AI cybersecurity: Advancing understanding of public opinion to create effective public policy

Charles W. Milam, *Middle Georgia State University, dr.charleswesleymilam@gmail.com*

Abstract

This paper investigates the development of opinions on artificial intelligence (AI) from the perspective of how we learn about AI and how often we interact with AI technology and media. AI awareness is nearly ubiquitous, far beyond the explanation of AI media presence since 2022 when ChatGPT became available to the public. However, since 2022 distrust in AI technologies has risen sharply in public opinion, spawning the first official AI regulations in the EU and US. These regulations have unintentionally shifted the cybersecurity advantage firmly to the cybercriminal. With each new incarnation of generative AI (GenAI) capability, a corresponding advancement of GenAI cybercrime tools evolves faster than cyberdefender tools. A better understanding of AI opinion development will hopefully lead to regulatory revisions, rebalance cybersecurity outcomes, and increase AI acceptance by the public.

Keywords: artificial intelligence, AI cybersecurity, AI acceptance, AI opinion, AI policy

Introduction

Artificial intelligence (AI) is a topic of near-ubiquitous interest in the public mind (Hobden & Begaj, 2023; Faverio & Tyson, 2023; O'Shaughnessy et al., 2023). In the US and UK, ongoing studies from 2021 to 2023 show that overall public awareness of AI and machine learning (ML) rose to greater than ninety percent of respondents in random population samplings (Hobden & Begaj, 2023; Faverio & Tyson, 2023). UK researchers credit the release of OpenAI's ChatGPT and the media coverage it received as fuel for the increased awareness (Hobden & Begaj, 2023). However, these studies also show that before ChatGPT's release in late 2022, public awareness in random population sampling exceeded eighty-five percent (Hobden & Begaj, 2023; Faverio & Tyson, 2023). Market researchers use a seventy-five percent benchmark for brand awareness in populations of potential users as a guide for market share calculations, which makes the awareness of AI in random populations before the release of ChatGPT's media firestorm a significant factor in AI acceptance research (Weiner, 2024; Hobden & Begaj, 2023; Faverio & Tyson, 2023).

In addition to overall awareness, research also suggests that as awareness has risen, so has an unfavorable public opinion of AI (Hobden & Begaj, 2023; Faverio & Tyson, 2023; O'Shaughnessy et al., 2023). In 2023, the White House released Executive Order 144110, and in 2024, the EU AI Act went into effect, representing the first incarnations of AI regulatory efforts in the US and EU (Waller, 2024; Chapman, 2023). While the US's EO only applies to government agencies and contracting partners in AI use, the EU AI Act amended the 2018 EU GDPR with the same application to any entity with access to EU markets and outlining harsh penalties for violations (Hickman et al., 2024; Waller, 2024; Chapman, 2023). Public distrust is driving the expansion of government regulatory efforts that slow the development and

deployment of AI cybersecurity technologies. While experts and the public do generally agree that careful development of AI is necessary to ensure that AI systems are safe, do not operate with cultural or gender bias, and protect data privacy, the delays in creating use consensus and favorable public opinion have critically imbalanced cybersecurity (O'Shaughnessy et al., 2023; Zarina et al., 2020).

OpenAI's generative AI (GenAI) platform, ChatGPT Chatbot, debuted in November of 2022, and by the summer of 2023, two subscription-based GenAI cybercrime tools, WormGPT and FraudGPT, appeared on the dark web (Gupta et al., 2023; Page, 2023). As subscription-based platforms, the developers of these and similar tools have enabled sophistication not previously found in most cybercrime actors, shifting cybersecurity paradigms (Mohamed, 2023; Liu et al., 2023). As GenAI capabilities and derivative technologies appear, cyberdefenders are falling behind cybercriminals at an alarming pace, with researchers suggesting that as much as 10% of global GDP will be at risk by 2030 and with cybercrime already exceeding the cost of all natural disasters annually (Fleck, 2024). It is imperative that technology leaders better understand the root cause of public distrust in AI technologies to develop effective strategies to improve public opinion and AI defense capability.

This study will create a prediction model that includes three predictor/independent variables to test two dependent variables. The first predictor variable is Origination, identifying how the respondents' opinion of AI was created. The second two predictor variables are the Frequency of AI USE and Frequency of AI MEDIA interaction. The dependent variables are Positive AI Opinion and Negative AI Opinion. This study will determine which predictor variable is significant in predicting each dependent variable. Consistent with the study's purpose, the researcher will ask the following questions.

RQ1: *Is Origination of Knowledge significant in predicting Positive AI Opinion?*
RQ2: *Is Origination of Knowledge significant in predicting Negative AI Opinion?*
RQ3: *Are Positive AI Opinion and Negative AI Opinion significantly correlated?*
RQ4: *Does Frequency of AI use significantly predict a positive or negative opinion of AI?*
RQ5: *Does Frequency of AI MEDIA Interaction significantly predict a positive or negative opinion of AI?*

The findings of this study will reveal significant relationships in predictor variables (root source of opinion development and frequencies of interactions) to positive or negative opinions of modern AI systems.

Review of Literature

AI public opinion phenomenon

Since 2021, the UK Centre for Data Ethics and Innovation (CDEI) has conducted an annual survey tracking overall public awareness of AI and the public's general view of AI use (Hobden & Begaj, 2023). CDEI found that from 2022 to 2023, overall awareness in UK residents rose from 89% to 95%, while the perceived impact of AI on society showed an increase in negative perceptions from 20% to 25% over the same period (Hobden & Begaj, 2023). In the US, a similar study over time by Pew Research Center found overall awareness of AI to be 90% in 2023, and from 2022 to 2023, respondents' concern/distrust of AI rose from 38% to 52% (Faverio & Tyson, 2023). While most UK and US residents in these studies remained neutral about the effect AI would have on daily life, the trend in both countries shows a rising negative view of AI (Ray, 2024; Faverio & Tyson, 2023).

In the US in 2023, a comparative study of AI opinion between the public and experts represented by surveying master's students found that more educated people generally have a more favorable opinion of AI use than the public (O'Shaughnessy et al., 2023). However, O'Shaughnessy et al. (2023) also found that

while experts were more favorable of AI use overall, both sides showed strong support for careful AI management, yet disagreed strongly on what agency management should take, such as government regulation, company oversight, or other entity oversight. The most common area of concern noted in several studies is the privacy of information, the belief that expanded AI use will be detrimental to personal information privacy (HAI Global AI Index, 2024; Ray, 2024; O'Shaughnessy et al., 2023; Faverio & Tyson, 2023).

