2019

The Impact of Wikileaks on the Public Opinion of Online Privacy

Hazel Small
Pace University

The Impact of Wikileaks on the Public Opinion of Online Privacy

Hazel Small
Global Marketing Management
Advisor: Vishal Lala
Pace University
Lubin School of Business
May 2019

Abstract

This paper explores the relationship between Wikileaks and online privacy concerns. The goal of the research was to establish that the public's concern about their online privacy was increased after reading about a relevant leak by posing a hypothesis and testing it. To do this, an A/B test survey was created and distributed through various social media platforms. The results were then statistically evaluated using a t-test for testing the equality of the means of independent samples. We did not have enough evidence to reject the null hypothesis in most cases, and therefore could not establish a correlation between Wikileaks publications and an increase in online privacy concerns. However, the paper proposes a follow-up hypothesis in which the goal was to establish that Wikileaks causes an increase in government distrust. Through the same research methods, we were able to reject the null hypothesis and establish that the article did cause more government distrust.

Table of Contents Page Number

Introduction

Wikileaks came to prominence in 2007 when they became the first, and to my knowledge only, non-profit organization that leaks secret information from anonymous sources. They've been seen as the emerging model of the hacktivist transnational organisation-network, calling out the U.S. Army, congressmen, private intelligence companies, universities, and churches, and released a wide range of private documents, emails and more content than one person could sort through on their own. Former FBI Director James Comey has referred to the organization as "intelligence porn". One of their most well known leaks was the "Iraqi Apache Helicopter Attack"- video footage of U.S. military air crew shooting down over 15 Iraqi civilians. The crew can be overheard laughing and making remarks such as "Light them up!" and "Keep shooting!".

This was back in 2010, and since then I find that the once household name is being heard less and less, but the underlying premise has continued to cause controversy.

I've asked many people their stance on the privacy concerns of Facebook. A few months ago, the personal information of 50 million users was exposed after the company was hacked. The news was highly publicized at the time, and people all over were outraged. Years before, Wikileaks published documentation insinuating a similarly disturbing story. A German surveillance malware company, Finfisher, was selling computer intrusion systems capable of intercepting communication and data from OS X, Windows, and Linux computers as well as Android, iOS, and Windows Mobile devices. This software could intercept files as well as Skype calls, emails, and video and audio through ones' webcam and microphone. Whether it is a data

hack or weaponized malware, privacy has been an issue throughout the entirety of the digital age. But the spark of concern for it began when we saw just what the Internet of Things (IoT) was capable of, and we have WikiLeaks to thank for that. Wikileaks was the first organization to expose the multitude of ways that companies and the government intrude into the general population's online data and information.

So what role and impact has WikiLeaks had on the public's value of online privacy as the frontrunner of the hacktivist movement? Wikileaks may have lit the "online privacy concerns" fire, but do they have enough sway to get the public to change their ways? Or are they only capable of creating an increase in awareness? In this paper, I will use surveys to understand the level of concern the public has on online privacy, and whether Wikileaks has the ability to affect one's opinion on the subject. Furthermore, does a concern for online privacy translate to a willingness to change the ways that individuals behave online? Or are we comfortable enough with our online choices to let the chips fall where they may? And finally, how do the explicit documents posted by Wikileaks effect ones' trust in the federal government? In other words, do individuals' trust that the government is always acting in our best interest, or do they feel as though the government's surveillance and methods of accessing our online data are an abuse of power?

