Preventing Covert Webcam Hacking in the Civilian and Governmental Sectors

Jayaram, Harshini	Lui, Jonathan	Nguyen, Peter	Zakarian, Sylvia
hjayaram@mit.edu	jlui@mit.edu	ptn24@mit.edu	sylviaz@mit.edu

May 14, 2014

Abstract: Over the past few years, webcam security has entered the national spotlight due to the increasing number of incidents in which a webcam was hacked by a malicious attacker, organization, or governmental agency. Because webcam hacking serves a variety of purposes—from the acquisition of photos and videos of a victim to the protection of national security—the need for a strong security policy that can delineate specific consequences for an individual hacker as well as provide oversight for governmental hacking is clear. In addition, the policy should deter future attacks and align with public opinion. This project aimed to raise awareness about webcam security issues and to design a security protocol based on public opinion. First, several well-known attacks on webcams as well as high-profile cases that involved webcam hacking were discussed. A survey was then generated to aggregate public opinion regarding the issues of webcam hacking and the policies and verdicts that surrounded the case studies. Some key issues addressed in the survey were **1)** *what is an appropriate level of punishment for different types of hacking* and **2)** *when is webcam hacking justified*. Based on the results, public opinion preferred more severe punishments for an individual hacker and stronger oversight with respect to governmental hacking. Finally, a security protocol was designed using the information gathered in the hopes of providing a fair policy that both aligned with public opinion and protected the privacy of the community.

Key words: Cassidy Wolf, clickjacking, FBI, Lower Merion School District, NSA, Trevor Harwell, webcam policy, webcam security

Contents

List of Figures

1 Introduction

Webcam security has become an increasingly important area of research over the past few years due to the ever-expanding presence of built-in webcams in commodity laptops and smart phones[1]. Webcams can be used for a variety of purposes: from holding casual conversations with friends and family to conducting professional meetings and interviews, and even to setting up a home surveillance system[2]. Although the integration of the webcam into daily life has facilitated long-distance communication as well as many other functions, the ubiquitous presence of the webcam has made it a prime target for malicious attackers. One of the most common questions posted on hack forums is: how can one disable the webcam's LED to enable the acquisition of covert photos and videos?

The widespread desire to disable the webcam's indicator LED illustrates the dangers associated with the use of passive sensors such as the webcam. Unlike active input devices like keyboards and mice that require direct user input, passive sensors require no action from the user to acquire input. Thus, specific mechanisms must be built into the passive sensor technology in order to alert users that the sensor is in use. In the case of a webcam, this mechanism is the indicator LED. When the LED is lit, users know that the webcam is active and can be acquiring input at any time. When the LED is off, users expect that the webcam is inactive and is not recording any input. As a result, the ability to disable the indicator LED while the camera is still active poses a serious security and privacy threat to the community.

Several mechanisms have been proposed to detect and prevent unprivileged webcam usage. From a hardware perspective, one method of defense is to connect the indicator LED circuit to the webcam in such a way that a hardware interlock enforces the LED to be lit when the camera is in use. From a software perspective, one possible method of defense is to install strong malware detection software in order to detect when a malicious attacker is attempting to gain access to the webcam and prevent the attack. Unfortunately, neither of these defenses has yet to prevent webcam hacking. To date, the best solution may be a low-tech one: to place a piece of tape over the lens when the webcam is not in use.

Although the ability to disable the indicator LED while the camera is in use can lead to serious privacy and security problems, the existence of legitimate use cases makes writing a satisfactory webcam security protocol an incredibly difficult task[1]. One use case is that users simply do not want the LED to be on while the camera is recording for aesthetic reasons. Another is that disabling the indicator LED may enable covert usage of the webcam to aid in laptop recovery after theft. Although the first use case may be a matter of opinion, the second use case has obvious communal benefits. The delicate balance between the costs and benefits of webcam hacking must be carefully investigated in order to establish a webcam security protocol that is fair and just.