In 2024, the HAI Global AI Index reported that the trend of more educated populations favoring AI use and concerns for privacy appeared in the 31 nations surveyed. Studies from the US, UK, and global index also show that many respondents believe they understand what AI is and could explain it to others (Hobden & Begaj, 2023; Faverio & Tyson, 2023). However, less than 40% of respondents tested could correctly identify recent interactions with AI systems (Hobden & Begaj, 2023; Faverio & Tyson, 2023). Respondents also tended to identify AI technology by mode of use, such as robotics, as opposed to software, machine learning, or natural language processing (Placani, 2024; Nader et al., 2022). These misconceptions also cross emerging differences in AI understanding by age or education, as shown by Gartner's CEO survey in 2024, where 64% of CEOs polled identified AI as the most impactful change in their industries over the next three years while less than 3% identified machine learning, automation, or natural language processing as significant (Furlonger, 2024).

AI Regulatory issues

2024, the EU AI Act went into effect, with punitive enforcement set to begin in 2026 (Hickman et al., 2024; Waller, 2024). To differentiate AI from previous or lesser technologies, the EU AI defines AI as a machine-based system that is designed to operate with varying levels of autonomy, may exhibit adaptiveness after deployment, and can infer or make predictions for outputs that influence virtual or physical worlds (Hickman et al., 2024). In addition, the EU AI Act also classifies AI systems based on the potential harm to humans in either virtual or physical space (Hickman et al., 2024; Waller, 2024). The AI Act works with the 2018 EU GDPR, applying to all entities with access to EU markets, with enforcement conducted by member states (Waller, 2024; Chapman, 2023). The penalties for non-compliance will be €35 million or 7% of worldwide annual turnover, whichever is greater, with provisions for further fines of €15 million or 3% of worldwide annual turnover if non-compliance continues (Waller, 2024).

While expected to become a global model for AI regulation, the EU AI Act and GDPR have already caused a pullback in AI investment and deployment as organizations wait to see how EU member states will interpret and enforce the laws (Waller, 2024; Chapman, 2023). Because of the GDPR and similar data privacy laws, such as HIPPA in the US, AI cybersecurity systems have been primarily delegated to outward-facing firewall monitoring to avoid inadvertent scanning or accidental access of protected data that create unacceptable regulatory risks for many organizations (Alrubayyi et al., 2024; Kouroupis, 2024; Chapman, 2023).

Where the EU has set steep financial penalties to discourage violations of the EU AI Act and GDPR in the US, EO 14110 relies on existing fines and penalties for the violation of executive orders in the US code as well as any penalties associated with other data privacy or reporting laws such as HIPPA or the Gramm-Leach-Bliley Act (Chapman, 2023; Gavoor, 2023). EO 14110 has, however, caused a similar stall in AI research and deployment as its requirements are creating barriers to AI market entry for new developers, are proving extremely difficult to coordinate across federal government agencies, could be abruptly altered by judicial review or EO amendment by a new administration, and most significantly because the federal workforce does not have the AI expert talent needed for implementation (Gavoor, 2023).

Media influence on AI opinion

The frequency of AI appearing as the primary subject in media articles started rising exponentially in 2014, with the tone of negative connotation bypassing positive connotation by 2017 (Ouchchy et al., 2020). While most media with AI as the primary subject is presented as neutral or balanced in tone, what is unknown is how frequently any individual media consumer may encounter positive, negative, or neutrally toned articles (O'Shaughnessy et al., 2023; Ouchchy et al., 2020). Following the release of the ChatGPT chatbot in November of 2022, rising public interest in AI has resulted in a substantial increase in AI-related media, disseminated mainly through social media channels (Rachmad, 2024; Faverio & Tyson, 2023). While some research shows that social media dissemination of AI content can result in a favorable AI opinion, critics note that this media consumer group overlaps demographic and education areas known to have more favorable opinions of AI (Li & Zheng, 2024; Rachmad, 2024; O'Shaughnessy et al., 2023).

Given the rise in unfavorable opinions in longitudinal studies in the US and UK, media cultivation theory could interpret the adoption of unfavorable AI opinions since 2022 (Gerbner & Gross, 1976). While cultivation theory focuses on the repeated content of media influencing consumers' opinions, social media expands this indirectly with integrated comment sections (Gunther & Storey, 2003; Gerbner & Gross, 1976). The influence of presumed media influence (IPMI) model suggests that where content may influence one group and have no direct influence on another, the secondary group is influenced by interpersonal communication between the groups (Li et al., 2024; Gunther et al., 2006). Data suggests that as AI is portrayed increasingly unfavorably, this cultivates an unfavorable opinion in less engaged consumers, and observations of discussions reinforce these opinions (Li et al., 2024; O'Shaughnessy et al., 2023; Ouchchy et al., 2020; Gunther et al., 2006; Gerbner & Gross, 1976). Conversely, where AI content is presented more favorably overall, the same pattern of cultivation and reinforcement occurs (HAI Global AI Index, 2024; Li et al., 2024; Lobera et al., 2020; Gunther et al., 2006; Gerbner & Gross, 1976).

AI security risks and emerging threats

Gupta et al. (2023) have found that with each new iteration of capability in OpenAI's GPT, a corresponding advancement occurs in AI cyber-crime tools. After the November 2022 release of ChatGPT 3.5, crime GPT programs appeared on the dark web as subscription-based platforms (Page, 2023). These tools' natural language processing (NPL) interface significantly lowered the skill level required for leveraging AI-powered tools for criminal activities (Djenna et al., 2023; Page, 2023). Researchers have found that the ChatGPT platform itself was exploitable, successfully causing it to bypass its ethical table and act as a platform for unethical activity or reveal its source code (Gupta et al., 2023; Liu et al., 2023).

As the Internet of Things (IoT), Industrial Internet of Things (IIoT), and next-generation networks utilize the automation of AI technologies through advanced sensors needed for high speed and precise control of smart tech, they are increasingly vulnerable to AI cybercrime exploitation (Alrubayyi et al., 2024). Even without regulatory burdens slowing their deployment, the effective deployment of AI security tools for high-speed network monitoring and intrusion detection is cumbersome because of the large amounts of data needed to effectively train the ML models (Arroyo-Figueroa, 2024; Djenna et al., 2023). Before the release of generative AI platforms in 2022, cybersecurity methodology was already falling behind the highly skilled use of AI capable of exploiting the undynamic nature of cybersecurity technology and the delay in security analyst response to intrusion attempts (Sarker et al., 2021).

