: Based on responses to questions 1, 4, and 6*

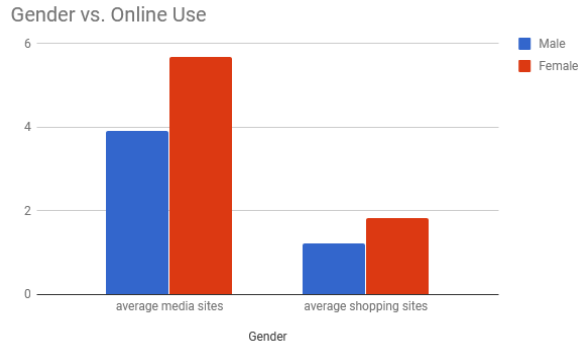


***Figure 2**: Based on responses to questions 1, 8, 9, and 10*

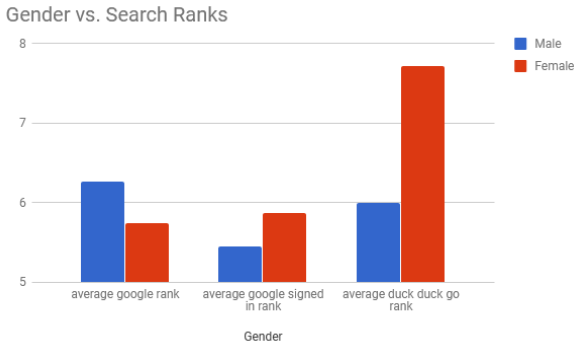


***Figure 3**: Based on responses to questions 1 and 5*

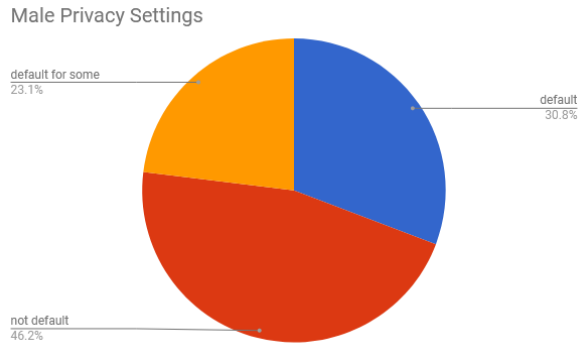


***Figure 4**: Based on responses to questions 1 and 7*

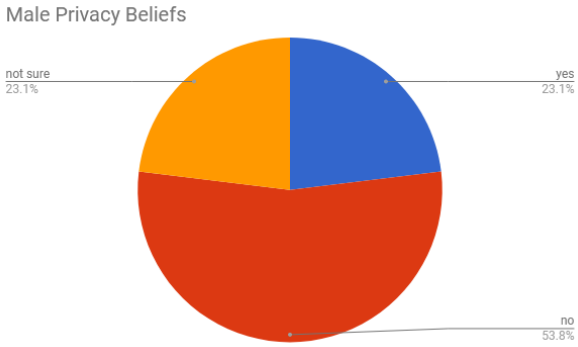


***Figure 5**: Based on responses to questions 1 and 5*

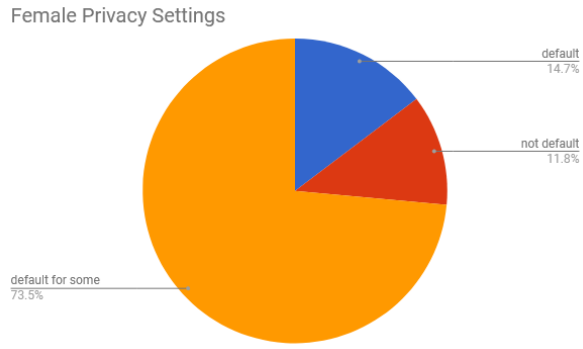
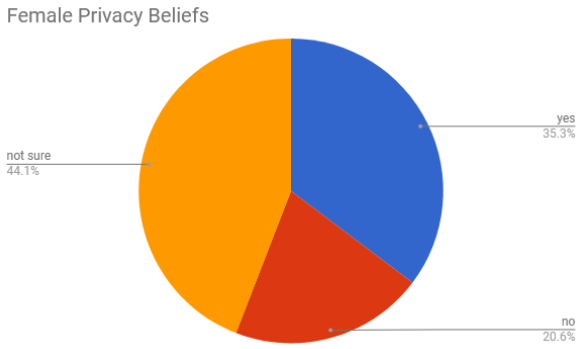