This project aims to raise public awareness about webcam security issues and to design a security protocol based on public opinion to handle the improper usage of webcams in the United States. First, this project will provide a brief overview of webcam security by analyzing various attacks that have exploited webcam vulnerabilities and discussing several high-profile cases in the United States that involved webcam hacking. A survey will then be developed to raise public awareness about these cases and to aggregate public opinion regarding the security policies surrounding the cases and the legal verdicts that resulted. Finally, the results from the survey will be compiled and used to generate a public opinion-based webcam security protocol for future cases of webcam hacking. The results from this study can be used to establish webcam security policies that are not only fair and just but also protect the security and privacy of the community.

2 History of Webcam Security and Privacy

This project begins with a brief overview of various issues related to webcam security and privacy. We first investigate several known attacks that have been used to exploit vulnerabilities in webcam security as well as several mechanisms of defense against those attacks. Then we discuss several high-profile cases in the

United States in which a malicious attacker or organization was able to acquire covert photos and videos of victims, focusing on both the events that occurred and the legal verdicts that ensued.

2.1 Exploiting Webcam Vulnerabilities

Several well-known attacks against webcams exist, but this project will focus on three known attacks. For each attack, we provide an overview of the webcam vulnerability being exploited, describe a specific attack that exploits that vulnerability, and discuss possible mechanisms of defense as well as ways to circumvent those defenses.

2.1.1 Trojan Horse Attack Using a Remote Administration Tool

A remote administration tool (RAT) is a program that is generally used to covertly monitor a computer without the user's knowledge[3]. RATs can capture every keystroke inputted by the user as well as covertly record video by accessing a host's webcam. Although RATs can play an integral role in laptop tracking and recovery after theft by covertly snapping photos of the thief, RATs can also be used by a malicious attacker to capture photos and videos of a victim without his or her knowledge.

One possible attack on webcams that utilizes a RAT is a trojan horse attack. Users can unknowingly install a RAT onto his or her computer in many different ways: by opening an infected attachment, clicking on a download link, installing a new toolbar with granted permissions, and many more[3]. Once a RAT is installed, an attacker can easily access the host's webcam software and turn on the webcam at any time.

This type of attack can be detected and prevented in various ways. First, a strong, up-to-date firewall can protect a user's computer from most malicious software. Installing trusted anti-malware and anti-virus software can also aid in the detection and removal of most known RATs. In addition, a RAT infection can be detected with vigilance. When an IP port is unexpectedly opened on a host's computer, particularly when the port number matches that of a known Trojan[4], there is a strong possibility that there is a RAT infection. In the case of a RAT infection, the host computer should be disconnected from the Internet and anti-virus software should be initiated. The computer should not be booted in safe mode because doing so can prevent the RAT from loading into memory and being detected by the anti-virus software. Although the aforementioned methods have been shown to detect and prevent a trojan horse attack using many types of known RATs, the methods are far from perfect. Many RATs still manage to slip past the host's defenses and allow an attacker to gain unprivileged access to a victim's webcam.

2.1.2 Clickjacking Attack on Adobe Flash

Clickjacking is a malicious technique in which iframes are used to hijack a user's web session[5]. Clickjacking allows an attacker to subvert innocuous clicks from a victim and send them to target webpages that are subframed with or without the use of JavaScript[6]. Because the target webpage can be subframed without the use of JavaScript, simply turning off JavaScript does not prevent clickjacking and, in addition, nullifies the frame busting code—which is written in JavaScript—used to defend against clickjacking. A common method of clickjacking is to model the hack in the form of a game in which a user is lured into clicking on something that is different from what is directly perceived by the user (Figure 1)[5]. Because some clicks can be real game clicks while others are jacked clicks[7], it is often difficult to detect a clickjacking attack.

Clickjacking can be used by a malicious attacker to gain unprivileged access to a victim's webcam and allow the attacker to both listen in and view the victim at will[8]. One specific attack involves placing the Adobe Global Settings Manager page in an iframe and setting the iframe to invisible[9]. The Settings Manager page is a prime target for attack because it controls all security functions for the Adobe Flash player. In addition,

Figure 1 Visualization of a clickjacking attack modeled as a game on Twitter's account deletion page (Rydstedt *et al.*[5]).

the Settings Manager page does not require any user authentication, so it is easy to clickjack this page without the user's knowledge. With only a few clicks, the user can unknowingly grant an attacker full access to the user's webcam. To facilitate the attack, an attacker can also ensure that the mouse is always placed in the correct position by hovering the iframe beneath the mouse pointer (Figure 2)[8].