The Rise of WikiLeaks

> *"The Internet, our greatest tool for emancipation, has been transformed into the most dangerous facilitator of totalitarianism we have ever seen"*
> *(Assange et al., 2012: 1)*

Wikileaks has paved the way for the public's concern about government and company transparency. **"**Wikileaks and Public Opinion" (Alberto Quian et. al) researches when, how, and why WikiLeaks emerged as a global phenomenon: "After 9/11, the United States was at a tipping point for security and the world order, the privacy of the individual and civil liberties… states undertook actions to break encryption systems and any others that guaranteed anonymity on the Internet, to engage in surveillance of our online communications." At this point in time, the country was ready and willing to hand over any privacy rights they had for the sake of safety. But the willingness became convoluted in the years to come, and Wikileaks swung the doors wide open on just how deep the invasion of our privacy was, and the sheer hypocrisy of the government asking Americans to confiscate their information, while leaving us in the dark. The massive leaks of secret documents about the wars in Iraq and Afghanistan was the tipping point. Americans finally said "If we are willing to share our information, you should be willing to share yours." The desire for disclosure and transparency of government activities is where the popularity of Wikileaks began.

Figure 1: Wikileaks Days of Greatest Impact on Twitter

TABLE 1. *Days of the greatest impact and influence of WikiLeaks on Twitter*

DATE	No. MENTIONS	EVENT
7 December 2010	161,776	Assange arrested in London. Visa and MasterCard suspend payment systems to WikiLeaks.
9 December 2010	144,650	Twitter shut down Anonymous accounts and Facebook shuts down the page for *Operation Payback*. Amazon suffers DDoS attacks. Lula da Silva defends WikiLeaks.
29 November 2010	140,816	One day after the start of *Cablegate*. Assange announces that he is planning to disseminate material about a large US bank in early 2011.
3 December 2010	139,291	WikiLeaks takes a Swiss domain name, WikiLeaks.ch, after its service was removed by its US provider, EveryDNS. A day earlier, the Swedish Supreme Court refused to examine the appeal filed by Assange against his international arrest warrant for alleged sexual abuse and rape; the arrest warrant was confirmed.
8 December 2010	133,102	DDoS attacks by WikiLeaks-supporting *hacktivists* against the Swedish Prosecutor's Office, the website belonging to Claes Borgstrom (lawyer of the two women who accused Assange of alleged sexual abuse) and Visa and MasterCard services.
27 February 2012	107,745	WikiLeaks starts releasing 5.5 million emails from Stratfor, in collaboration with 29 news organisations.
1 December 2010	107,363	The head of the National Security Commission of the United States Senate, Democrat Joe Lieberman, urges all companies that provide services to WikiLeaks to terminate their relationship with the organisation. Amazon expels WikiLeaks from its servers, where it had been hosted since 29 November, claiming numerous computer attacks received since the beginning of *Cablegate*. Interpol confirms that a Red Alert (that is, an international arrest warrant against Assange) had been issued on 20 November, 2010.

Source: Developed by the authors based on data obtained from PeopleBrowsr.

Figure 1 above, presented in the data collected by Alberto Quian and Carlos Elias, pinpoints the exact days on which Wikileaks got the most mentions on Twitter, and what occurence set this off. As one would expect, all of the days of peak popularity for Wikileaks coincided with specific events, and were ranked by greatest impact. It was verified that

WikiLeaks achieved its highest impact levels on Twitter during Cablegate: from November 28, 2010 up to and including December 9, 2010, there were 1,357,984 mentions on WikiLeaks; an average of 113,165 daily mentions. Cablegate, in short, was the leak of over 250,000 US Diplomatic cables alleging everything from child prostitution among US private contractors to American diplomats bartering with Guantanamo Bay prisoners. Through identifying major Wikileaks milestones, they were able to establish a correlation between the type of event occuring and the online public reaction.

"Oh, Wikileaks, I would so love to RT you" (Lynch, 2014) discusses the peak of Wikileaks as one of the first accounts on Twitter to surpass 1 million followers, back in 2011. "As WikiLeaks weathered legal investigation by the U.S. government, an international financial blockade, and a sexual scandal involving the group's founding member and spokesperson, Twitter evolved into a primary information source for both the group's followers and media outlets reporting on WikiLeaks-related events." She discusses the motivation behind Twitter users to follow WikiLeaks, an outlier in the million-plus club amongst celebrities and media outlets, and the presence of "Social Media activism" on the site. WikiLeaks used Twitter to solicit money for special projects that expanded on the group's basic mission. They also often asked their followers to assist with tasks, and in doing so, depending on the ethic of free labor in an online space. Wikileaks' popularity on social media, and ability to make requests of their followers' and actually have them followed through, indicates a significant amount of intrigue on the organization's subject matter - people were watching, and they cared about what Wikileaks had to say.