***Figure 6**: Based on responses to questions 1 and 7*



For this study, 13 men and 34 women participated from different levels of education and educational backgrounds. I compared the results of these men and women from the survey to test

the hypothesis. Recall, the hypothesis was that men would have a lower rank in all search algorithms as they stereotypically use social media and shopping sites less.

As shown in Figure 1, men use fewer social media and online shopping sites then the women. The average is the number of social media accounts that the men and women have. The lower average means that men tend to have fewer social media accounts and visit fewer shopping sites than the women do. In theory, this should result in men having a lower rank for search algorithms, as was hypothesized. This is true for the case of a simple Google search of themselves, without signing into any google account (shown in Figure 2). However, for both the search in Google while signed into a Google account and for the DuckDuckGo search the ranking for men was higher than the ranking for women (also shown in Figure 2). When looking at Figures 3 and 5 though it is clear why such a phenomenon occurs. A higher percentage of the men had less private settings associated with their social media accounts. 30.8% of the men who participated had default settings for all of their account. This means that only 69.2% of the participating male population had more private settings for some of their social media accounts. On the other hand, only 14.7% of women who participated had the default settings. Meaning 85.3% of the women had modified the default settings. I believe this led to the women having a higher rank when using a search algorithm that accounts for location and user but lower rank when searching with a search algorithm that is not dependent on location or user.

Another observation recognized by Figure 2 is the jump in rank for the women. There is a huge difference between the ranks for the women while utilizing the Google search algorithm and the rank for the women while utilizing the DuckDuckGo search algorithm. Again, this difference is caused by the privacy settings managed by the women for their social media accounts.

Despite all that is observed the men seemed more aware of what online privacy is in terms of data privacy (shown in Figures 4 and 6). When asked whether or not the online shopping sites value their privacy, 53.8% of the men stated that no these sites do not value their privacy. Women only had 20.6% believe the same. We must note however that when faced with a question like this many of the responders may reconsidered their beliefs in relation to data privacy. Many students stated that they were not sure about the answer to this question. For women this 44.1% of the female students and for men this is 23.1% of the male students. Also we must consider that many men do not like to be unsure of themselves so probably would have answered "no" simply because they perceived this is what could be the answer rather than what they truly believed about data privacy online[6]. Accordingly, most of the men may have answered "no" for this reason, even if they were not sure what they truly thought.

***Figure 7**: Based on responses to questions 2, 4, and 6*

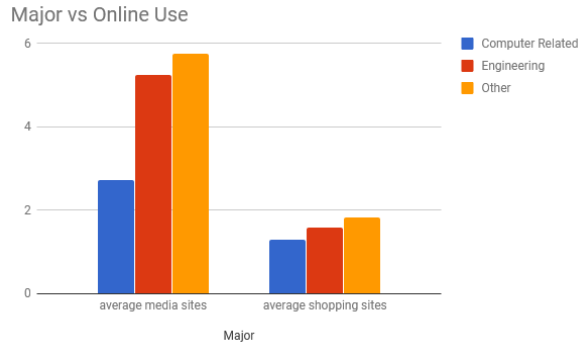
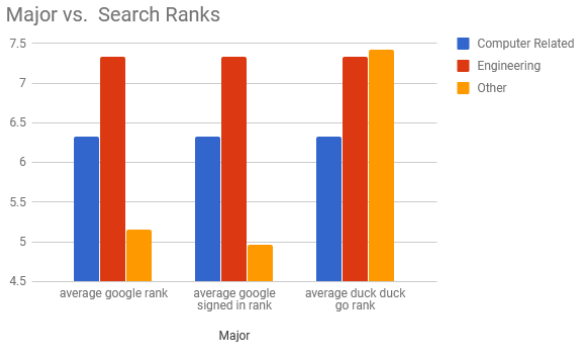