Frame busting is the recommended defense against clickjacking[5]. Frame busting is code provided by a webpage that is intended to prevent the page from being loaded in an iframe or other subframe. By placing frame busting code in the Settings Manager page, an attacker is no longer able to place the page in an iframe and clickjack a victim. However, the defense can be circumvented if an attacker loads only the Adobe settings SWF (Small Web Format) file into the iframe[9]. Because the frame busting code is only present in the main page, this circumvention allows an attacker to bypass frame busting and still gain access to a victim's webcam. Although this circumvention has been blocked by Adobe, there are still many ways to bypass existing defenses.

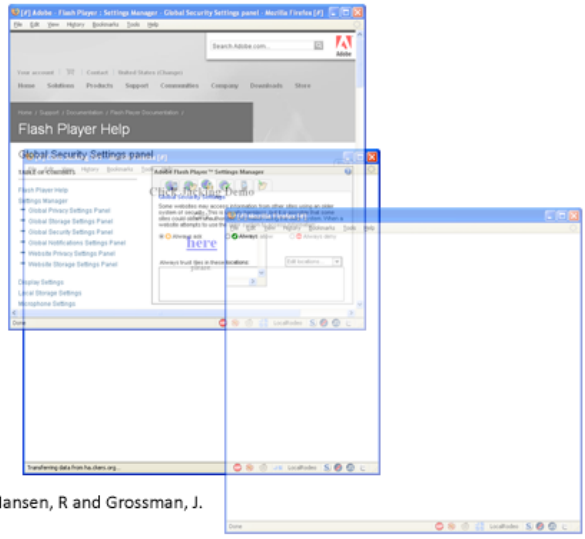

Figure 2 Visualization of a clickjacking attack in which the iframe is made to hover beneath the mouse pointer (Hansen, R and Grossman, J[8]).

2.1.3 Firmware Reconfiguration and Virtual Machine Escape

A recent study by Brocker and Checkoway in 2008 demonstrated that video could be captured on several MacBook and iMac models produced prior to 2008 with the webcam indicator LED disabled[1]. This finding presented a serious security and privacy threat to the community because the indicator LED functioned to alert users that the webcam was in use and could be recording input at any time. In the study, Brocker and Checkoway aimed to describe the architecture of the Apple internal iSight webcam used in the aforementioned computer models; to demonstrate how to bypass the hardware interlock that turns on the indicator LED in order to disable the LED while the webcam is in use, and to build a proof-of-concept (PoC) user space application to do so; to perform a virtual machine (VM) escape that can execute shell commands from user space and enable malware to

reprogram the webcam to act as a USB human interface device (HID); and to design a model for building more secure webcams as well as build a PoC application to defend against attacks.

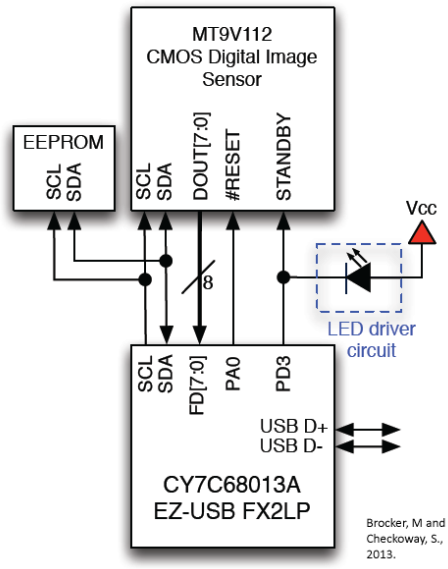

Figure 3 Architecture of the internal iSight, consisting of a Cypress EZ-USB microprocessor, a Micron digital image sensor, a 16-byte configuration EEPROM, and an indicator LED.

The architecture of the internal iSight consists of a microprocessor, a digital image sensor, an EEPROM, and an indicator LED (Figure 3). When the image sensor transmits an image to the microprocessor, a hardware interlock forces the LED to become illuminated. More specifically, when the image sensor is in use, pin `PD3` is low, thereby deasserting `STANDBY` and illuminating the LED. When the image sensor is turned off, `PD3` is switched to high, which asserts `STANDBY` and turns off the LED.