In an interview, Birgitta Jónsdóttir, a member of the Icelandic parliament and an early WikiLeaks volunteer, says “In reality we don’t have any privacy. It has been that way for a long time; now it is just out in the open, and the scary part is that people don’t care.” Jónsdóttir is responsible for the leak of the famous Collateral Murder video - a classified US military video depicting the indiscriminate slaying of over a dozen people in the Iraqi suburb of New Baghdad. When asked how her privacy has been impacted by her involvement in the organization, she responded: “This is not about me; it is about you all. It’s about our responsibility as members of parliament to address the issues of privacy and lack thereof.” She goes on to discuss how Wikileaks publications “humanized” the privacy battle. Beforehand, privacy was always in the technology section of the newspaper. Managing to get the attention about our privacy and the lack thereof into the human-interest section of the media is very significant to the basis of my research. The public has to have a degree of knowledge and understanding on how, why, and when our privacy is being evaded in order to be concerned about it.

Privacy Concerns Now

Information privacy, defined as the ability of the individual to control when, how, and to what extent his or her personal information is communicated to others (Westin, 1967), is one of the most important ethical, legal, social, and political issues of the information age. Lawsuits against popular websites (e.g., Facebook, Google, etc.) for violation of online privacy, and the implementation of online privacy protection acts (e.g., Federal Trade Commission 2007), serve as evidence of the increased importance and interest in online privacy. A valuable study conducted by Weiyin Hong and James Y. L. Thong dissects the area of Internet privacy concerns

(IPC), through four online surveys involving nearly 4,000 Internet users. Their results confirm that "the third-order conceptualization of IPC has nomological validity, and it is a significant determinant of both trusting and risk beliefs." One part of the study dives specifically into consumers concern about how their personal information is collected and used when interacting with websites. The example they used was Travelocity - a website that uses business intelligence software to track consumers' search behavior and use the data to predict consumers' needs and make personalized recommendations. While such a personalized service may provide convenience to consumers, it also raises their privacy concerns about the websites using their personal data without their approval. This is one in a multitude of ways in which people are becoming increasingly alarmed about the amount of information websites really are tracking and storing.

Information sharing and exchanging ideas is the basis behind most communication and interaction on the Internet and social media platforms, but while people like to share their ideas with others who have common interests, there is increasing worry about potential privacy violations that could lead to negative impacts on their reputations. People want to be able to express themselves on sensitive topics online, such as politics, but fear prosecution in these situations. About 77 percent of social network users do not allow disclosure of their personal information, and even more users have expressed a lack of confidence that their privacy will be protected (Pan et. al, 2017). A 2017 study explores the subject of group privacy concerns and how to improve the cohesion and vitality of online communities by reducing these concerns. The premise relates back to my research by insisting that "people who trust an organization or a

group show less privacy concerns and are more willing to provide private or non private information. When personal information is overexposed, consumer privacy concerns will be positively influenced owing to decreased trust."

According to Twitter (2019), the social media platform has 321 million monthly active users. College students specifically are heavy users of Twitter, with a study by The Higher Education Research Institute (HERI, 2007), stating that 94% of college students use social media. A study done by Kenneth Yang (et. al) tested college students' privacy concerns and impacts on their Twitter usage behaviors. Through an online questionnaire, they tested the predictive power of privacy management variables on Twitter usage among college students from a large public university in the United States. Their data showed that college students' privacy control of private information on Twitter was found to be statistically significant and the most consistent predictor of their Twitter usage behaviors, measured in daily minutes spent on Twitter. The main concern of privacy management is of the control and protection of private information such as a person's daily activities, lifestyle choices, finances, their whereabouts, or any information a person feels they need not disclose (Dolan, 2012). The similarities in demographic and methodology make this study particularly relevant to my own.

