

Generational Social Media Privacy Perceptions

(Word Count: 3111 words)

1. Introduction

The purpose of this paper is to evaluate the importance of privacy in contemporary life. Technology has brought unquantifiable benefits to everyday people allowing us to receive information whenever we want, record whatever we want, and communicate with whoever we want. On the other hand, there are some major implications in the background of progress that is heavily under-discussed by society. A simple question like who knows us best could have been answered with our best friend or a family member in simpler times. However, the answer today is indisputably our technology. Our technology knows when our birthday is, what we are scheduled to do, where we are at all times, and essentially whatever information we are willing to feed it. Upon realizing this, it is evident that our idea of privacy is degrading before our eyes and we are accepting it as the direction of progress.

This paper will help determine if the direction of the future is what users of technology truly value. This information can prove to be vital in ensuring that future technology benefits everyone involved in it. The motivation behind such a study stems from the potential for improvement in the design philosophy of online security.

1.1 Arguments

The Internet environment has developed with the intention of processing requests faster, storing masses of information, creating user-friendly and appealing sites, etc. Among these positives has always been the consequence of surveillance. One of the biggest

phenomena is the filter bubble caused by personalized search. The filter bubble is best defined as a situation where an Internet user is only given information to reinforce beliefs. According to “Filter Bubbles, Echo Chambers, and Online News Consumption,” the filter bubble may actually introduce opposing views to users, but it also creates ideological segregation (Flaxman 299). Another technological invasion of privacy is video surveillance. In Newark, New Jersey, mass surveillance of the city is put into place and has left all citizens with a sense of fear (Rouse). The common citizens commented on the potential abuse of this system, whereas business owners saw it as free security. In addition, the burden of the privacy issue has been unequally felt. According to “Digital Privacy Is a Class Issue,” targeted advertising affects people of lower socioeconomic class because they rely more heavily on free services (O’Shea). All of these arguments approach the consequences of technology in a different manner, but the result is a negative mindset known as privacy cynicism. Privacy cynicism is defined as the negative mindset characterized by feelings of powerlessness online due to a lack of control in handling personal data (Hoffmann et al. 47). All this shows the trend of where technology is headed, but not all of this progress destroys privacy. Differential privacy is an approach to statistical analysis designed to protect individual information in aggregate studies by adding random noise to a given set (Wood et al. 212). This type of developing methodology is what minimizes the impact that Big Data has on individuals, and it shows that technology does not have to rely on pure data collection. However, the overall research still argues the more prevalent direction of invasive technology.

1.2 Cornerstone Work

“Do Privacy and Security Regulations Need a Status Update? Perspectives from an Intergenerational Survey” is the most foundational work in this study. It addresses the deteriorating value of privacy by analyzing different generations’ valuing of words connoted around privacy through a survey. The study did find that privacy concerns decreased over generations and provided explanations for the effects of the Millennials’ behavior as a result of desensitization from the Internet environment. This work serves as the basis for this study’s methodology as the premises of both studies are similar.

1.3 Gap in Knowledge

The specifics of this study will focus on the role privacy plays within user experience for social media. This gap came from various sources focusing on user opinion, cybersecurity developments, privacy law, etc. None of them focuses on the privacy policy and user experience, and that is what this study focuses on. A basic assumption of this study is that people have a basic understanding of the utilities of social media and have a vested interest in it. The research question will be to what extent does privacy perceived differ by social media users in [REDACTED]? I hypothesize that privacy perceptions vary much greater in younger generations than older ones and overall privacy concerns are low.

2. Privacy in Philosophy and Law

According to the Stanford article “Privacy,” the concept of privacy has origins in Greek philosophy beginning with Aristotle. The distinction between the social spheres of work and voting and life at home are what defined the early conception of private and public life (DeCew). Since then, privacy has served a background role throughout many philosophical, political, and legal discussions from the Enlightenment era to modern times.

According to Duke article “Philosophical Views on the Value of Privacy,” privacy would not be upheld as a natural right (Negley 319). Privacy has always served as a means rather than an end as philosophers only see privacy as that which empowers individuals to choose for themselves. However, the practical need for privacy is apparent, especially when technology continues to develop more intrusive by design. There are two main schools of thought on privacy: reductionism and coherentism (DeCew). The former agrees with Negley’s view, but the former supports the idea that privacy has inherent value, especially in the application.

Within a political lens, privacy is an implicit right. During the Enlightenment era of philosophy, privacy would often be discussed through property rights. According to peer-reviewed article “Decrypting the Fourth Amendment: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Encryption Technologies,” the US Constitution has the 4th amendment to protect against searches and seizures, which is slowly being evolved for online information in regards to the encryption process (Gliksberg 771). The US Supreme Court case of *Griswold v. Connecticut* even created a “constitutional” right to privacy but under the terms of sexual relations and marriage (DeCew). With all of this in mind, it is clear that the right to privacy is slowly progressing towards an explicit right over time.

2.1 Users

The most well-researched aspect of online privacy would be users: behaviors, habits, and mindsets. The reason is to meet the demands and concerns of the true benefitters of technology.

According to a peer-reviewed study “Do Privacy and Security Regulations Need a Status Update? Perspectives from an Intergenerational Survey,” Millennial generations are less concerned about health information privacy than older generations due to desensitization from the Internet (Pereira et al. 8). This finding proves the degrading concept of informational privacy and the decreasing concept of personally identifiable information. Another study is focused on the differing privacy views based on sex within specifically Snapchat. According to “Millennials Sex Differences on Snapchat Perceived Privacy,” the study concluded that men and women do not differ significantly in privacy concerns for the case of Snapchat, but both sexes show privacy as an important concern (Rauzzino and Juan 113). On the other hand, privacy could be argued as a class issue. People of lower socioeconomic background rely more heavily on free services, and they become exploited as a product as a result (O’Shea). Data is incredibly valuable to the monolith of the advertising industry. Finally, the concept of privacy cynicism is the consequence of these poor privacy practices. According to “Privacy Cynicism: A New Approach to the Privacy Paradox,” users express concerns over personal information and express no behaviors to protect themselves, thus creating the privacy paradox (Hoffmann et al. 46). Privacy cynicism is the negative mindset that comes from the desensitization of the online experience in regards to privacy. Hoffmann expresses the need for the government to hold business accountable as this mindset leads to distrust in society.