While threat actors' motivations remain relatively unchanged, such as state actors using it for geopolitical interests or criminals seeking profit, the sophistication and frequency of attacks have risen sharply (Kovaci, 2024; Fleck, 2024). Ransomware, malware, and social engineering attacks have risen sharply as GenAI platform scanning, code generation, image generation, and voice file creation aid the successful delivery of

attack packages (Mohamed, 2023). The cost of this AI-powered cyber-attack escalation is expected to reach 10.5 trillion dollars annually by 2025 and as much as 10% of global GDP by 2030 (Fleck, 2024; Guembe et al., 2022).

Methodology

Instrument

The instrument used in this study is a survey developed by the researcher to assess participants' current opinion of AI technology as a concept for society and participants' opinion of AI technology use when it impacts them personally. The survey also collected data on how participants first learned of AI, how frequently they use AI technologies, and how often they observe media about AI. Survey questions 1-3 obtain demographic information about the respondents. Question 4 identifies the origin of AI awareness as a media or non-media source. Questions 5 and 6 obtain the frequency of AI technology use and AI media consumption data, respectively. Questions 7-27 of the survey use a seven-point Likert scale to generate quantifiable data to assess the respondent's opinion of AI when presented as in use with no general connection to them, affecting them personally, or subject to some authority using AI, which could impact them. The selections provided for questions 7-27 were: 1 = Completely Agree, 2 = Mostly Agree, 3 = Somewhat Agree, 4 = Neither Agree nor Disagree, 5 = Somewhat Disagree, 6 = Mostly Disagree, 7 = Completely Disagree. The selections for question 5 frequencies were: 1 = Daily, 2 = Weekly, 3 = Monthly, 4 = A Few Times a Year, 5 = Never. The selections for question 6 frequencies were: 1 = Always, 2 = Frequently, 3 = Occasionally, 4 = Infrequently, 5 = I Usually Ignore it.

Subjects and procedure

The research study was conducted electronically using SurveyMonkey© to collect data from the Middle Georgia State University (MGA) community of students, faculty, staff, and alumni. According to its website, the population of the MGA comprises around 8500 enrolled students, faculty, and staff, with as many as forty thousand alumni (Sheron, 2024). This university-associated population was chosen to test emerging trends in AI opinion research from random sample studies that suggest more educated populations have a more favorable overall opinion of AI (Nader et al., 2024; Hobden & Begaj, 2023; Faverio & Tyson, 2023). The survey was distributed through mga.edu email by supervising faculty, and responses were collected from January 24th, 2025, until February 10th, 2025. To access the survey, participants were required to provide consent, and the SurveyMonkey© platform collected no identifiable data to ensure anonymity. Institutional Review Board (IRB) approval for the study was provided on November 22nd, 2024; see Appendix A for approval documentation. Prior to analysis, incomplete responses were removed from the data.

Data analysis and results

An exploratory factor analysis using varimax rotation was performed to identify emergent factors from the Likert scale questions. Three factors emerged from testing. Factor 1 included survey questions 7, 6, 16, 11, 5, and 8 and was designated as variable AI_Opinion. Factor 2 included survey questions 1, 2, and 3 and were designated as variable AI_Awareness. Factor 3 included survey questions 20, 21, and 10 and were designated as variable AI_Industry_Trust. EFA assumptions were met as KMO was greater than 0.6 and Bartlett's test was significant at $p < 0.05$ (Knapp, 2018).

Table 1. KMO Measure and Bartletts's Test for EFA Factors

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.742
Bartlett's Test of Sphericity	Approx. Chi-Square	708.697
	df	91
	Sig.	<.001

Two additional variables, Negative_AI_Opinion and Positive_AI_Opinion, were created by analyzing the descriptive statistics for questions 7-27 and grouping the top five questions with relatively similar homogeneity and distributions that leaned to either the positive scale, Likert responses 1-3, or negative, Likert responses 5-7. Negative_AI_Opinion was created using survey questions 4, 10, 12, 13, and 16. Positive_AI_Opinion was created using survey questions 5, 6, 7, 8, and 9.

Cronbach's Alpha was calculated to assess the reliability of the items making up each factor (Knapp, 2018). AI_Opinion (Factor 1) was found to be highly reliable (6 items; α= .84). AI_Awareness (Factor 2) was found to be highly reliable (3 items; α= .88). AI_Industry_Trust (Factor 3) was found to be reliable (3 items; α= .73). Negative_AI_Opinion was found to be reliable (5 items; α= .73). Positive_AI_Opinion was found to be highly reliable (5 items; α= .85).

Descriptive statistics for the predictor variables show that AI_Opinion and AI_Awareness in the MGA population trend from neutral to positive (below scale average = 4) while AI_Industry_Trust trends negatively in the MGA population (above scale avg = 4). The means of variables Negative_AI_Opinion and Positive_AI_Opinion behave as expected with negative above average and positive below scale average.

Table 2. Descriptive statistics for predictor variables.

Variable	N	Minimum	Maximum	Mean	Std. Deviation
AI_Opinion	102	1	7	3.45	1.102
AI_Awareness	102	1	7	3.10	1.500
AI_Industry_Trust	102	1	7	5.00	1.270
Negative_AI_Opinion	102	1	7	5.00	1.160
Positive_AI_Opinion	102	1	7	3.25	1.112

The researcher then addressed the research questions using one-way univariate analysis of variance (ANOVA), linear regression, and correlation analysis (Knapp, 2018). The results from the survey were analyzed in IBM SPSS version 30.0.0.0. The component factor analysis shows that AI_Opinion has a negative loading with AI_Awareness, suggesting that the elements have an inverse relationship and a positive loading with AI_Industry_Trust, suggesting a positive relationship. (Table 3)

Research questions 1 and 2 were evaluated using one-way ANOVA to compare the effect of the independent variable, Origination, to the dependent variables Positive_AI_Opinion, Negative_AI_Opinion, and AI_Opinion. The influence of Origination on a Positive_AI_Opinion was not significant $F(1,100) = 2.215$, $p = .140$ (see Table 5). The influence of Origination on Negative_AI_Opinion was not significant $F(1,100) = 1.148$, $p = .287$ (see Table 6). The influence of Origination on overall AI_Opinion was not significant $F(1,100) = 3.069$, $p = .083$ (see Table 7).