Smart devices, such as smartwatches and smartphones have been the most recent technologies associated with the concern of privacy discussion due to their obvious security vulnerabilities that make these devices prone to data leaks. Smartphones carry a large quantity of sensitive information to satisfy people's various requirements, but the way this information is

used cross-functionally effects the security of users' privacy. Android devices specifically have been under fire due to their permission-based security, which allows users to directly approve permissions requested by an app when installing it. Much of the research I crossed when diving into this particular topic involved a privacy calculus model, where individuals weigh the anticipated risks of disclosing personal data against the potential benefit. Obviously, it's impossible to stay completely "off the grid" and have absolute privacy. So, everyday we make the choice to surrender a certain degree of privacy in exchange for an outcome that we believe to be worth the risk of information disclosure. Everytime we order something online from Amazon we are disclosing personal information over the internet. This model allows researchers to depict how individuals develop privacy concerns and what consequences these perceptions have in influencing interactions with other individuals, groups, and agencies. My study indicates internet privacy concern and perceived internet privacy risk, however the willingness of individuals to provide personal information despite concern is fairly relevant to the results of the research.

Hypotheses

H0: Wikileaks does not increase the public's concern on online privacy.

H1: Wikileaks increases the public's concern on online privacy.

These hypotheses are tested against every individual question. The general outcome of the study is to establish whether or not Wikileaks publications have an effect on the public's perceived value of online privacy. When presented with a particular instance in which Wikileaks posted that the government and private intelligence companies were indeed hacking into the

online data of the general population, do people express concern? Or do people, in general, not care that their data isn't private, as long as it hasn't caused them any harm? The vast majority of Americans are aware of the government's online surveillance programs, and 57% believe that monitoring of the general population is unacceptable. But does awareness and justification of these initiatives alter individuals' willingness to disclose personal information online? I will provide answers to these questions.

In the event that my results for these hypotheses did not provide conclusive results, I also proposed an alternative:

H0: Wikileaks does not cause an increase in government distrust.

H1: Wikileaks causes an increase in government distrust.

Is Wikileaks influential enough to cause people to trust the government less? Fewer than 3 in 10 Americans have expressed trust in the federal government in every major national poll conducted since July 2007 (Blumenthal, 2015). Can this number be influenced further when people are presented with a particular instance in which in which Wikileaks posted that the government and private intelligence companies were indeed hacking into the online data of the general population?

Methodology

My study sets out to analyze the impact of WikiLeaks today on the individual's privacy concerns. A survey experiment was developed using Qualtrics to understand the impact of two articles on the privacy concerns of various individuals as a method of A/B testing. The survey was distributed through various social medias including Twitter, Facebook, and Nextdoor. This method was chosen due to the vast exposure offered on these platforms. Web surveys also offer the benefit of low distribution costs vs. minimal time required to obtain a sufficient number of results.

The individuals surveyed were presented with one of two articles, both reviewed to ensure face and content validity and to remove any potential discrepancies with wording and layout, and assigned at random using the Randomizer feature of Qualtrics. The first article, which will be referred to as article A, pertained specifically to a Wikileaks breakthrough, in which secret CIA documents were posted revealing that the government agency was hacking into the public's technological devices in order to surveil unsuspecting people. The leak included specific details on how to hack into target TVs in "Fake Off" mode, and how to penetrate high-security networks that are disconnected from the internet. The second article, which will be referred to as article B, acting as a control in the experiment to ensure that the opinions expressed in the questions to follow were influenced by Wikileaks itself, was about the leak of secret Russian documents that were anonymously posted online. These documents included hundreds of thousands of messages and files from Russian politicians, journalists, oligarchs, religious figures, and nationalists/terrorists in the Ukraine.

The first set of questions after the article are various comprehension checks to ensure the surveyors actually read and understood the article. If the surveyor answered more than 1 of the 3 multiple choice question checks wrong, their responses were not included in the final results.