Altogether, these studies have established crucial groundwork on what technology has done to users. The gap needed to further these studies is that of the relationship between

privacy and users. Understanding the concerns of users will allow for the future to encompass all that benefits all.

3. Methodology

3.1 Research Design

The primary purpose of this method was to determine potential gaps in the perceptions of privacy on social media platforms and the overall user experience. The question that guides this study is, to what extent does privacy perceived differ by social media users in [REDACTED]? The hypothesis was that privacy perceptions vary much greater in younger generations than older ones and overall privacy concerns are low between both groups. The method used was a cross-sectional, close-ended questionnaire about social media, privacy policy, and user experience over on Google Forms. There were two sections with Yes or No questions and scale questions to ensure quantifiable results. The scale used was a 5 point Likert scale for frequency or agreement. The Yes or No questions will target the user's understanding and behavior, while the scale questions try to determine the user experience. The reason this method is the best one is that it allows for a greater quantity of participants and allows quantifiable results to determine numeric gaps. It is superior in accomplishing the primary goals as opposed to interviews, which would grant in-depth individual insight but at the cost of understanding the general population.

3.1 Participants

A stratified sample was collected with a teacher set of 20 participants and a student set of 100 participants, all randomly picked. These groups were decided in order to compare for the purposes of the research question in comparing adult and adolescent behavior. In

addition, they are the most feasible populations. Additionally, the participants need to have some form of social media for their responses to be relevant. Social media is defined as online services that allow users to create and share content and interact with each other. Popular examples include Snapchat, Instagram, Twitter, and Facebook.

3.2 Data Collection

The questionnaire had been conducted on Google forms. For the privacy of participants, all data has been made anonymous and a small degree of differential privacy will be applied. Specifically, a random 5% of data will be added to each set using a coin flip and random number generator. These random answers are known as noise. The idea is that the aggregate results are similar enough for statistical significance, but this random noise will protect individual responses in the aggregate.

3.3 Instrument

The survey questions asked followed the format below:

How often do you use social media daily? 0-2 hrs, 2-4 hrs, 4-6 hrs, 6-8 hrs, 8+hrs

To what extent do you feel that your information is safe? 5pt

How important do you think privacy is for social media? 5pt

How satisfied are you with the updates and features on social media? 5pt

How much information do you think social media companies need to collect? 5pt

How comfortable are you with the information you've put online? 5pt

Are you aware that your (location/photos/searches/purchases/name) is being tracked/saved?

Y/N

Have you read any of the privacy policies? Y/N

Do you keep your account private? Y/N

Have you or someone you know ever been hacked? Y/N

Are you concerned about being hacked? Y/N

Do you use a strong password(8 char, num, sym)? Y/N

Do you use different passwords? Y/N

Do you use any extensions to block ads? Y/N

Do you use any extensions to block trackers/encrypt yourself? Y/N

Do you use a VPN? Y/N

3.4 Procedures

1. Creating the survey on the forms. The idea is to make a short and simple questionnaire for participants. The Y/N questions and 5pt questions should be grouped together.
2. Determine the participants. The sample used for this is 20 teachers and 100 students. For the purposes of random sampling, grade levels do not matter and the participants will be chosen simply by random encounters throughout the day.
3. Finally, the data needs to be organized into some form of spreadsheet to be useful. Once the data is collected and formatted, it must be adjusted in accordance with the differential privacy procedure shown above. Essentially, 5 student responses and 1 teacher response will be altered using a coin flip test. Once the data is modified, then the analysis begins.

3.5 Analysis

The analysis afterwards had calculated percentages for the Yes and No questions. The scaled questions have the average and variance of the student and teacher sets taken to evaluate gaps in privacy perceptions.

The equations are as follows:

$$\mu = \frac{\sum(N)}{|N|} \quad \text{where } \mu \text{ is the mean and } N \text{ is the whole data set}$$

$$\sigma^2 = \frac{\sum(x-\mu)^2}{|N|} \quad \text{where } \sigma^2 \text{ is the variance and } x \text{ represents individual data points}$$

Depending on which average is higher, I assessed how high privacy is valued and by which group. The purpose of calculating the variance in each group is to determine whether or not the groups agree with each other. In addition, the averages can be compared to a theoretical medium of 2.5 for each question to determine the general attitudes held towards understanding the privacy policy and how the participants perceive it. With all of these calculations, the following questions were answered-

- Which group values privacy more?
- Is there a significant gap between the two groups?
- Is there a significant gap within each group?
- What percent of each group understands online data collection?
- What percent of each group uses security measures?
- How concerned are the groups on privacy issues?

4. Conclusion

In conclusion, this disproves of my hypothesis about the behaviors of adults and adolescents; however, my hypothesis on the general values were true. All this signifies the status quo still supports the jaded idea of privacy between adolescents and adults. My original thinking was that these groups would not be well informed on privacy issues because it is not a mainstream issue. However, the data shows a strong support of privacy and awareness of online tracking. It is apparent now that this new generation of adolescents and adults understand the Internet a lot better than predicted, likely due to growing online culture and the spread of technology over time. Simply put, we are connected now on the cloud more than ever, and many have an understanding of what happens online. My values were correct when I predicted that adults have a higher average and lower variance, while students had the lower average and higher variance. In addition, there was a minimal gap between the two sets as well. In terms of the habits, it seems that despite the support of privacy, there is a lack of action on the part of both groups. The password habits of both groups show that a majority do maintain strong actions on this part. In addition, a majority also keeps social media accounts private. However, a majority of both groups do not take any further action in terms of browser extensions and VPNs in order to further encrypt their experience. Interestingly enough, while both groups expressed awareness of online tracking, a majority of both groups do not read the privacy policies of their apps. Altogether, privacy is something that many are aware of and support, but not enough methods to protect is known by the public.