Brocker and Checkoway demonstrated that the microprocessor could be reprogrammed with new firmware to allow the image sensor to be reconfigured to bypass the hardware interlock to the LED and developed a PoC user space application (*iSeeYou*) to do so. To disable the LED while the webcam is in use, an attacker must **1)** configure the image sensor to ignore `STANDBY` because `STANDBY` must be asserted in order to turn off the LED and **2)** reprogram the microprocessor with new firmware in order to maintain normal function while asserting `STANDBY` (`PD3` high). Brocker and Checkoway were able to use *iSeeYou* to successfully disable the indicator LED and record covert videos using the internal iSight webcam.

In addition to performing an attack on the iSight webcam, Brocker and Checkoway also developed a defensive mechanism against such attacks called *iSightDefender*. *iSightDefender* functions to block all user space reprogramming attempts against the firmware of the iSight webcam, including those mounted from within a VM. Although *iSightDefender* represents one of the strongest possible software-based defenses against a VM escape aimed at reprogramming the webcam from user space, any malware with root access can successfully bypass the hosts defenses from kernel space. As such, the best defense is still a hardware-based defense or a low-tech solution.

2.2 Case Studies

There have been several high-profile attacks on webcams in the past couple of years. The attacks ranged in severity and nature, thus resulting in varying degrees of punishment from the judicial system. We choose to analyze four cases in which attacks were successfully performed on webcams.

2.2.1 Miss Teen USA - Cassidy Wolf

In 2013 Miss Teen USA, Cassidy Wolf, had her e-mail, social media accounts, web camera, and entire computer hacked by an attacker. The attacker, Jared Abrahams, was a first year student and he attacked multiple victims all over the world. He was diagnosed with autism and doctors say he has the maturity of a 12 year-old.

The events leading up to Miss Cassidy Wolfs extortion are no different from situations that could happen to other civilians. For almost an entire year Miss Cassidy Wolf was actually unaware that her accounts and laptop had been compromised by an attacker. She realized that her accounts and laptops had been

compromised when she received an e-mail from the attacker. The e-mail had several requests such as sending nude photos or undressing in front of the camera for the attacker. Miss Cassidy Wolf did not believe the e-mail until she scrolled down to the bottom of the e-mail to find photos of her that had been taken through her webcam. She realized that the attacker had been stalking her for almost one year.

The case was reported to the FBI and an investigation led to the attacker being caught. Abrahams attended a therapeutic program for adults with autism at UCLA and also enrolled in another program at Loma Linda University Medical Center. His autism and the diagnosis of his maturity level heavily influenced the courts ruling for his sentence. He was ultimately sentenced to 18 months in prison and three years of restrictive supervised release which includes restrictions on his computer use. As an example of how Abrahams disabilities worked in his favor, U.S. Attorney Vibhav Mittal actually advocated for a 21-month sentence. However, U.S. District Judge James Selna stated that Abrahams medical health and age justified a shorter sentence of 18 months.

2.2.2 Lower Merion School District

In February 2010 Blake J. Robbins, Michael E. Robbins, and Holly S. Robbins decided to sue the Lower Merion School District for its actions in a case dubbed WebcamGate scandal. In this case a 15-year old high school sophomore, Blake Robbins, was disciplined at school for his use of drugs at home. When he was punished for his actions at home he realized that the school had been illegally spying on him without his knowledge.

At the start of the 2009-2010 school year the Lower Merion School District started an initiative to issue Apple MacBook computers to high school students for educational purposes. The laptops were meant to be used in school and at home. As part of the distribution process the school district decided to install tracking software, TheftTrack, in order to locate a computer in the case that it were to go missing. However, the school did not notify students and families that this software were installed on the laptops. Not only did they not give notice that the software was installed but they also did not give notice that they would be taking thousands of images, screenshots, and videos through the software.

In total the school took more than 58,000 photos from November 2008 through February 2010. The details are very garbled and inconsistent but the school technician Kyle OBrien testified that the Harriton High School Assistant Vice Principal Lindy Matsko directed OBrien to activate and use the tracking software. Over a 15 day period, 210 web camera photos and 218 screenshots were taken. The information captured ranged from photos of Robbins sleeping, photos of his father, to screenshots of his chats. When Matsko received pictures of Robbins using and distributing drugs in his room she decided to call Robbins into his office and discipline him for his improper behavior.