The second set of questions pertain to writing quality and comprehension. Using a 5-point Likert scale, the surveyors are asked to rate various aspects of the article including organization and grammar on a scale of extremely bad to extremely good. These are distractor questions. I specifically establish that these questions are the basis of my research to not let on to the respondent the true purpose of the study.

The following four models are all various previously tested and validated 5-point Likert marketing scales, with minor tweaks to ensure the relevance of the questions to my study. The questions are as follows.

Figure 2: Online Privacy Survey Question Scales

Model Used and Latent Variable	**Item**	**Scale**
Extended Privacy Calculus Model for E-Commerce Transactions Internet Privacy Concerns (PC)	PC1: I am concerned that the information I submit on the Internet could be misused. PC2: I am concerned that a person can find private information about me on the Internet. PC3: I am concerned about submitting information on the Internet because of what others might do with it. PC4: I am concerned about submitting information on the Internet because it could be used in a way I did not foresee.	Strongly disagree - Strongly agree
Extended Privacy Calculus Model for E-Commerce Transactions Internet Trust (T)	T1: Internet websites are safe environments in which to exchange information with others. T2: Internet websites are reliable environments in which to conduct business transactions. T3: Internet websites handle personal information submitted by users in a competent fashion.	Strongly disagree - Strongly agree
Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns Internet Usage Privacy Concerns (IU)	IU1: You receive an email and have no idea how the company got your address. IU2: A notice on a webpage states that information collected may be sold to other companies. IU3: You are asked to provide your name to access a homepage. IU4: You are asked to provide your Social Security Number to access a homepage.	Extremely low concern - Extremely high concern
Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model Internet Users' Response to Privacy Concerns (IURPC)	IURPC1: How likely are you to refuse to give information to an online company because you think it is too personal? IURPC2: How likely are you to take actions to have your name removed from e-mail lists for catalogs, products, or services? IURPC3: How likely are you to write or call an online company to complain about the way it uses personal information? IURPC4: How likely are you to write or call an elected official or consumer organization to complain about the way online companies use personal information? IURPC5: How likely are you to refuse to purchase a product because you disagree with the way an online company uses personal information?	Extremely unlikely - Extremely likely

The 4 models represented in Figure 2 all have a different purpose, which is represented by the latent variable. Model 1 most blatantly indicates the level of concern the surveyor feels toward the use of their data online. The 4 questions within the model pose the various ways in which their information can be taken advantage of. Model 2 is intended to understand the degree of trust the surveyor has in internet websites. In other words, do they feel the internet is a safe space to express their feelings, conduct business, and offer up personal information? Model 3 tests the level of concern an individual would feel towards particular scenarios. The 4 questions are intended to start with a low level of concern, i.e. small and more frequent occurrences, and escalate to a level of high concern, i.e. obscure and outlandish requests such as sharing a social security number. These first 3 models pertain to overall online privacy concerns, and should the surveyors who read article A have an increased level of concern compared to article B, it will be represented most clearly through these models. Model 4 is intended to display a willingness to take action. After establishing whether or not these individuals express concern, these questions will determine if they surveyors are concerned enough to refuse information or be proactive in preventing intrusions of privacy in the future.

The final two models used relate to trust in the federal government. In the event that the results from my various privacy-related questions provided no substantial results, I proposed a follow-up hypothesis to test whether the Wikileaks article induced less trust in the government than the control article. The following Five-Point Likert Scale questions were asked.

Figure 3: Government Trust Survey Question Scales

Model Used and Latent Variable	**Item**	**Scale**
Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring Government Monitoring (GM)	GM1: Online government surveillance is a necessary part of national security. GM2: The government needs to monitor U.S. citizens online to keep the country safe. GM3: The government can track my online behavior because I have nothing to hide.	Strongly disagree - Strongly agree
Trust in Government NES Pilot Report Government Trust (GT)	GT1: How often do you think you can trust the government to do what is right? GT2: How often do you think you can trust the federal government to make decisions in a fair way? GT3: How often do you trust the federal government to do what is best for the country?	Never - Always

The two models in Figure 3 use the latent variables government monitoring and government trust. The results from these questions are intended to show how the surveyors This will give me a sense of whether or not the surveyors are affected by the behaviors occurring in Article A since only this article pertains to the federal government, or whether they have the same response to those in the control group and thus feel unaffected.