***Figure 8**: Based on responses to questions 2, 8, 9, and 10*



[6] Read the research paper "Highly confident but wrong: Gender differences and similarities in confidence judgments" by Mary A. Lundeberg, Paul W. Fox, and Judith Punćcohaŕ for more details

***Figure 9**: Based on responses to questions 2 and 5*

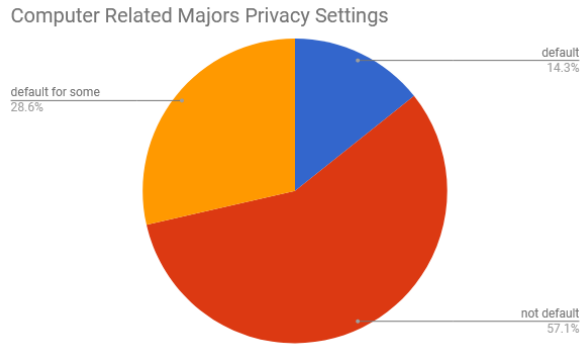


***Figure 10**: Based on responses to questions 2 and 7*

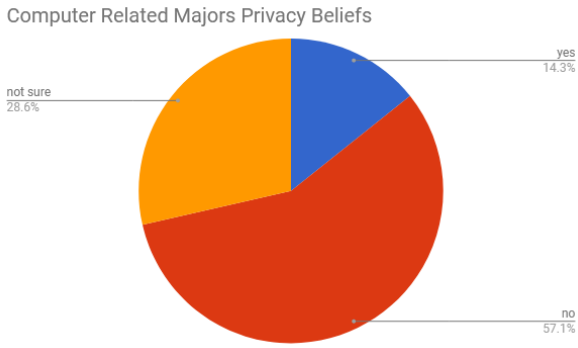


***Figure 11**: Based on responses to questions 2 and 5*

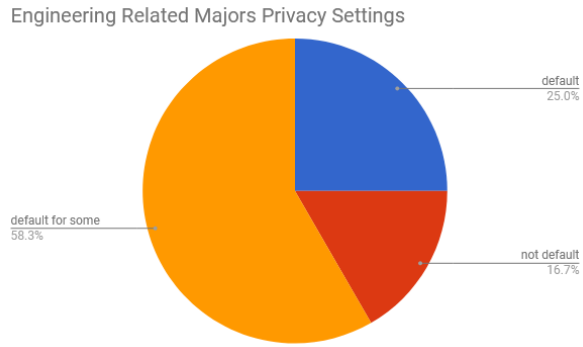


***Figure 12**: Based on responses to questions 2 and 7*

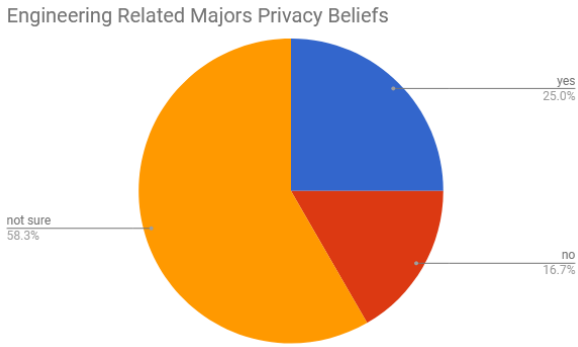


***Figure 13**: Based on responses to questions 2 and 5*

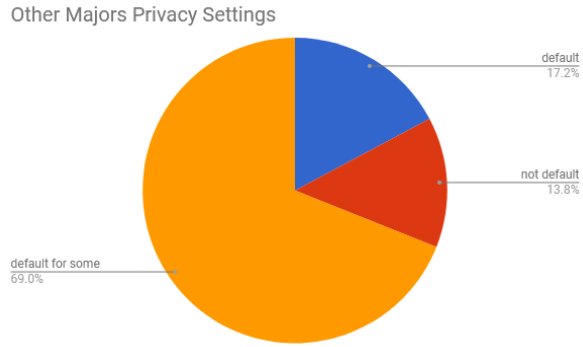
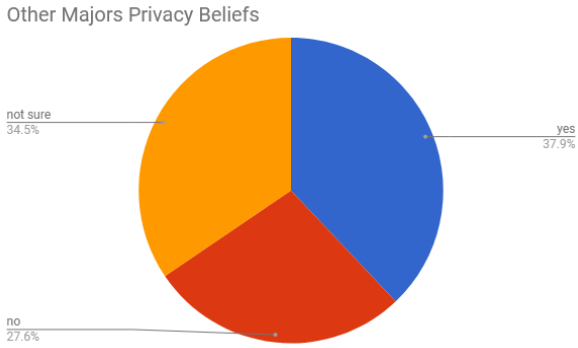


***Figure 14**: Based on responses to questions 2 and 7*



There were a variety of majors represented by the students who participated in the study. These majors were sorted into three groups: students with computer related majors, students with engineering majors that is not computer related, and students with majors that are not

engineering or computer related. We have 7 students with computer related majors, 12 students with engineering majors, and 29 students with a major other than computer related and engineering. The hypothesis for this demographic was that students with computer related majors will know more about online privacy and should then have lower averages for online use and lower rankings for search algorithms.

According to Figure 7, the students with computer related majors had a lower average of social media accounts and shopping sites used. Meaning that these students did not have as many social media accounts and did not shop on many shopping sites. This is as predicted by the hypothesis. Yet, according to Figure 8, these students did not have the lowest rank in search algorithms. For the Google search algorithms, the students with engineering majors had the lowest rank. This was followed by students with computer related majors and the students with majors not engineering or computer related had the highest rankings.