In July 2010 another student, Jalil Hasan, decided to sue the Lower Merion School District regarding over 1,000 images that were captured from his computer over a 2 month period. Hasan misplaced his laptop in December and it was found by a teacher. He retrieved the laptop but was not informed that the TheftTrack software was re-activated. It was not until several months later that the school district notified Hasan that the TheftTrack software had been capturing images and screenshots from his computer.

Both the Robbins and Hasans lawsuits against the Lower Merion School District resulted in a total of $610,000 in settlements. No one was fired from the school district nor were there further lawsuits taken against the school districts actions.

2.2.3 Trevor Harwell Case

In 2011 Trevor Harwell was able to covertly take photos and video of victims through their webcams. Harwell was a repair technician for a computer company, Rezitech Inc. Since Harwell worked as a computer repair

technician he was able to install spyware on some of the computers. The spyware would cause an error message to pop up on users screens. The error message would indicate that users should put their laptop near hot steam for several minutes in order to clean the sensor. As a result, several of the victims followed the instructions and proceeded to bring the laptops to the restroom while they showered.

When the victims brought their laptop into the restroom Harwell would take photos of the victims and send them to a remote server where he could later download the photos to his personal computer. Harwell faced 12 felony counts and used software called CamCapture to upload the images to the remote server. The lawsuit resulted in 1 year in prison for Trevor Harwell. He was not required to register as a sex offender for his actions.

2.2.4 NSA Webcam Hacking

The National Security Agency has the mission of confronting formidable challenge and preventing foreign adversaries from gaining access to sensitive or classified national security information. Data was just released from Edward Snowden stating that the National Security Agency has been posing as Facebook in order to gain access to millions of computers worldwide.

The National Security Agency constructed a fake Facebook server and used Facebook as a launch pad to infect computers all over the world. The NSA was able to covertly record audio from computers and take snapshots through the webcams. The NSA had no explicit reason to launch such an industrial scale attack. Facebook was unaware of the NSAs malware infection attack and has since protected itself against the problem.

Between 2008 and 2010 the NSA also worked with Britains GCHQ to run a program, Optic Nerve in which they covertly intercepted webcam imagery from 1.8 million Yahoo users globally. According to zdnet, the NSA and Britains GCHQ were running the program to monitor existing suspects and to discover new targets of interest. A significant amount of the images captured were explicit. Yahoo released a statement that they did not take part in the attack.

3 Aggregating Public Opinion

3.1 Survey Design

The survey was designed to inform our team about public opinions surrounding webcam hacking. Using this information, we wanted to create a policy which would better align public opinion and policy. Given the cases coming into the spotlight about webcam hacking, we wanted to help form policy that would guide rulings in cases such as those. To this end we designed a survey which would inform us of public opinion so our policy can be an accurate representation. Views on webcam hacking are very hard to gauge generally - few would disagree that it is immoral, or that they would punish violators. The clearest method was to take existing cases with lots of concrete details, and ask how individuals react to those cases.

When considering past cases, especially those explained above, it became clear that there were two different categories of webcam hacking: that done by civilians and that done by the government. The crime when committed by civilians resulted in fines, jail time, and punishment in that realm. However, when the government used hacking, the question changed to whether the action is illegal, and what the oversight should be. Hence we structured our survey into two sections accordingly, one considering civilian hacking and one regarding the government.

In the survey, we gave participants basic information about five different cases: an outline of the situation and punishment or outcome. While there were many more examples, we wanted to limit the length to

encourage greater participation. We also wanted to dig into public opinion by understanding the reactions people had to different cases. To do so, we asked several types of questions: 1) What the punishment should be for the situation, 2) How do specific American laws relate to the situation, and 3) How do people feel morally about the use of this technology. One key aspect of our survey, made clear to participants, was that we did not want them to guess the actual outcome of situations or rulings made relating to the cases. Instead, we asked for what they thought was fair. Again, this will help with the goal of aligning opinion and policy.

Please note that we did not request that participants refrain from outside sources. It is highly unlikely anyone consulted outside material, but we were open to them getting more information to inform their decision if they wanted.