Results and Discussion

After removing any responses that did not pass the comprehension checks, the study was left with 88 results. The first step to understand the results was to divide the responses of the two articles. Article A received 57 responses and Article B received 31. The questions were divided up into various blocks based on the model used but were tested individually. All responses were on a 5-point Likert scale, and were re-coded so that the values were on a 0 to 4 scale. The most

negative responses received a 0, the quantitative values being extremely bad, strongly disagree, extremely low concern, extremely unlikely, and never. A response of a 4 had the quantitative values of strongly agree, extremely high concern, extremely likely, and always. A 2 was considered a neutral response.

The Qualtrics Reports feature allows the surveyor to filter the data and view the statistics of the results including the mean, variance, and count. Filtering the data for those who responded to Article A (Q1 equal to 'I have read the article'), I was able to establish a mean for each of the questions asked ($\overline{X}_A$). I then filtered the data for those who responded to Article B (Q2 equal to 'I have read the article') and included the mean for each of the questions asked in my data ($\overline{X}_B$). I compared the mean for the responses from article A to Article B. A higher mean in the responses to article A would insinuate that the respondents had a higher level of concern than those who read article B, and meant that those results could potentially prove my alternative hypothesis. Therefore, any question in which $\overline{X}_A$ was greater than $\overline{X}_B$ was tested and included in the data. Questions that resulted in $\overline{X}_A$ being smaller than $\overline{X}_B$ were thrown out.

Since the alternative hypothesis is specifically an *increase* in online privacy concerns, and not just a difference, I used a one-tailed t-test to test the difference between the two means-independent samples. A t-test is a type of inferential statistic used to determine if there is a significant difference between the means of two groups, which may be related to certain features.

The first step of the t-test was to find the critical value. I established the degrees of freedom was 30, since the degrees of freedom (df) are equal to the smaller of $n_A - 1$ and $n_B - 1$, i.e.

$$df = min\,(n_A - 1, n_B - 1)$$

Table F on page 784, (Bluman, 2009), shows that the critical region for a one-tailed test with $\alpha = .05$ and $df = 30$ equals 1.697, indicating that any t-value larger than that is significant and supports my alternative hypothesis.

From there, I used the following formula to establish the t value of every question asked:

$$t = \frac{\overline{X}_A - \overline{X}_B}{\sqrt{\frac{s_A^2}{n_A} + \frac{s_B^2}{n_B}}}$$

In this equation, $\overline{X}_A - \overline{X}_B$ is the observed difference between the sample means (equal to zero if the null hypothesis is true), and $\sqrt{\frac{s_A^2}{n_A} + \frac{s_B^2}{n_B}}$ is the standard error of the difference between the two means. $\overline{X}_A$ is the mean, s_A^2 is the variance, and n_A is the number of responses for the given question in article A. $\overline{X}_B$, s_B^2, and n_B are the mean, variance, and number of responses for the given question in article B, respectively. Once I found the t-value for each question, I compared it to the critical value. Any t-value that supported the alternative hypothesis was highlighted.