4.1. Analysis

Student Set:

```
C:\Users\danny\Documents\Programs\Research\DataAnalysis.exe
*****
Q1 Mean: 4.07143
Q2 Mean: 3.09524
Q3 Mean: 3.17619
Q4 Mean: 2.85238
Q5 Mean: 3.62857
Aggregate Mean: 16.8238
Q1 Variance: 1.19014
Q2 Variance: 1.60998
Q3 Variance: 1.30705
Q4 Variance: 1.69726
Q5 Variance: 0.0118369
Set Variance: 9.54515
*****
Process returned 0 (0x0)   execution time : 0.031 s
Press any key to continue.
```

Teacher Set:

```
C:\Users\danny\Documents\Programs\Research\DataAnalysis.exe
*****
Q1 Mean: 4.04762
Q2 Mean: 3.2381
Q3 Mean: 3.28571
Q4 Mean: 2.95238
Q5 Mean: 3.66667
Aggregate Mean: 17.1905
Q1 Variance: 1.47392
Q2 Variance: 1.03855
Q3 Variance: 0.680272
Q4 Variance: 1.56916
Q5 Variance: 0.126984
Set Variance: 6.72562
*****
Process returned 0 (0x0)   execution time : 0.022 s
Press any key to continue.
```

A C++ program was created in order to calculate the mean and variance of the data using the formulas in the methodology. The averages of responses to each of the scale questions were calculated and then added together to determine an aggregate mean. In other words, the individual question means represent the average response to each question being from 1 to 5 and the aggregate mean is a value that shows the average sum of all questions of this section being from 5 to 25. Higher values in the mean indicate higher privacy values and perception due to the way the questions and responses were structured. The question variance demonstrates how much the individual responses differ from each other in each set and the set variance is how much the sum of the responses differ. In other words, a higher value indicates that the responses differed more and a lower value indicates that the responses were more similar. Finally, the section with Y/N questions was analyzed using the bar charts of Google Forms and the percentages were compared. The most significant were charts that demonstrated majorities instead of mere pluralities, shown in the examples. With all of this data, the questions from the methodology section can be answered.

- Which group values privacy more?
 - Teachers
- Is there a significant gap between the two groups?
 - No, similar aggregate mean (difference of .37)
- Is there a significant gap within each group?
 - No, variance was around 1 or less.
- What percent of each group understands online data collection?

- A majority of each group (<50%)
- What percent of each group uses security measures?
 - Both focus on passwords(<80%), but a majority (<50%) do not use VPNs or extensions
- How concerned are the groups on privacy issues?
 - They value privacy (~50%) for both groups, but they are not concerned about security or being hacked or information they've put online (~3 average response)

4.2. Reflection

The major limitations of this project were the small number of responses from teachers, the fact [REDACTED] High is a Title I school, and questionnaire structure. Teachers are just a smaller population at school so the adult set is much smaller to analyze and may be more extreme than it actually is. The fact that [REDACTED] High is a Title I school shows that there are many students from low income families, so it is possible that technology access is an issue for them. Finally, the questionnaire structure did provide limited choice in response to more easily analyze it. Due to this, there is a lack of understanding of nuance between what users truly perceive as privacy on social media. The next steps of this research should focus on online culture in terms of why many users are so aware of tracking yet not aware of methods to better protect themselves. It could be a qualitative interview in order to capture what individual experiences say about the entire online experience for many. Alternatively, it could still be a quantitative survey that focuses on where all of this online knowledge is

focused. Another way to expand on the research of our heavy tech-based culture is to see where users and creators would like to be headed with it in the future. The possibilities to research our relationship with the machines we use are limitless.

Works Cited

DeCew, Judith. "Privacy." Stanford Encyclopedia of Philosophy, Stanford University, 18 Jan.

2018, <https://plato.stanford.edu/entries/privacy/>.

Flaxman, Seth, et al. "Filter Bubbles, Echo Chambers, and Online News Consumption." Public

Opinion Quarterly, vol. 80, Mar. 2016, pp. 298–320.

<http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=114678730&site=ehost-live>.

Gliksberg, Candice. "Decrypting the Fourth Amendment: Applying Fourth Amendment

Principles to Evolving Privacy Expectations in Encryption Technologies." Loyola of Los

Angeles Law Review, vol. 50, no. 4, June 2019, pp. 765–792.

<http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=135551230&site=ehost-live>.

Hoffmann, Christian Pieter, et al. "Privacy Cynicism: A New Approach to the Privacy Paradox." Cyberpsychology, vol. 10, no. 4, Dec. 2016, pp. 43–60.

Cyberpsychology, vol. 10, no. 4, Dec. 2016, pp. 43–60.

<http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=120586469&site=ehost-live>.

Negley, Glenn. "Philosophical Views on the Value of Privacy." Law and Contemporary

Problems. 1966, pp. 319–325.

<https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3111&context=lcp>.

O'Shea, Lizzie. "Digital Privacy Is a Class Issue." *The New Republic*, 30 May 2019,

<https://newrepublic.com/article/154026/digital-privacy-class-issue>.

Pereira, Stacey, et al. "Do Privacy and Security Regulations Need a Status Update? Perspectives from an Intergenerational Survey." *PLoS ONE*, vol. 12, no. 9, Sept. 2017, pp. 1–11.

<http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=125226550&site=ehost-live>.