When considering webcam hacking in the civilian sector, we focused primarily on the first type of question - determining what is considered an appropriate punishment for a given crime. Though our options would naturally frame the expectations of participants, we tried to make them broad enough to not be misleading.

When the government employs hacking techniques, they are not typically subject to the same penalties as civilians, so here we focused more on the second two types of questions: how laws apply to the cases, and whether the use of these technologies is just.

3.2 Limitations

Although we tried our best to design an unbiased and informative survey, our survey does have some limitations. The first limitation is the amount of text that was present on the survey. There were several questions for each case and it was crucial that our survey responders understood the case scenarios to the best of their abilities. As a result, we included a background of each case before each major section. The wordiness and length of the survey could have deterred some responders from putting in their full effort to answer the questions.

Another limitation of the survey is the terminology used. Some of the terminology was slightly more complicated than the everyday use. For example, one survey responder was an international student and informed us that he did not understand the term due process of law. Due process of Law is a term that is mainly used in the United States. As a result, it is possible that several of our responders selected a random answer for the questions that they did not understand.

A third limitation of the survey is the target audience. For our research purposes the broadest range of users is ideal. Our goal is to have responders of all genders, all regions, and all political stances. However, the four team members of this project are all MIT students. As a result, a significant portion of our responders were students attending the Massachusetts Institute of Technology.

4 Survey Results

In this section, we discuss the results of the survey. As previously stated, we asked our participants 18 questions related to webcam security policy followed by 3 demographic questions. These questions were arranged by case, and results are explained below. Detailed graphs of questions with responses are included in Section 8.

4.1 Miss Teen USA

The first question asked about how much time the participants thought that the perpetrator in the Miss Teen USA case should have spent in jail, and were given 4 options. He received 18 months in jail, and 40% of people thought he should have received less (6 or 12 months), 35% thought he should receive more time (18 months), and 25% agreed with this. The actual ruling is very much in the middle of public opinion, indicating that this is already well aligned. Thus we want to replicate this close match between policy and public opinion in other cases, and make sure our policy does not change the rulings made in this case.

4.2 Lower Merion School District

The second set of questions considered the Lower Merion School District case.

We first asked the participants how much they thought the district should have been fined for their misdeeds. 68% of the responders said that the district should have been fined over $600,000, which is the amount the school was actually fined. 36.8% of responders believed that the fine should have even been over $1,000,000. This is an example of a case in which the penalty seemed to be too low. Aside from indicating that the judicial system made a decision not aligned with public opinion, it could be that the penalty is too low as a deterrent against future attacks. Public opinion on a fine indicates what they think the action is worth. If the cost of taking a certain action is not high enough, it will not prevent future attacks because the benefit of taking the action outweighs the consequence.

Our second question asked if a fine was an appropriate punishment for the school district. The response to this question was very divided, with 52% of people believing that a fine was not appropriate. It is difficult to draw any conclusions from these results because the question does not give us any information as to why the participant believed a fine to be inappropriate. Possible reasons could include that they thought they should have been punished in a different way entirely, they should have faced another punishment on top of the fine, or that the district should not have been punished at all. This question currently does not provide enough information to impact in our policy recommendation.

Third, we asked the participants if they would still use the laptop if they knew that the school could access the laptop camera, and 74% of people said they would not. This is a very interesting result because knowing that the camera can be remotely accessed allows users to control what the camera can access. This implies that there is also a moral aspect to consider in this case beyond fear of being recorded. Several of the responders felt that they could not accept the computer simply because they know someone else can access the computer.

4.3 Comparison of Miss Teen USA and Lower Merion

We next asked participants to determine whether or not they thought what was fair or not about the rulings in these cases Figure 4. It is interesting to note that only 9% of the responders believed that the ruling in both cases was fair. This largely validates our study, showing that people do believe there is large room for improvement in court decisions surrounding cases like the ones presented here. Policy can help make that adjustment. Looking at the number of people who believed that an individual in the school case should have been held accountable (fired or gone to jail) shows one specific set of improvements we can recommend: individuals responsible for hacking should face a penalty themselves.