For the DuckDuckGo search the students with computer related majors had the highest rank. Then came the students with engineering majors and finally the students with non-engineering or computer related majors who had the lowest ranking of all the students. I found evidence that the students with computer related majors *should* have the lowest rankings. These students had the most restrictive privacy students (shown in Figures 9, 11, and 13) with only 14.3% of the students having default settings. For engineering students 25% of the students had default settings and 17.2% of the students with major in neither of these categories had default settings. The results of the search rankings do not reflect the online use and privacy settings. These students indicated that they post their work online in forums similar to GitHub or their own websites. One participant stated this is done so that potential employers will view their work and hire them. It is in these students' best interest if their search rankings are higher. It

appears these students use the online world to showcase their work. Consequently, these students can be seen as purposefully manipulating their online presence.

Another phenomena noticed is the constant in ranking for students with computer related majors and engineering majors. The overall rankings do not change at all. This provides evidences of my earlier hypothesis that these students are aware of their presence and promote themselves.

One more observation on the rankings in Figure 8 is that there is a big difference in the rankings from the Google search algorithms and the DuckDuckGo algorithm for the student with majors not related to computers or engineering. I believe this is due to the privacy settings of these students, only 17.2% (shown in Figure 13) of these students have default settings so when searching using a search algorithm that ignores user and location the rank will be markedly lower.

As expected the students with computer related majors were the most aware of data privacy (as shown in Figures 10, 12, and 14). Only 14.3% of these students stated that the online shopping sites value their privacy. Amongst the other students, only 25% of those with engineering majors and 37.9% of the remaining group thought that companies valued their privacy. Additionally, 57.1% of the students with computer related education background correctly stated that the companies do not value their privacy. This leads to the conclusion that this group of students really is more aware of online privacy.