Rauzzino, Antonietta, and Juan C. Correa. "Millennials Sex Differences on Snapchat Perceived Privacy." *Suma Psicológica*, vol. 24, no. 2, July 2017, pp. 129–134.

<http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=125578782&site=ehost-live>.

Rouse, Karen. "Newark Police Camera System Relies On Residents, Stirring Privacy Concerns."

NPR. 26 May 2018. NPR. 23 Sept. 2019,

<https://www.npr.org/2018/05/26/614387170/newark-police-camera-system-relies-on-residents-stirring-privacy-concerns>>.

Wood, Alexandra, et al. "Differential Privacy: A Primer for a Non-Technical Audience."

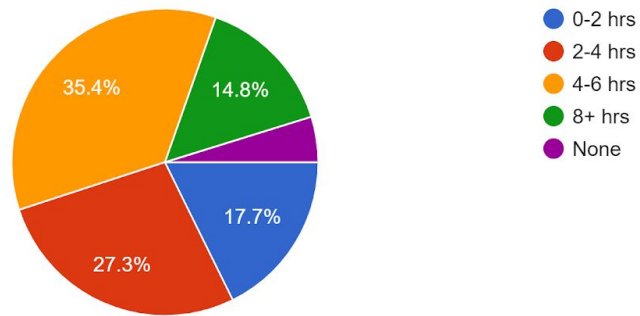
Vanderbilt Journal of Entertainment & Technology Law, vol. 21, no. 1, Sept. 2018, pp. 209–276.

<http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=133592662&site=ehost-live>.

Appendix-

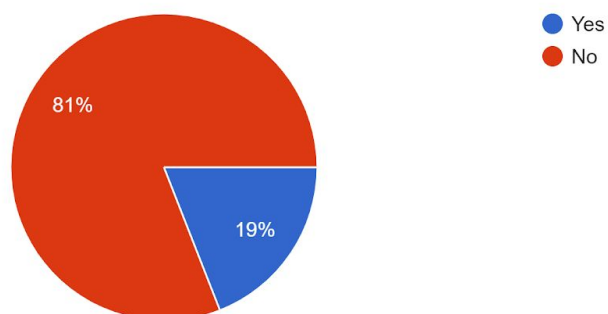
Student Survey Results:

How often do you use social media daily?
209 responses



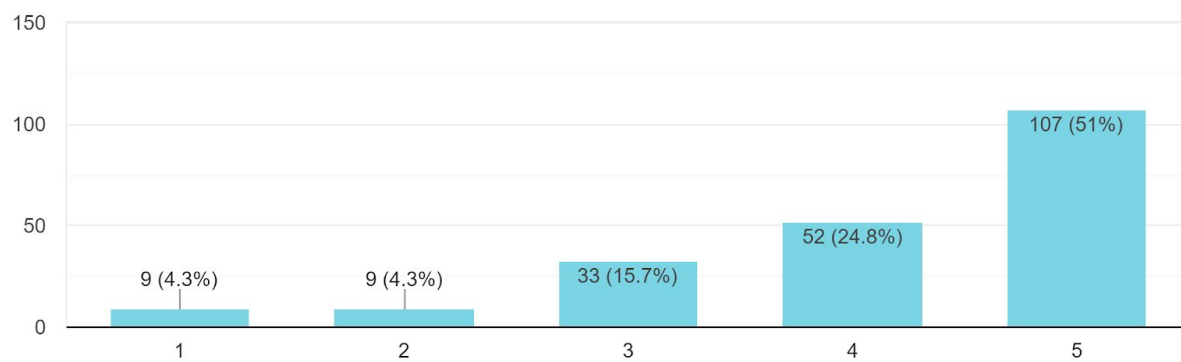
Do you use a VPN?

21 responses



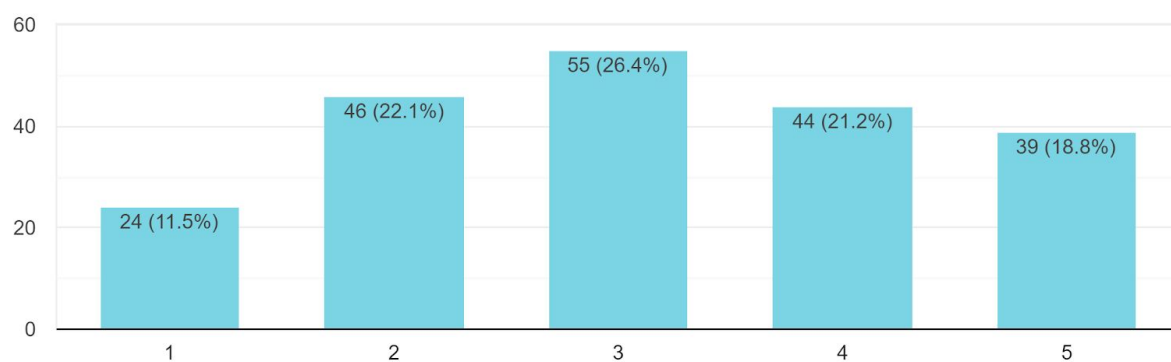
How important do you think privacy is for social media?

210 responses



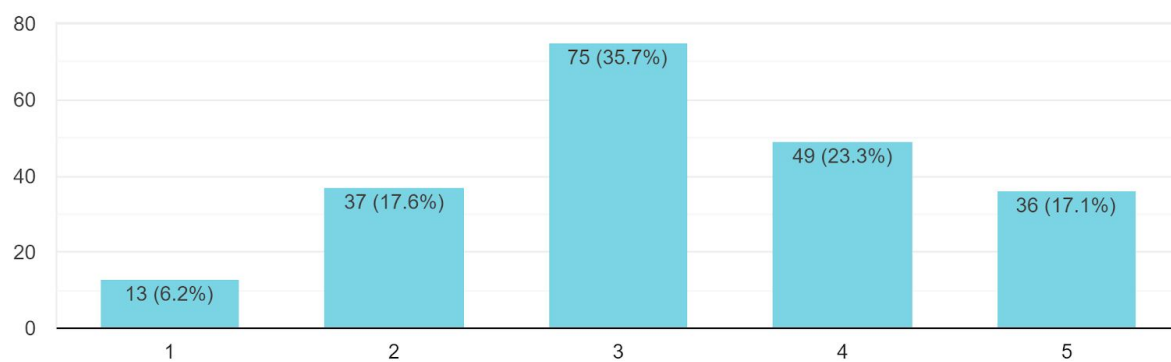
How concerned are you about being hacked?