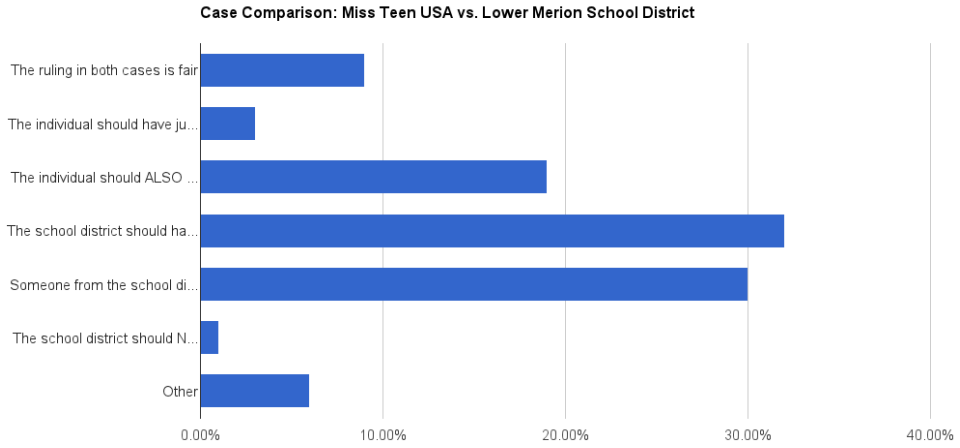

Figure 4 The graph above displays statements regarding the Miss Teen USA and Lower Merion School District court cases. These statements refer to either or both of these two cases. The graph shows the percentage of people who agree with each of the statements.

4.4 Trevor Harwell

Our final questions about cases in the civilian sector focused on the Trevor Harwell case. In the first question, we asked the participants if they felt that the company Harwell worked at, Rezitech Inc, should face punishment if it turned out that Harwell has used his position at the company to help him execute his crime. The vast majority, 69%, believed that the company should not be faulted in any way. Reasons for this could include that people felt that even if Harwell did use his position at Rezitech to commit the crime, he acted of his own accord and the company should not be punished because of him. This will have implications in our policy recommendation about liability between different parties. The second question asked how much time they thought Harwell should spend in jail. 78% of responders believed that Harwell should have spent a year or more in jail. Coincidentally, this is almost exactly the same as the number of people who believed that the Miss Teen USA perpetrator should have spent at least a year in jail. These cases do have similarities, and this suggests a minimum jail time for violations of this nature. Finally, the third question of this set asked if the participants felt that Harwell should have been required to register as a sex offender, given that he took photos of people in various states of undress. An overwhelming 86% of responders thought that he should be required to do so, a striking contrast to the fact he was not required to register. This will lend itself to a look at the laws surrounding registering sex offenders in order to establish why there is such a striking difference between public opinion and the decision made in this case.

4.5 NSA

Next the survey shifted to the use of webcam hacking techniques by government agencies, and we started by considering the NSA.

The first question explained the difference between the US and UK policies on data collection, and asked the participants which policy they thought better protected the rights of individuals. 81% of responders said that they preferred the UKs policy, which states that the government must get extra warrants to access user data, compared to the USs policy that the government must minimize the amount of data collected. The

UK is a close ally of the US, and perhaps this suggests that the US should consider adopting a more similar strategy to the UK in this case. The implications are further discussed in our policy recommendation.

The second question asked if people felt that the NSA and FBI should be granted similar permissions in terms of hacking webcams. 62% of people thought that they should be granted similar permissions. In this case, it would seem that the public does sees the NSA and FBI as similar entities who should have the same rights, even though they are quite different. Perhaps the government should clarify what these two organizations are and why they are distinct, helping the pubic have a more informed and accurate impression. In this case, we believe that the public dissent with the different oversight of the two agencies does not entirely suggest a restructuring by the agencies, but rather that the government should have stronger communication to explain the differences.

The third and final question in this section asked the participants about the legitimacy of certain reasons for the Department of Justice not to share details with the Senate - something that has happened in the past. The results are summarized in Figure 5. It was interesting to note that 20% of responders believed that the bi-partisanship of the Senate slowing things down was enough of a reason for the Department of Justice not to share information with them which is a reflection on political views overall. The question had limited sets of options—given additional time we may have been able to create a stronger and clearer question whose results could better inform our recommendation.