When analyzing the data for the students based on class standing, I could not find meaningful patterns. This leads me to conclude that class standing does not affect the online privacy of UConn students.

I believe students chose to participate in this study based on some amount of social pressure based on our relationship. This may have caused more women to respond than men. The students recognized that I am also a woman and participated accordingly. Also, I am a part of a female dominated section of the UConn Marching Band which may have contributed to the higher percentage of female participants.

Conclusion

The major and gender of UConn students affects their online privacy. Class standing of the student does not affect their online privacy.

It was observed that men tended to be more aware of privacy and had fewer social media accounts than the women. However, men have higher rankings from the search algorithms due to their privacy settings for social media. These settings were less restrictive then the women's privacy settings.

Students with computer related majors were more aware of privacy, their studies discuss these topics. However, they have a higher online presence as shown in their rankings from search algorithms. I believe the reason for this is that these students purposefully manipulate their online presence so that their work is visible to potential employers.

Overall, students should be made more aware of online privacy and what it does to them personally. This is especially important for those students who do not realize how their online presence can be used by others without them realizing it. These students should be told how their online presence is perceived from the outside and how this information is used by other parties for their own needs. If students are more aware of their privacy, they can make informed decisions, protect themselves from cybercriminals, and even manipulate their online presence to make themselves look better in the eyes of potential employers.

Acknowledgements

I would like to first and foremost thank Professor Benjamin Fuller of the Computer Science and Engineering Department at UConn. He took the simple idea I had and guided me in formulating it into a research project. Professor Fuller's door was always open for any questions that I had and without him this thesis would not have reached the caliber that it is today.

Second, I would like to thank the individuals who participated in the survey. Their responses were key for the development of this thesis. I would also like to thank the student leaders and faculty of the UConn Marching Band and UConn Cybersecurity Club for allowing me to survey their organizations.

Third, I would like to thank my friends for being there for me in the ups and downs of college life. Without their continuous encouragement I would not have been able to finish my senior year on time.

Finally, I would like to thank my family, especially my parents, for supporting me through everything. They have been my motivation to succeed in all that I do. I hope they are proud of who I am today.

Resources

"Differential Privacy." *Wikipedia,* Wikimedia Foundation, 13 Apr. 2018, en.wikipedia.org/wiki/Differential_privacy.
"DuckDuckGo." *Wikipedia*, Wikimedia Foundation, 30 Apr. 2018, en.wikipedia.org/wiki/DuckDuckGo.
Dwork, Cynthia. "Differential Privacy." *Automata, Languages and Programming Lecture Notes in Computer Science*, 2006, pp. 1–12., doi:10.1007/11787006_1.
Green, Matthew. "What Is Differential Privacy." *A Few Thoughts on Cryptographic Engineering*, 15 June 2016, blog.cryptographyengineering.com/.
"How Search Algorithms Work." *Google*, Google, www.google.com/search/howsearchworks/algorithms/.

Vadhan, Salil, et al. *Differential Privacy*. President and Fellows of Harvard College, 2014, *Differential Privacy*.
"What Is Internet Privacy? - Definition from Techopedia." *Techopedia.com*, 2018, www.techopedia.com/definition/24954/internet-privacy.

IRB-1 Study Protocol

Protocol Version # and/or Date: December 6, 2017
Study Protocol Title: The Online Presence of UConn Students

Clinical Trial/GCP Training

Is this a research study in which one or more human subjects are prospectively assigned[1] to one or more biomedical or behavioral interventions[2] (which may include placebo or other control) to evaluate the effects of those interventions on health-related biomedical or behavioral outcomes[3] (i.e a clinical trial)? Indicate "yes," "no," or "N/A" in the space immediately below.
No
Is the study fully or partially funded by the NIH? Indicate "yes," "no," or "N/A" in the space immediately below.
No
Have the required key personnel completed Good Clinical Practice (GCP) Training? Indicate "yes," "no," or "N/A" in the space immediately below. (Note that IRB approval will not be given for NIH funded clinical trials until all required key personnel complete the GCP training.)
No