208 responses



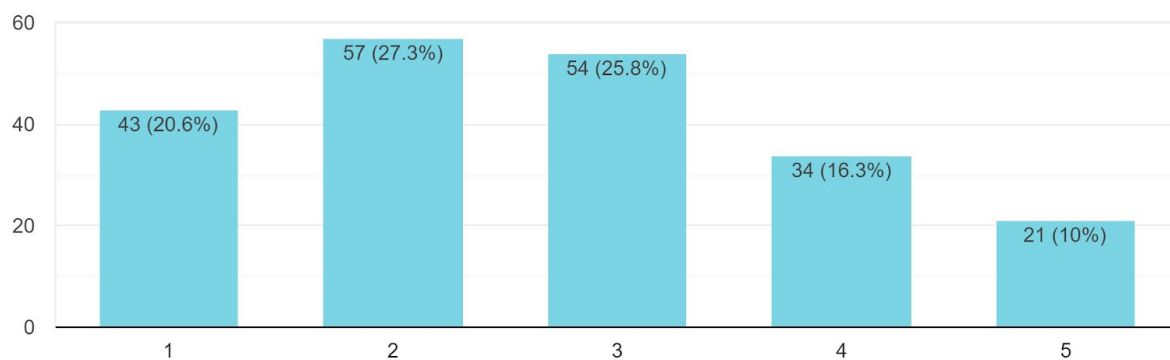
How worried are you about the lack of privacy or security updates?

210 responses



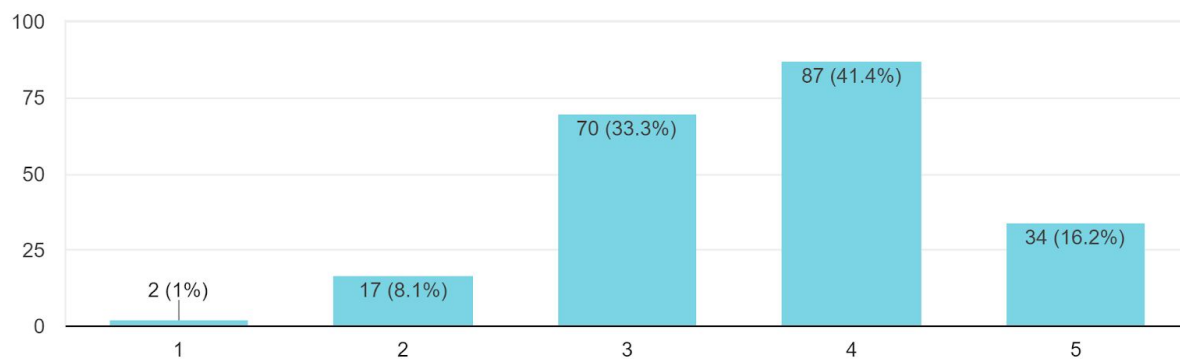
How concerned are you with all of the information you've put online?

209 responses



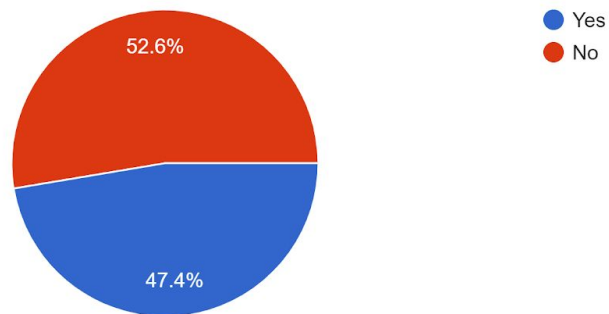
How much information should you give up on social media?

210 responses



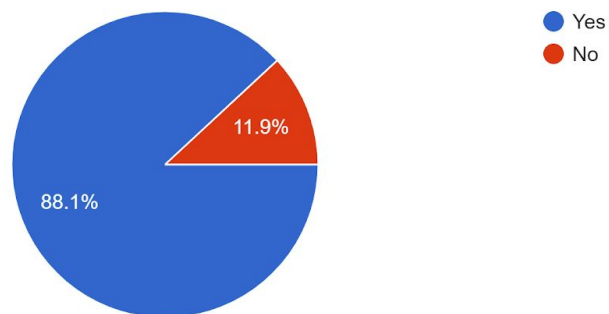
Have you read any of the privacy policies?

209 responses



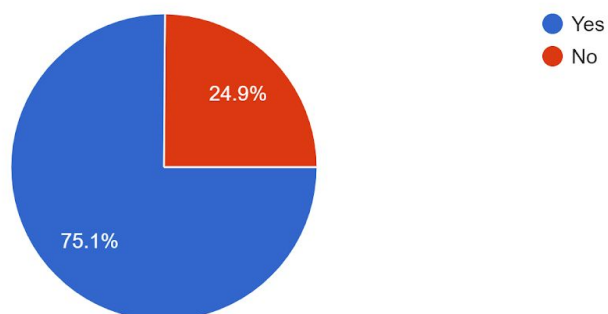
Are you aware that your location, photos, searches, purchases, and name are being tracked/saved?