Figure 4: Online Privacy Survey Question Results

Question	$\overline{X}_A$	$\overline{X}_B$	n_A	n_B	s_A^2	s_B^2	t
PC1	2.86	2.94	57	31	1.27	1.00	Not tested, $\overline{X}_B > \overline{X}_A$
PC2	3.18	3.13	57	31	1.00	1.52	0.18
PC3	3.12	2.94	57	31	0.97	1.13	0.81
PC4	3.16	3.23	57	31	0.81	0.85	Not tested, $\overline{X}_B > \overline{X}_A$
T1	2.60	2.87	57	31	1.03	0.92	Not tested, $\overline{X}_B > \overline{X}_A$
T2	2.04	2.32	57	31	1.14	1.23	Not tested, $\overline{X}_B > \overline{X}_A$
T3	2.30	2.65	57	31	1.43	1.04	Not tested, $\overline{X}_B > \overline{X}_A$
IU1	2.23	1.55	57	31	1.57	1.19	2.65
IU2	2.63	2.23	57	31	1.13	1.31	1.63
IU3	2.58	2.42	57	31	1.18	1.58	0.60
IU4	3.84	3.81	57	31	0.56	0.63	0.21
IURPC1	3.21	3.32	57	31	1.13	1.09	Not tested, $\overline{X}_B > \overline{X}_A$
IURPC2	3.07	3.29	57	31	0.92	0.75	Not tested, $\overline{X}_B > \overline{X}_A$
IURPC3	1.82	1.65	57	31	1.75	1.70	0.61
IURPC4	1.56	1.52	57	31	1.39	1.79	0.16
IURPC5	2.54	2.77	57	31	1.54	1.65	Not tested, $\overline{X}_B > \overline{X}_A$

Figure 5: Aggregated Online Privacy Survey Question Results

Block	$\overline{X}_A$	$\overline{X}_B$	n_A	n_B	s_A^2	s_B^2	t
PC	3.08	3.06	57	31	1.02	1.11	0.10
T	2.31	2.61	57	31	1.24	1.09	Not tested, $\overline{X}_B > \overline{X}_A$
IU	2.82	2.5	57	31	1.47	1.83	1.10
IURPC	2.44	2.51	57	31	1.76	1.98	Not tested, $\overline{X}_B > \overline{X}_A$

As you can see, there was only one question that supported the alternative hypothesis. The question was:

"Please indicate your level of concern about your own privacy for the given situation: You receive an email and have no idea how the company got your address."

I found that the results to 'Internet Users' Response to Privacy Concerns (IURPC)' questions had a mean score of 2.434 amongst the individuals who read article A and 2.51 amongst the individuals who read article B. Both groups expressed a willingness to make changes to the way they behaved online or proactively prevent future privacy intrusions between 'neither likely or unlikely' and 'somewhat likely'.

Since the results from my first hypotheses were scarce, I continued to test for the second hypotheses using the data from the two government trust questions. I followed the same procedure and conducted various t-tests. Any t-value that supported my alternative hypothesis was highlighted.

Figure 6: Government Trust Survey Question Results

Question	$\overline{X}_A$	$\overline{X}_B$	n_A	n_B	s_A^2	s_B^2	t
GM1	2.77	2.68	57	31	1.00	1.16	0.40
GM2	2.11	2.35	57	31	1.35	1.64	Not tested, $\overline{X}_B > \overline{X}_A$
GM3	1.88	2.48	57	31	2.07	1.72	Not tested, $\overline{X}_B > \overline{X}_A$
GT1	2.02	1.45	57	31	0.66	0.52	3.36
GT2	1.91	1.45	57	31	0.65	0.52	2.74
GT3	2.16	1.61	57	31	0.49	0.45	3.59

Figure 7: Aggregated Government Trust Survey Question Results

Block	$\overline{X}_A$	$\overline{X}_B$	n_A	n_B	s_A^2	s_B^2	t
GM	2.25	2.51	57	31	1.60	1.49	Not tested, $\overline{X}_B > \overline{X}_A$
GT	2.03	1.51	57	31	0.61	0.49	3.22

In this case, 3 questions supported the alternative hypothesis - all of which were questions from the same model, *Trust in Government NES Pilot Report,* with the same latent variable, Government Trust (GT).

Conclusion

For almost all of the questions we did not have enough evidence to reject the null hypothesis. The only result that concluded that the Wikileaks article increased concern for online privacy was the Internet Usage latent variable question "You receive an email and have no idea how the company got your address." Article A respondents had a mean response of moderate concern. Article B respondents had a mean response of somewhat low concern. It's likely that this is the result of random error since it seems to be an anomaly.