Research Plan

Purpose/Introduction:

The purpose of this study is to analyze the online presence and privacy of University of Connecticut Students. We are currently living in the Information Age where everyone is expected to provide some personal information to everyone else. This leads to an increase in our individual online presence and a decrease in our personal privacy. This study will examine the usage of UConn students on popular shopping and social media sites. The study will attempt to identify underlying variables controlling such usage including major and class year.

For EACH Participant Population State the Number of Participants to be Enrolled and Screened, if applicable: Note that the range must be justified in the **Justification of Sample Size section below**.
We will recruit from the following communities:
350 UConn Marching Band students
100 UConn Cybersecurity Club Members
Approximately 5000 Students in UConn Honors Program
Thus, our possible population size is approximately 5,500 students. We expect less than a 10% response rate from this population.

Justification of Sample Size:
The study requires a variety of students from many majors to participate in the survey. We will ask the above groups to participate as they provide a variety in the intended demographics. Since we expect a low response rate we are soliciting a large number of individuals.

For EACH Participant Population State Describe the Study Population(s):
For all population groups
Gender: all
Ethnicity: all
Income: all
Level of Education: undergrads and grads students
Age range: 18-24

Enrollment of UConn Students and/or Employees:
UConn students will be enrolled. We will not recruit relations to key personnel.

Enrollment of Key Personnel, Spouses or Dependents/Relatives: Will study key personnel, spouses of key personnel, or dependents/relatives of any key personnel be enrolled in the study? If so, describe and provide justification.
No.

For EACH Participant Population Describe Recruitment Methods:
An email invitation to an online survey will be sent to multiple groups. Shreya is affiliated with these groups.

For EACH Participant Population Describe Screening Procedures, if applicable:
In the consent form, students will be asked to verify that they are UConn students and at least 18 years of age. No other screening will be used.

Design, Procedures, Materials and Methods

The research will be conducted via an online survey created through SurveyMonkey. The individual will be asked to complete 10 questions pertaining to online presence and privacy. The survey should only take about 5-10 minutes. The intention of the survey is to prove that our online presence is very high. The following are the questions on the survey:

1. What gender are you most associated to?
2. What is you major?
3. What is your class standing?
4. Which of the following social media do you use?
5. What is the security setting for these social media accounts?
6. Where do you shop online?
7. Do you think these shopping sites value your privacy?
8. Go to google.com
   Make sure that you are signed out of all accounts.
   Type in your whole name into the search bar.
   Look at the results.
   Enter the number of the search result that is actually about you (ie. 1, 2, 3), or indicate that you do not show up on the results of the first page.
9. Now sign into your google account, and repeat the previous step. (Your school email @uconn.edu is a google account)
10. Sign out of google and proceed to another search engine called duck duck go (found at www.duckduckgo.com). Repeat the steps of question 8.

Data Analysis:

We will compare the demographics obtained through the survey with known results for participation in social media and online shopping. This comparison will be restricted to genders, class years, and technical background.

Inclusion/Exclusion Criteria:

Minors and non UConn students will be excluded from the survey. Minors are being excluded since we are asking individuals to waive consent documentation. Individuals who are not UConn students are being excluded as the goal of the study is to understand the UConn population.

Potential Harms/Risks and Inconveniences:

There will be minimal risk as the study will be conducted over a web based survey. There are some minor risks to privacy but we are not collecting any identifiable information.

Benefits:

The study is intended to enlighten the researcher and reader. All solicited individuals will receive a second email allowing them to enter an email to win an Amazon gift card. This second email will not be linked to any data collected in the first email.

Risk/Benefit Analysis:

Risks are minimal. Participants have a small possibility of financial gain. However, this possibility exists whether or not students agree to participate in the study so there is no undue pressure to participate.