Research question 3 shows that there is a significant correlation between Negative_AI_Opinion and Positive_AI_Opinion $r = .705$, $p < .001$. Additionally, AI_Opinion significantly correlates with Positive_AI_Opinion $r = .912$, $p <.001$, and Negative_AI_Opinion $r = .791$, $p < .001$ (see Table 4).

Multiple regression was used to test research questions 4 and 5, investigating whether the frequency of AI technology use or AI Media consumption significantly predicts AI opinions.

The results of the regression for *Negative_AI_Opinion* indicated that the predictors explained 10% of the variance ($R^2 = .100$, $F(2,99)=5.520$, $p = .005$). It was found that Frequency_of_Use did significantly predict negative opinion ($\beta = .244$, $p =.006$); however, the Frequency_of_Media interaction was not a significant predictor ($\beta = .119$, $p = .349$) (Table 8).

The results of the regression for *Positive_AI_Opinion* indicated that the predictors explained 16% of the variance (R^2 = .161, F(2,99)=9.472, p < .001). It was found that Frequency_of_Use did significantly predict positive opinion (β = .200, p =.015), as did Frequency_of_Media interaction (β = .322, p = .007) (Table 9).

The results of the regression for *AI_Opinion* indicated that the predictors explained 19% of the variance (R^2 = .192, F(2,99)=11.780, p < .001). It was found that Frequency_of_Use did significantly predict opinion development (β = .262, p =.001), as did Frequency_of_Media interaction (β = .281, p = .016) (Table 10).

Table 3. Component Transformation Matrix

Component	1	2	3
AI_Opinion	.732	.523	.415
AI_Awareness	-.245	.800	-.515
AI_Industry_Trust	.381	-.187	-.145

Extraction Method: Principal Component Analysis | Rotation Method: Varimax with Kaiser Normalization

Table 4. RQ3: Correlation AI_Opinion, Negative_AI_Opinion, and Positive_AI_Opinion

		AI_Opinion	Negative_AI_Opinion	Positive_AI_Opinion
AI_Opinion	Pearson Correlation	1	.761**	.912**
	Sig. (2-tailed)	-	<.001	<.001
	N	102	102	102
Negative_AI_Opinion	Pearson Correlation	.761**	1	.705**
	Sig. (2-tailed)	<.001	-	<.001
	N	102	102	102
Positive_AI_Opinion	Pearson Correlation	.912**	.705**	1
	Sig. (2-tailed)	<.001	<.001	-
	N	102	102	102

**. Correlation is significant at the 0.01 level (2-tailed)

Table 5. RQ1: Origination to Positive_AI_Opinion ANOVA

	Sum of Squares	df	Mean Square	F	Sig
Between groups	2.705	1	2.705	2.215	.140
Within Groups	122.088	100	1.221		
Total	124.793	101			

Table 6. RQ2: Origination to Negative_AI_Opinion ANOVA

	Sum of Squares	df	Mean Square	F	Sig
Between groups	1.53	1	1.533	1.148	.287
Within Groups	133.553	100	1.336		
Total	135.086	101			

Table 7. Origination to overall AI Opinion ANOVA

	Sum of Squares	df	Mean Square	F	Sig
Between groups	3.653	1	3.653	3.069	.083
Within Groups	119.034	100	1.190		
Total	122.688	101			

Table 8. RQ4 and RQ5: Frequency of AI Use and AI Media Interaction predicting Negative_AI_Opinion

Variable	Beta	SE	95% CI		β	p
			LB	UB		
(Constant)	3.772	.361	3.056	4.487	-	<.001
Frequency_of_Use	.244	.087	.071	.417	.278	.006
Frequency_of_Media	.119	.126	-.132	.370	.093	.349

Note. R^2 = .100, *F*(2,99) = 5.520, *p* = .005

Table 9. RQ4 and RQ5: Frequency of AI Use and AI Media Interaction predicting Positive_AI_Opinion

Variable	Beta	SE	95% CI		β	p
			LB	UB		
(Constant)	1.898	.335	1.234	2.562	-	<.001
Frequency_of_Use	.200	.081	.040	.361	.237	.015
Frequency_of_Media	.322	.117	.089	.555	.263	.007

Note. $R^2 = .161$, $F(2,99) = 9.472$, $p < .001$

Table 10. Frequency of AI Use and AI Media Interaction predicting overall AI Opinion

Variable	Beta	SE	95% CI		β	p
			LB	UN		
(Constant)	2.062	.326	1.416	2.708	-	<.001
Frequency_of_Use	.262	.079	.105	.418	.313	.001
Frequency_of_Media	.281	.114	.054	.508	.232	.016

Note. $R^2 = .192$, $F(2,99) = 11.780$, $p < .001$

Discussion and Conclusion

This study found that how we first learn about AI as a concept has no significant effect on either positive or negative opinions of AI. This outcome could be influenced by smaller sample sizes, in overall survey response (n = 102) and in the low sampling of respondents who identified non-media origination of AI knowledge (n =29).

The study found that positive AI opinions and negative AI opinions are significantly correlated (Table 4). AI opinion in the survey population was generally positive, and the population reported comfort with explaining both AI and machine learning concepts but was generally less confident in explaining natural language processing. Where AI was presented as a general concept used in education, the entertainment industry, or medicine, the overall opinion was neutral to generally positive. However, when presented with AI being used directly to interact with the respondent individually, opinion shifted to the overall negative. When presented with the idea of AI being used with authority over them, such as being subject to traffic court rulings by AI systems, the opinion was overall very negative. While there is a strong correlation between positive and negative AI opinions, how the AI technology is presented to the individual appears to determine the specific opinion outcome.

This study found that the frequency of AI use and frequency of AI media consumption are significant predictors of AI opinion. 76% of survey respondents use AI applications at least monthly, and 86% consume AI subject media frequently. While both variables are significant predictors of AI opinion, they are less likely to predict a negative opinion ($R^2 = .10$) than a positive opinion ($R^2 = .161$) and makeup roughly 20% ($R^2 = .192$) of overall opinion outcome. This variability is a significant finding from a social science perspective, given the complexity of AI opinion tracking (Valchanov, 2023). Where 72% of the surveyed population first learned of AI as a concept in the media, the media also plays a continuous role in shaping public opinion of AI (Gerbner & Gross, 1976).