210 responses



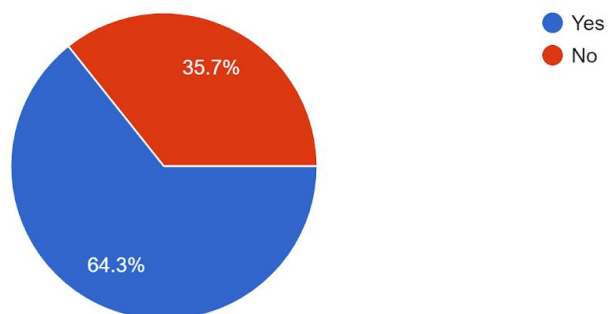
Do you keep your account(s) private?

209 responses



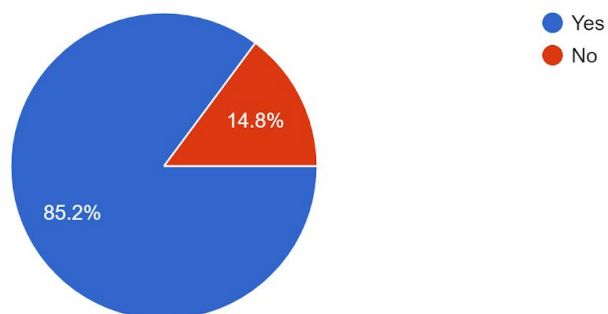
Have you or someone you know personally ever been hacked?

210 responses



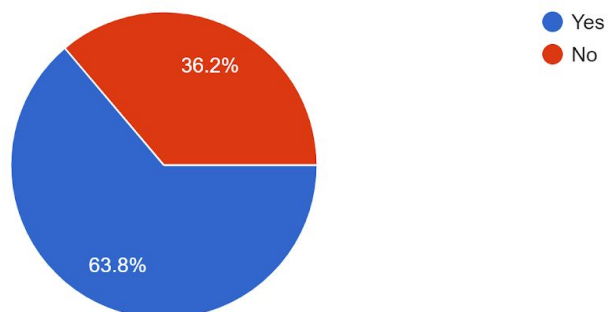
Do you use a strong password (includes 8 characters, CAPS, numbers, symbols)?

209 responses



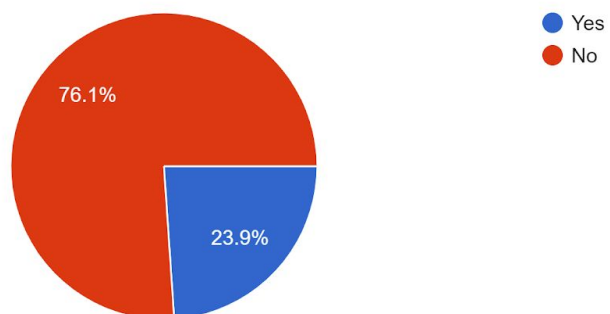
Do you use different passwords?

210 responses



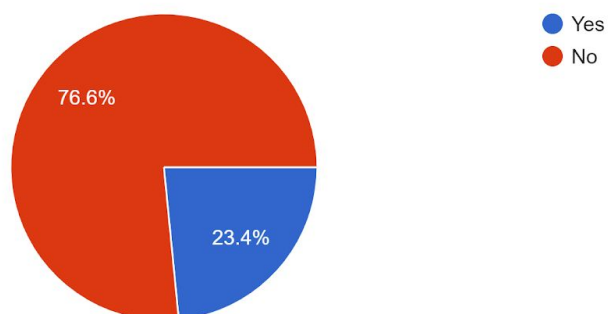
Do you use any extensions to block ads?

209 responses



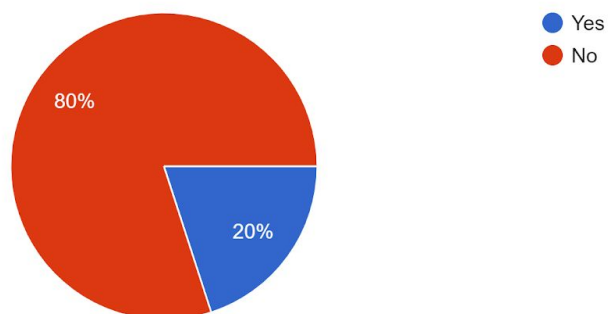
Do you use any extensions to block trackers/encrypt yourself?

209 responses



Do you use a VPN?

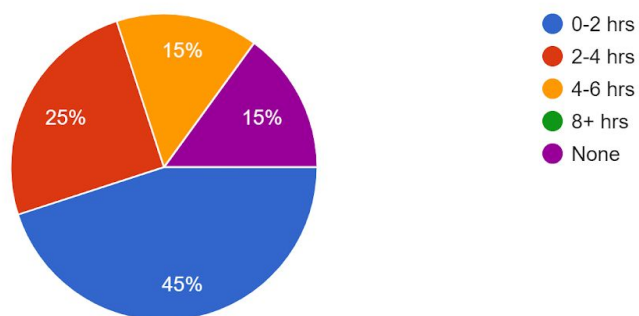
210 responses



Teacher Survey Results:

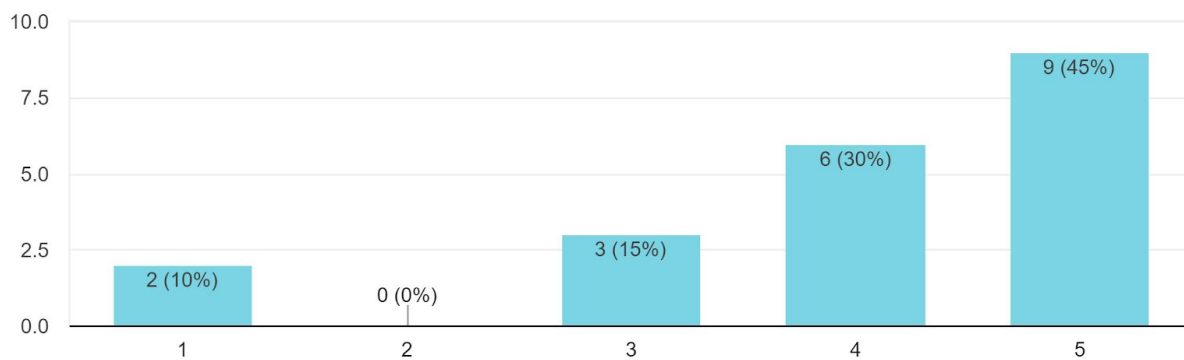
How often do you use social media daily?