Since these questions were from previously tested scales, it's possible they were not specific enough to my study. While there was a lot of research on online privacy, and a fair amount on Wikileaks, there was no research previously conducted on the correlation of these two subjects. I chose this subject because of the relationship between the publications of Wikileaks and technology hacking. Many of the leaks posted by Wikileaks mention that private companies and government agencies are hacking into the phones, computers, and TVs of individuals. While the article mentions these facts, it appears as though awareness does not translate to unwillingness to disclose personal information online, as posed in some of the questions asked.

The second set of hypotheses were proposed because of the obscurity of my original hypotheses. 3 of the 6 questions asked regarding my second alternative hypothesis were significant. These results concluded that Wikileaks causes an increase in government distrust. I believe these results were more conclusive than my previous hypotheses because of their direct correlation to the Wikileaks article. Article A very explicitly mentions the various ways in which

the federal government is surveilling individuals. While one might assume that reading said information would cause distrust, it's never been previously tested.

There were quite a few limitations to my study, one of which being the method in which the surveys were distributed. Using personal Twitter and Facebook accounts, the groups who were exposed to the study were likely to be people who I knew and therefore could create bias. When these methods did not turn over enough responses, I posted the survey on Nextdoor, which is a private social network for members of my neighborhood community. In other words, all of the results came from individuals living in my local neighborhood of West Byram, New Jersey. It's likely that the limited geographical location could also cause bias. On top of that, only 89 responses were substantial enough to be included in my research. Over 32 responses were thrown out because they responded that they did not read the article, or they did not get more than one of the three comprehension checks correct. Lastly, one article A participant failed to answer the last question of the survey, and thus the n_A value changed, which may or may not have affected the data, though it would not have had enough effect to cause the hypotheses conclusion to change.

Were I to conduct further research into this subject, I would delve more into the relationship between government distrust and Wikileaks, instead of online privacy. I also would have considered creating my own scale to test the hypotheses, but this would take significantly more time and resources.

Works Cited

Bluman, A. G. (2009). *Elementary Statistics* (7 ed.). McGraw Hill.

Blumenthal, D. (2016). WikiLeaks and the Crisis of Government Communication. Govexec.Com.

Christensen, C., & Jonsdottir, B. (2014). WikiLeaks, Transparency, and Privacy: A Discussion with Birgitta Jónsdóttir. International Journal of Communication (19328036), 8, 2558.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17(1), 61–80.

Dolan, Emily A. (2012). Exploring privacy online social networks in civil cases. Paper presented at the International Communication Association.

Gershtenson, J., & Plane, D. L. (2007). Trust in government. American National Election Studies pilot report.

Hong, W., & L. Thong, J. Y. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1), 275–298.

Lynch, L. (2014). "Oh, WikiLeaks, I would so love to RT you:" WikiLeaks, Twitter, and information activism. *International Journal of Communication (Online)*, 2679.

Naresh K. Malhotra, Sung S. Kim, & James Agarwal. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336.

Pan, Y., Wan, Y., Fan, J., Liu, B., & Archer, N. (2017). Raising the Cohesion and Vitality of Online Communities by Reducing Privacy Concerns. International Journal of Electronic Commerce, 21(2), 151–183.

Quian, A., & Elías, C. (2018). Strategies and Reasons for the Impact of WikiLeaks on World Public Opinion. Revista Española de Investigaciones Sociologicas, (162), 91–110.

Sheehan, K., & Grubbs Hoy, Mariea. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising*, vol. 28, no. 3, pp. 37-51. *JSTOR*, www.jstor.org/stable/4189116.

Stoycheff, E. (2016). Under surveillance: examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. Journalism & Mass Communication Quarterly, (2), 296.

Yang, K. C. C., Pulido, A., & Yowei Kang. (2016). Exploring the Relationship between Privacy Concerns and Social Media Use among College Students: A Communication Privacy Management Perspective. Intercultural Communication Studies, 25(2), 46–62.