The data shows us that before the explosion of AI content in popular media after ChatGPT's chatbot debut in late 2022, AI awareness rates in random population samples in the US and UK exceeded usual market awareness standards (Weiner, 2024; Hobden & Begaj, 2023; Faverio & Tyson, 2023). Li. et al. (2024) surveyed the consumption of AI media in Hong Kong using the indirect media effects model and found that in groups, when an individual consumed media about AI, they were more likely to be receptive to the content when they presumed their peers were also interested in it. Assumptions of peer influence could be

a key indicator of why educated populations in random studies and this study of the MGA community reflect a positive opinion of AI. Simply stated, if we perceive our peers to be interested in a topic, we as individuals will become more receptive to that topic (Li et al., 2024; Gunther & Storey, 2003). Hence, peer assumptions in educated populations appear to create a more positive overall opinion of AI in this study and random sample studies (Hobden & Begaj, 2023; Faverio & Tyson, 2023). However, this trend disappears when the content presented shifts from society at large to you as an individual.

In random population surveys in the US and UK, AI awareness before ChatGPT was very high and largely negative in opinion, yet in both studies, the same phenomenon exists; where AI is presented as society at large, the overall opinion ranges from neutral to positive but where directed to the individual respondent the opinion ranges from neutral to negative (Hobden & Begaj, 2023; Faverio & Tyson, 2023). This trend is reflected in this MGA study, where AI use in medicine (society at large) scores largely neutral to positive, and consent to treatment by AI medical systems (personal involvement) scores overall negatively. This phenomenon has been described as cognitive dissonance in AI technology acceptance, where individuals and organizations appeared supportive and skeptical of AI integration on the same subject matter (Li & Zheng, 2024; Richards, 2023). Recent studies show that the Technology Acceptance Model (TAM) and other acceptance models are not behaving as expected with AI technologies, leading to the creation of newer Cognitive Acceptance Modeling (COG) theories (Sobhanmanesh et al., 2023). Eliminating dissonance in COG modeling should improve opinions and acceptance rates.

In 2022, Nader et al. at the University of Texas looked specifically at the effect of AI understanding through entertainment media. The study showed that younger respondents were more likely to have used and could correctly identify specific AI technologies, confirming usage rates in the MGA population primarily represented by young adult students (see Appendix B). UT students surveyed also followed suit with MGA students as the overall use of AI was considered positive until the perspective shifted to meaningful individual interaction (Nader et al., 2022). The UT study also examines the effect of entertainment media on AI recognition, with most respondents equating AI with robots (Nader et al., 2022). The anthropomorphism of AI in media and reality serves the same purpose: to build trust in human and robotic interactions by evoking emotional responses in the user or audience (Placani, 2024; Bailey, 2023). However, the cumulative effect of the various entertainment media incarnations of AI, where AI robots either turn on humanity or become victims of humanity, also appears integral to the reoccurring dissonance phenomenon of distrusting AI with meaningful human interaction while being generally positive about the technology itself (Nader et al., 2022).

In 2024, Gartner's annual CEO poll showed that 59% of CEOs believe AI is the technology that will impact their industries the most over the next three years (Furlonger, 2024). However, in that same poll, only 1% of CEOs said robotics and machine learning would have a significant impact, and only 3% said automation would have a significant impact (Furlonger, 2024). 44% of polled CEOs report using ChatGPT in their jobs, and 49% have workforce productivity plans that include GenAI. However, they report no specific insight into how to apply GenAI to increase productivity (Furlonger, 2024). Media consumption and non-specific use of GenAI applications may cause strategic leaders to overestimate the impact and expose a fundamental misunderstanding of AI. While strategic leaders do not conform to the anthropomorphic association views of AI found in other studies, they show less understanding of AI's foundational technologies, such as machine learning and automation (Nader et al., 2022).

AI acceptance by the public is essential for IT industry hardware and software leaders looking to get ahead of the disruptive business curve. However, early integration into primary products is largely falling flat in consumer response (Sidhu, 2024). Furthermore, as AI media continues to grow in volume, the public is being overwhelmed with negatively biased content from the industry leaders themselves, such as the CEO

of Google failing to explain the behavior of its AI products (Adarlo, 2024). Industry efforts to draw attention to specific products fail to consider how the context of their efforts alludes to existing and well-established beliefs created by nearly seventy-five years of AI media content or its effect on consumers (Nader et al., 2022). These industries and their marketing teams have primarily relied on a decade of social media theory that suggests engagement equals success (Rachmad, 2024). Consumer test groups may report overall positive expectations of AI products, but as soon as consumers interact with solicitations for these products the cognitive dissonance phenomenon shifts consumer receptions from positive to negative (Hobden & Begaj, 2023; Faverio & Tyson, 2023; O'Shaughnessy et al., 2023; Sobhanmanesh et al., 2023).

This effect does appear limited to specific instances of consumer interaction. As demonstrated in this study, AI use in healthcare is generally positively received, while consenting to direct treatment would be negatively received. Non-meaningful interactions, such as entertainment media produced with GenAI, remain neutral. At the same time, presentations of AI used with authority over the respondent will garner negative reactions, such as traffic court rulings by an AI system. As demonstrated in EFA testing, AI opinion can have an inverse relationship with trust and awareness, even in educated population studies (see Table 3). Because of this inverse relationship, it appears that non-specific AI use (uses that do not directly affect the respondent) will generate distrust where industry practice is questioned or where AI use or product design aligns with negative impressions created by previous media consumption (Nader et al., 2022).

AI opinion and acceptance research are rarely directly related to cybersecurity. However, demands for increased AI regulation appear as consumer distrust grows. In this study, trust in the AI industry was low, and the desire for regulation and advanced warning of AI use was high (see Appendix C). Cybercriminals are using AI platforms for increasingly complex and successful attacks, while cyberdefenders are mired by regulatory risk and business delays (Waller, 2024; Page, 2023; Li et al., 2023). The EU AI Act and EO 14410 have burdened AI cyberdefense developers to limit the scope of AI use to ensure AI defense systems do not access protected data, while cybercriminals have free reign to target that data without an equal defense measure to oppose them (Hickman et al., 2024; Waller, 2024; Chapman, 2023; Page, 2023; Gupta et al., 2023).