20 responses



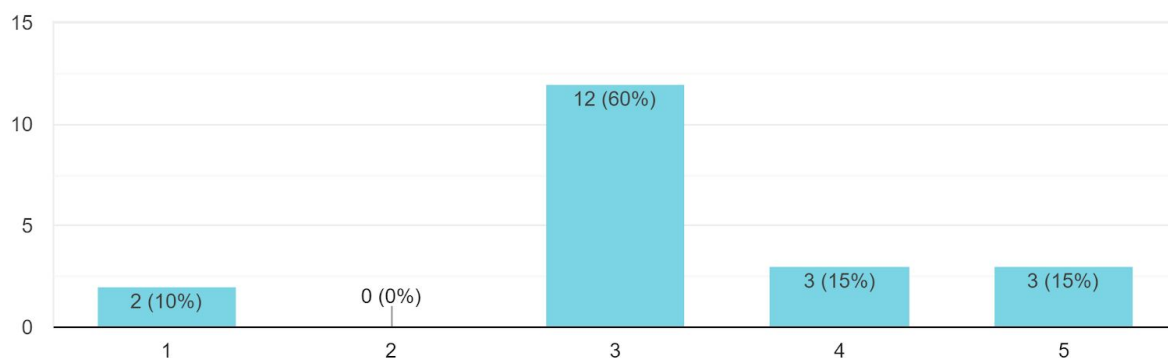
How important do you think privacy is for social media?

20 responses



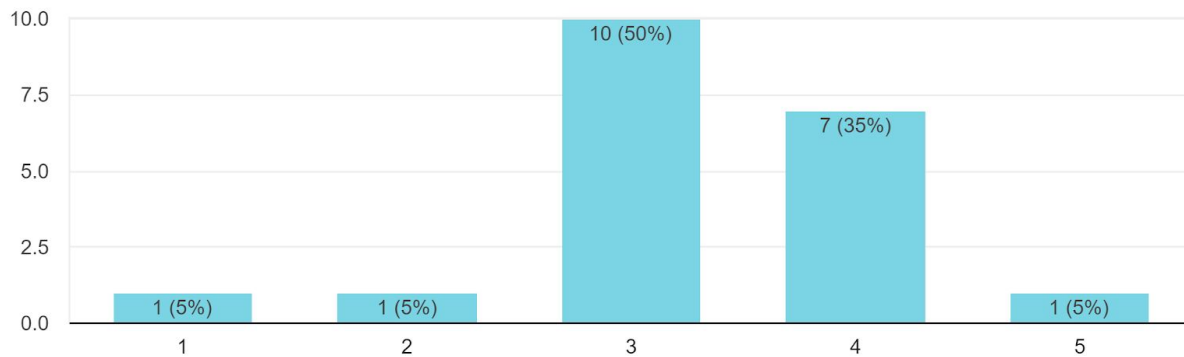
How concerned are you about being hacked?

20 responses



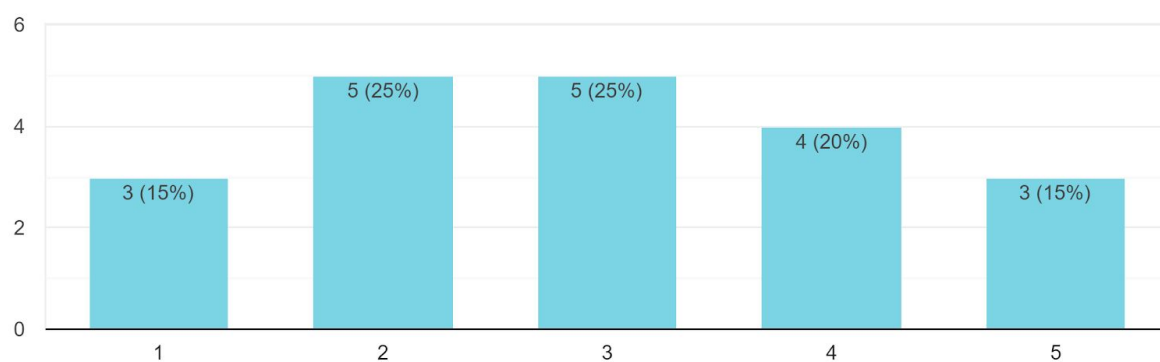
How worried are you about the lack of privacy or security updates?

20 responses



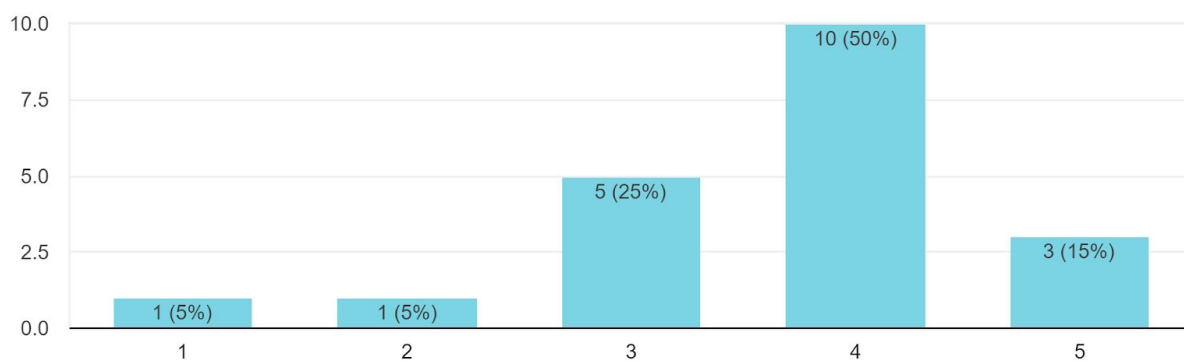
How concerned are you with all of the information you've put online?