Economic Considerations: [Describe any costs to the participants or amount and method of compensation that will be given to them. Describe how you arrived at the amount and the plan for compensation; if it will be prorated, please provide the breakdown. Experimental or extra course credit should be considered an economic consideration and included in this section. Indicate when participants will receive compensation.]

No financial compensation will be provided to each participant. But the solicited individuals can decide to be entered into a lottery for a gift card of 20 dollars. The lottery will be kept as a separate survey that will not affect the data collected.

Data Safety Monitoring:

See attached.

Privacy/Confidentiality Part 1:

The study will be conducted over a web-based survey, therefore individual data will not be distinguishable. Once data is transfer to a UConn computer access will be restricted to the PI and the student investigator.

Privacy/Confidentiality Part 2: Complete the Data Security Assessment Form:.

Informed Consent

The study will be conducted via a web based survey where risks are minimized and participants provide consent by participating. Note we are requesting a waiver on documentation of consent as this will be the only record of identifiable information.

Capacity to Consent:

Since the population is restricted to UConn students we assume all individuals possess capacity for consent.

Parent/Guardian Permission and Assent:

N/A

Documentation of Consent:

We are requesting a **waiver of documentation of consent** due to minimal risks and the fact that consent will be the only storage of identifiable information.N/A

Waiver or Alteration of Consent:

Waiver of *signed* consent (i.e. participants give consent only after reading an information sheet):

- Why is the study considered to be minimal risk?

The study is a web based study where the data of an individual will not be distinguishable. No personal identifiable information will be stored so privacy risk is minimal.

- Does a breach of confidentiality constitute the principal risk to participants? Relate this to the risks associated with a breach of confidentiality and indicate how risks will be minimized because of the waiver of signed consent.

  Yes. This data will collect privacy related information. Linking this information to names will increase the risk of collecting this information.
- Would the signed consent form be the only record linking the participant to the research? Relate this to the procedures to protect privacy/confidentiality.

  Yes
- Does the research include any activities that would require signed consent in a non-research setting? For example, in non-research settings, normally there is no requirement for written consent for completion of questionnaires.

  No

References / Literature Review:

Consent Form for Participation in a Research Study

UCONN
UNIVERSITY OF CONNECTICUT

Principal Investigator: Benjamin Fuller
Student Researcher: Shreya Varshney
Study Title: The Online Presence of UConn Students

You are invited to participate in a research study to observe the online presence of UConn students. You are being asked to participate because you are a UConn student. To participate you must be at least 18 years of age and a UConn student. The purpose of this study is to determine what the online presence is of a UConn student. If you agree to take part in this study you will be asked to complete a 10-question survey that will take approximately 5-10 minutes to answer. The questions asked will pertain to your online activity, namely activity on social media and online shopping. There are minimal risks associated with this research study: a minor inconvenience may be the time it takes to complete the study.

You may not directly benefit from this research however, we hope that your participation in the study will help in enlightening the UConn community about the online presence of its members.

There will be no compensation for participation but should you wish to you will be entered in to a lottery-based drawing to win a gift card. Participation in this study will not cost you any monetary expenses.

The following procedures will be used to protect the confidentiality of your data. The researchers will keep all study records (including any codes to your data) locked in a secure location. Your responses will be marked with a code corresponding to the order in which you took the survey. No additional identifying information beyond this code and your responses will be kept. All electronic files (e.g., database, spreadsheet, etc.) containing identifiable information will be password protected. Any computer hosting such files will also have password protection to prevent access by unauthorized users. Only the members of the research staff will have access to the passwords. Data that will be shared with others will be coded as described above.