This study focused on the potential factors that develop the individual's opinion of AI. It was demonstrated in this study that how we first learn about AI has no significant impact on opinion and that most respondents credit the media with the origination of knowledge. Previous awareness and opinion studies in larger random populations fail to confirm the origination of knowledge, which in turn causes the cumulative effect of media influence to be overlooked as a significant factor in AI acceptance research (Hobden & Begaj, 2023; Faverio & Tyson, 2023; Nader et al., 2022).

This study also found that positive and negative opinions significantly correlate, confirming a perspective phenomenon in AI opinion data (Richards, 2023; Hobden & Begaj, 2023; Faverio & Tyson, 2023; Nader et al., 2022). Where the context of AI consideration relates away, not directly affecting the individual, the opinion of AI trends from neutral to positive. However, where the context of perspective relates inward, affecting the individual in a meaningful way, the opinion of AI shifts from positive to negative.

This study showed that frequency of AI technology use and AI media consumption are significant predictors of AI opinion outcomes. This study confirmed longitudinal data from US and EU papers showing that populations identified as higher educated are more AI positive in baseline opinions, however this study revealed that inside AI positive populations cognitive dissonance still shifts opinion from positive to negative (Hobden & Begaj, 2023; Faverio & Tyson, 2023; Nader et al., 2022). This study also revealed a significant distrust of AI industry developers inside higher educated populations with a corresponding positive opinion for greater legal oversight of AI.

Additional research should be done in larger random populations to confirm that most people first become aware of AI through the media. Identifying the most consumed types of AI media, such as broadcast news, entertainment, or social media, could be used to identify the most effective channels for improving AI acceptance. As the only consistently AI positive demographic in AI opinion studies in western civilization more educated populations should also be studied to determine how opinion differs by age, degree level, institution type such as technical or traditional university, to better understand which subpopulation is most effected by cognitive dissonance in AI opinion. Further research should also be done to confirm and identify specific subject matter and specific AI technology uses that create the cognitive dissonance phenomenon in AI acceptance research.

References

Adarlo, S. (2024, May 25). *CEO of Google says it has no solution for its AI providing wildly incorrect information*. Futurism.com. https://futurism.com/the-byte/ceo-google-ai-hallucinations

Alrubayyi, H., Alshareef, M. S., Nadeem, Z., Abdelmoniem, A. M., & Jaber, M. (2024). Security threats and promising solutions arising from the intersection of ai and iot: A study of iomt and ioet applications. *Future Internet*, *16*(3), 85. https://doi.org/10.3390/fi16030085

Arroyo-Figueroa, G. (2023). Artificial intelligence the strategic key of cybersecurity: Cyber defense intelligence: the strategic key of cybersecurity. *International Journal of Combinatorial Optimization Problems and Informatics*, *14*(3), 16–23. https://doi.org/10.61467/2007.1558.2023.v14i3.372

Bailey, M. (2023, October 3). *How can we trust AI if we don't know how it works?* Scientific American. https://www.scientificamerican.com/article/how-can-we-trust-ai-if-we-dont-know-how-it-works/

Chapman, D. (2023). The Ideal Approach to Artificial Intelligence Legislation: A Combination of the United States and European Union. *University of Miami Law Review*, *78*(1), 265–396.

Djenna, A., Barka, E., Benchikh, A., & Khadir, K. (2023). Unmasking cybercrime with artificial-intelligence-driven cybersecurity analytics. *Sensors*, *23*(14), 6302. https://doi.org/10.3390/s23146302

Faverio, M., & Tyson, A. (2023, November 21). What the data says about Americans' views of artificial intelligence. *Pew Research Center*. https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/

Fleck, A. (2024, February 22). Cybercrime expected to skyrocket in coming years. *Statista Daily Data*. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Furlonger, D. (2024). How your CEO is Thinking About AI. *Gartner*. https://www.gartner.com/en/articles/how-your-CEO-is-thinking-about-ai

Gavoor, A. (2023). *Structural challenges loom for biden's executive order on artificial intelligence*. Regulatory Studies Center, Columbian College of Arts & Sciences, George Washington University. https://regulatorystudies.columbian.gwu.edu/structural-challenges-loom-bidens-executive-order-artificial-intelligence

Gerbner, G., & Gross, L. (1976). Living with television: The violence profile. *Journal of Communication*, *26*(2), 172–199. https://doi.org/10.1111/j.1460-2466.1976.tb01397.x

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254. https://doi.org/10.1080/08839514.2022.2037254

Gunther, A. C., Bolt, D., Borzekowski, D. L. G., Liebhart, J. L., & Dillard, J. P. (2006). Presumed influence on peer norms: How mass media indirectly affect adolescent smoking. *Journal of Communication*, *56*(1), 52–68. https://doi.org/10.1111/j.1460-2466.2006.00002.x

Gunther, A. C., & Storey, J. D. (2003). The influence of presumed influence. *Journal of Communication*, *53*(2), 199–215. https://doi.org/10.1111/j.1460-2466.2003.tb02586.x

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access*, *11*, 80218–80245. https://doi.org/10.1109/ACCESS.2023.3300381

HAI Global AI Index. (2023). Stanford University. https://aiindex.stanford.edu/report/

Hickman, T., Lorenz, S., Teetzmann, C., & Jha, A. (2024, July 16). *Long awaited eu ai act becomes law after publication in the eu's official journal | white & case llp*. https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal

Hobden, S., & Begaj, D. (2023, December 6). *The tide is changing: Monitoring public attitudes towards data and AI – Responsible Technology Adoption Unit Blog*. https://rtau.blog.gov.uk/2023/12/06/the-tide-is-changing-monitoring-public-attitudes-towards-data-and-ai/

Knapp, H. (2018). *Intermediate statistics using spss*. Sage.