20 responses



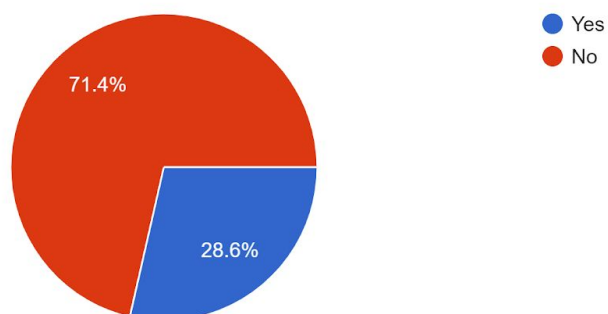
How much information should you give up on social media?

20 responses



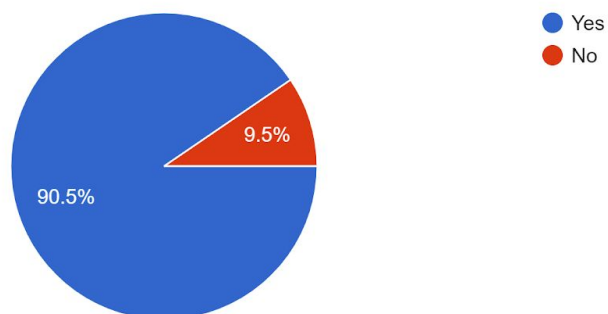
Have you read any of the privacy policies?

21 responses



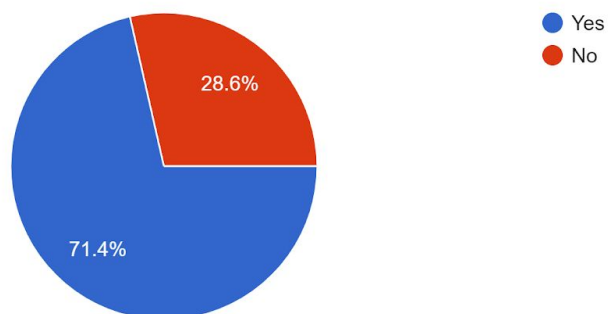
Are you aware that your location, photos, searches, purchases, and name is being tracked/saved?

21 responses



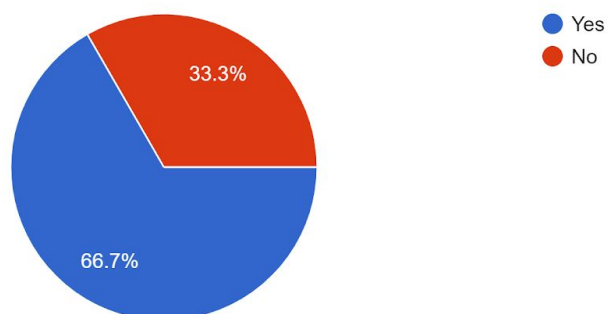
Do you keep your account(s) private?

21 responses



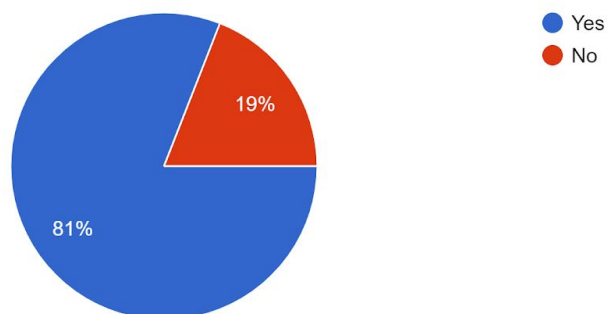
Have you or someone you know personally ever been hacked?

21 responses



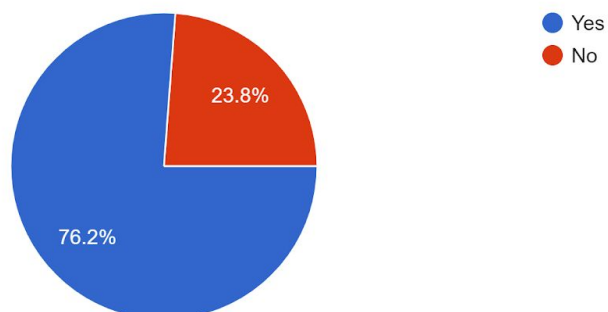
Do you use a strong password (includes 8 characters, CAPS, numbers, symbols)?

21 responses



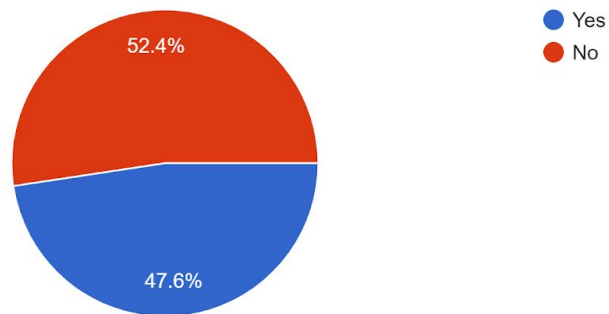
Do you use different passwords?

21 responses



Do you use any extensions to block ads?

21 responses



Do you use any extensions to block trackers/encrypt yourself?

21 responses