At the conclusion of this study, the researchers may publish their findings. Information will be presented in summary format and you will not be identified in any publications or presentations. We will do our best to protect the confidentiality of the information we gather from you but we cannot guarantee 100% confidentiality. Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties. You should also know that the UConn Institutional Review Board (IRB) and Research Compliance Services may inspect study records as part of its auditing program, but these reviews will only focus on the researchers and not on your responses or involvement. The IRB is a group of people who review research studies to protect the rights and welfare of research participants. Participation in this study is purely optional. Should you wish to not answer a question or should wish to leave the study at any time you may do so without any repercussions to you or you person. Take as long as you like before you make a decision. We will be happy to answer any question you have about this study. If you have further questions about this study or if you have a research-related

problem, you may contact Shreya Varshney at shreya.varshney@uconn.edu Or Benjamin Fuller at Benjamin.fuller@uconn.edu. If you have any questions concerning your rights as a research participant, you may contact the University of Connecticut Institutional Review Board (IRB) at 860-486-8802. Taking this survey serves as your consent to have your data used as part of the research.

Invitation Letter

Hello (faculty member),
I am conducting a research study to observe the online presence of UConn students. This study will ask the students to take a 10 question survey on their online presence. There is minimal risk to the students and no harm is intended to the participants. Please forward to the following, non italicized portion to your students. If you have questions about the survey you may contact me at Shreya.varshey@uconn.edu or my faculty advisor, Benjamin Fuller at Benjamin.fuller@uconn.edu or the UConn IRB at 860-486-8802.
Hello Student,
You are invited to participate in a research study to observe the online presence of UConn students. You are being asked to participate because you are a UConn student. To participate you must be at least 18 years of age and a UConn student. The purpose of this study is to determine what the online presence is of a UConn student. If you agree to take part in this study you will be asked to complete a 10-question survey that will take approximately 5-10 minutes to answer. The questions asked will pertain to your online activity, namely activity on social media and online shopping. There are minimal risks associated with this research study: a minor inconvenience may be the time it takes to complete the study.
You may not directly benefit from this research however, we hope that your participation in the study will help in enlightening the UConn community about the online presence of its members. There will be no compensation for participation but should you wish to you will be entered in to a lottery-based drawing to win a gift card. Participation in this study will not cost you any monetary expenses.
The following procedures will be used to protect the confidentiality of your data. The researchers will keep all study records (including any codes to your data) locked in a secure location. Your responses will be marked with a code corresponding to the order in which you took the survey. No additional identifying information beyond this code and your responses will be kept. All electronic files (e.g., database, spreadsheet, etc.) containing identifiable information will be password protected. Any computer hosting such files will also have password protection to prevent access by unauthorized users. Only the members of the research staff will have access to the passwords. Data that will be shared with others will be coded as described above.
At the conclusion of this study, the researchers may publish their findings. Information will be presented in summary format and you will not be identified in any publications or presentations. We will do our best to protect the confidentiality of the information we gather from you but we cannot guarantee 100% confidentiality. Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties. You should also know that the UConn Institutional Review Board (IRB) and Research Compliance Services may inspect study records as part of its auditing program, but these reviews will only focus on the researchers and not on your responses or involvement. The IRB is a group of people who review research studies to protect the rights and welfare of research participants. Participation in this study is purely optional. Should you wish to not answer a question or should wish to leave the study at any time you may do so without any repercussions to you or you person. Take as long as you like before you make a decision. We will be happy to answer any question you have about this study. If you have further questions about this study or if you have a research-related problem, you may contact Shreya Varshney at shreya.varshney@uconn.edu Or Benjamin Fuller

at Benjamin.fuller@uconn.edu. If you have any questions concerning your rights as a research participant, you may contact the University of Connecticut Institutional Review Board (IRB) at 860-486-8802. Taking this survey serves as your consent to have your data used as part of the research.
This is the link to the survey (link to the survey).
Should you wish to enter in the drawing for the gift card please go to this link (link for gift card drawing).
Thank you,
Shreya Varshney
If you have any questions about the study please contact me at shreya.varshney@uconn.edu.
Thank you,
Shreya Varshney

Data Security Assessment Form