Kouroupis, K. (2024). AI and politics: Ensuring or threatening democracy? *Juridical Tribune*, *13*(4). https://doi.org/10.24818/TBJ/2023/13/4.05

Kovaci, P.-D. (2024). Threat actors seeking to exploit ai capabilities. Types and their goals. *Strategic Impact*, *89*(4), 53–63. https://doi.org/10.53477/1842-9904-23-21

Li, J., Maiti, A., & Fei, J. (2023). Features and scope of regulatory technologies: Challenges and opportunities with industrial internet of things. *Future Internet*, *15*(8), 256. https://doi.org/10.3390/fi15080256

Li, W., & Zheng, X. (2024). Social media use and attitudes toward ai: The mediating roles of perceived ai fairness and threat. *Human Behavior and Emerging Technologies*, *2024*, 1–11. https://doi.org/10.1155/2024/3448083

Li, Z., Shi, J., Zhao, Y., Zhang, B., & Zhong, B. (2024). Indirect media effects on the adoption of artificial intelligence: The roles of perceived and actual knowledge in the influence of presumed media influence model. *Journal of Broadcasting & Electronic Media*, *68*(4), 581–600. https://doi.org/10.1080/08838151.2024.2377244

Lobera, J., Fernández Rodríguez, C. J., & Torres-Albero, C. (2020). Privacy, values and machines: Predicting opposition to artificial intelligence. *Communication Studies*, *71*(3), 448–465. https://doi.org/10.1080/10510974.2020.1736114

Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2), 2272358. https://doi.org/10.1080/23311916.2023.2272358

Nader, K., Toprac, P., Scott, S., & Baker, S. (2024). Public understanding of artificial intelligence through entertainment media. *AI & SOCIETY*, *39*(2), 713–726. https://doi.org/10.1007/s00146-022-01427-w

O'Shaughnessy, M. R., Schiff, D. S., Varshney, L. R., Rozell, C. J., & Davenport, M. A. (2023). What governs attitudes toward artificial intelligence adoption and governance? *Science and Public Policy*, *50*(2), 161–176. https://doi.org/10.1093/scipol/scac056

Ouchchy, L., Coin, A., & Dubljević, V. (2020). AI in the headlines: The portrayal of the ethical issues of artificial intelligence in the media. *AI & SOCIETY*, *35*(4), 927–936. https://doi.org/10.1007/s00146-020-00965-5

Page, M. (2023, August 22). *Malicious AI arrives on the dark web*. The Strategist. https://www.aspistrategist.org.au/malicious-ai-arrives-on-the-dark-web/

Placani, A. (2024). Anthropomorphism in AI: Hype and fallacy. *AI and Ethics*, *4*(3), 691–698. https://doi.org/10.1007/s43681-024-00419-4

Rachmad, Y. (2024). *Social media influence theory*. https://doi.org/10.17605/OSF.IO/6MQA5

Ray, J. (2024, August 27). *Americans express real concerns about artificial intelligence*. Gallup.Com. https://news.gallup.com/poll/648953/americans-express-real-concerns-artificial-intelligence.aspx

Richards, M. B. (2023). Artificial intelligence in marketing communication: Adoption challenges and opportunities through a lens of cognitive dissonance. *Journal of Marketing Development and Competitiveness*, *17*(3). https://doi.org/10.33423/jmdc.v17i3.6480

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173. https://doi.org/10.1007/s42979-021-00557-0

Sidhu, B. (2024, June 10). Is apple's ai a game-changer or a privacy risk? *Medium*. https://medium.com/@bilawal/is-apples-ai-a-game-changer-or-a-privacy-risk-c18796d384e4

Sobhanmanesh, F., Beheshti, A., Nouri, N., Chapparo, N. M., Raj, S., & George, R. A. (2023). A cognitive model for technology adoption. *Algorithms*, *16*(3), 155. https://doi.org/10.3390/a16030155

Waller, J. (2024). *The EU AI Act: Pioneering the Future of AI Regulation*.
https://www.nccgroup.com/us/the-eu-ai-act-pioneering-the-future-of-ai-regulation

Weiner, G. (2024). The 6 ways to measure awareness campaigns. *Whole Whale*.
https://www.wholewhale.com/tips/measure-awareness-campaigns/

Zarina I., K., Ildar R., B., & Elina L., S. (2020). *Artificial intelligence and problems of ensuring cyber security*. https://doi.org/10.5281/ZENODO.3709267

Appendix A

Middle Georgia
State University

Department of Political Science
100 University Parkway, Macon, GA 31206
478.757.2544 mga.edu

Macon
Cochran
Dublin
Eastman
Warner Robins
and online everywhere

November 22, 2024

TO: Dr. Alex Koohang & Charles Wesley Milam

FROM: Dr. John Powell Hall
Institutional Review Board Chair 2023-2025
Middle Georgia State University

SUBJECT: Approval of Project # 202411 – R
Title: "A.I. Cybersecurity: Advancing Understanding of Public Opinion to Create
Effective Public Policy."

I am pleased to inform you that your project has been approved under the Exempt
Review protocol of the Middle Georgia State University Institutional Review Board.
Your project complies with the IRB guidelines for exempt proposals, including
"research projects which present no more than minimal risk and therefore can be
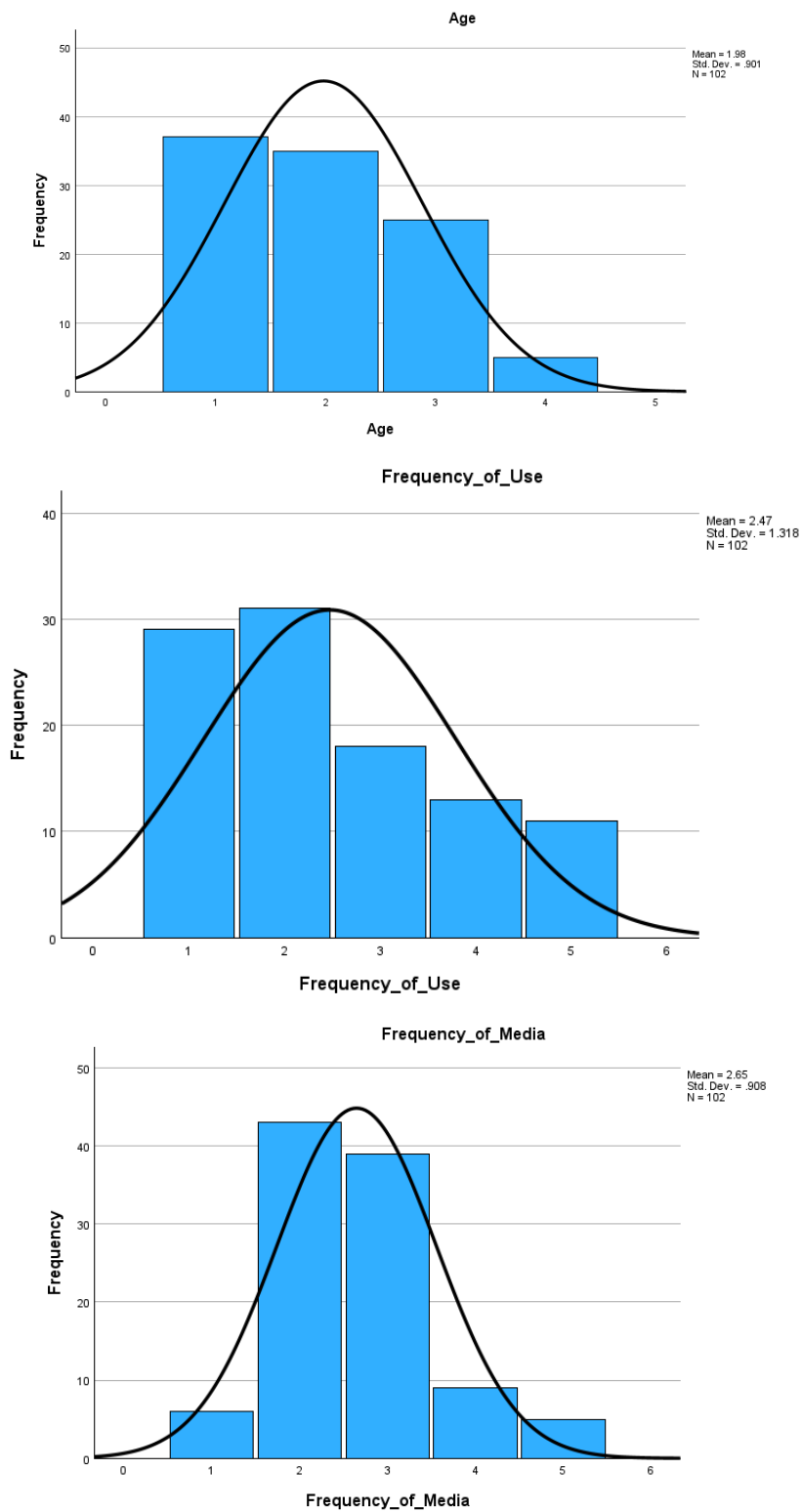reviewed without a convened meeting."

If you wish to make any changes to this protocol, you must disclose your plans
before you implement them so the IRB Board can assess their impact on your
project. In addition, you must report to the Board any unexpected complications
arising from the project that affect your participants. Approval of this project is for
a period of one year from the date of this letter, the maximum duration permitted by
the Federal Office for Human Research Protections (OHRP). If the project will not be
completed by November 21, 2025, then you must submit a Renewal Form notifying
the IRB of the continuation of this project. It is recommended that you keep your
unit supervisor informed about the status of this project. If you have any questions
regarding this project, please contact the current Chair of the IRB at irb@mga.edu.

Sincerely,

Dr. John Powell Hall
IRB Chair
2023-2025

Appendix B

Age

Mean = 1.98
Std. Dev. = .901
N = 102

Frequency_of_Use

Mean = 2.47
Std. Dev. = 1.318
N = 102

Frequency_of_Media

Mean = 2.65
Std. Dev. = .908
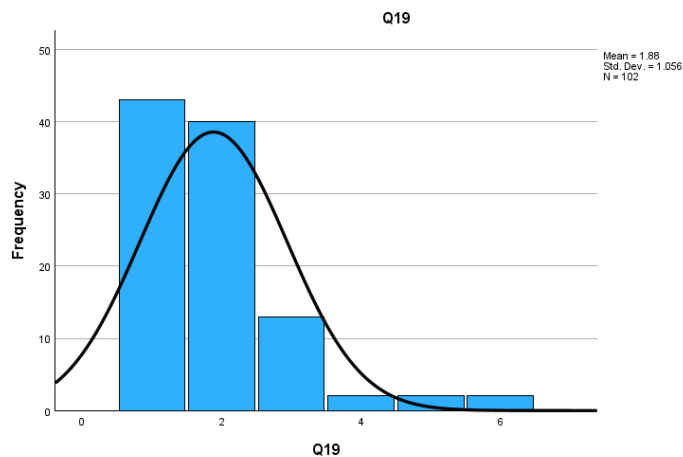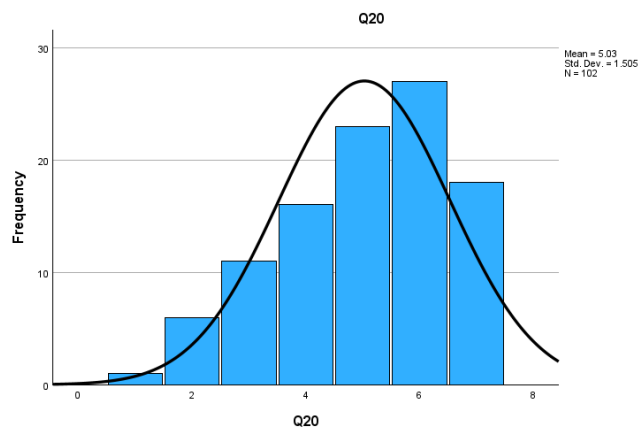N = 102

Appendix C

Question 18. I think we need more government regulation of AI systems.
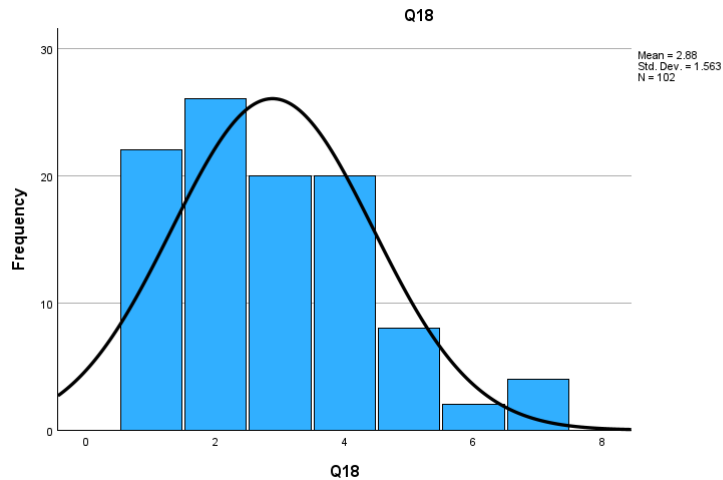
Question 19. I think we need more transparency in AI use, like how websites notify us of cookies and data privacy now.

Question 20. I trust the people developing AI have everyone's best interests in mind.

Appendix C cont.

Question 21. I trust the companies deploying AI have my privacy in mind.

Mean = 5.63
Std. Dev. = 1.421
N = 102