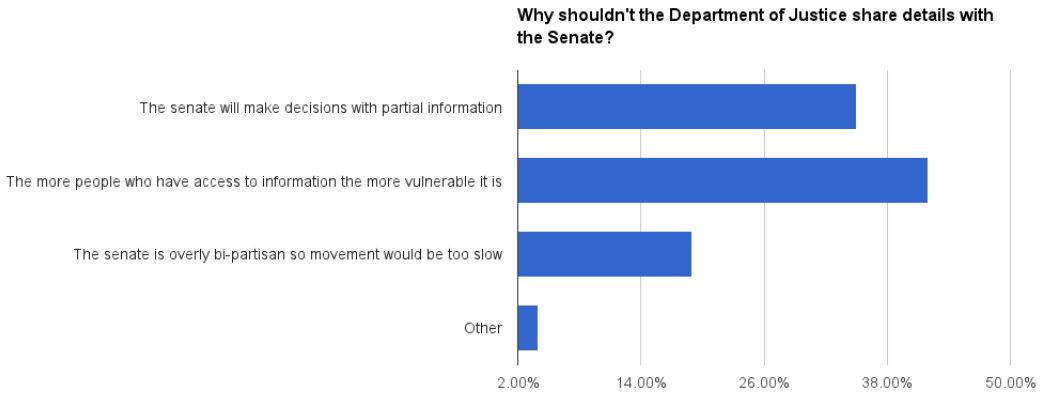

Figure 5 The graph above displays possible reasons why the Department of Justice would not share details with the senate, and the percentage of people who believed that each reason is legitimate.

Next we turned to the specific case where the NSA posed as Facebook to infect computers and get access to the webcam. First we inquired how frequently people thought it was okay for the NSA to use this tactic to gain access to peoples files. On a spectrum from 1 to 7, with 1 being never and 7 being always, 81% of people were on the lower end of the spectrum (1-3), leaning more towards never, results summarized in Figure 6. The second question of this set dealt with the amount of oversight the NSA should have in their use of hacking. On a scale from 1 to 7, with 1 being needing a warrant for every attack, and 7 being no oversight needed, 88% of people were on the lower end (1-3) of the scale. Results are in Figure 7. The results to both of these questions show the difference between public opinion and what is actually happening, showing a desire for stronger oversight and greater limitation on the use of these techniques.

4.6 FBI

The sixth set of questions were focused on the FBI. The first question asked the participants if they thought that the FBI should have to reveal that they had the capability to turn on a computers camera without

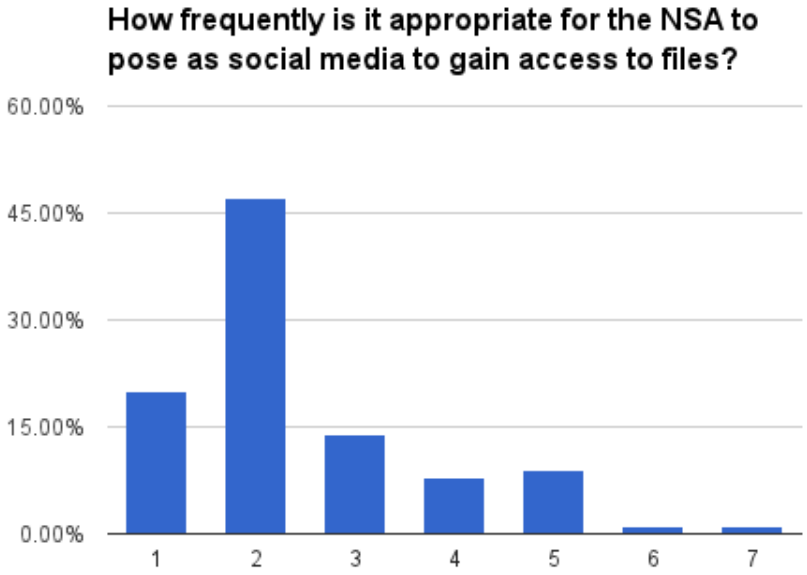

Figure 6 This graph displays the spectrum of responses regarding how frequently people believe it is appropriate for the NSA to pose as social media to gain access to peoples files, audio, and video. On the x-axis, 1 represents never and 7 represents okay on anyone, anytime.

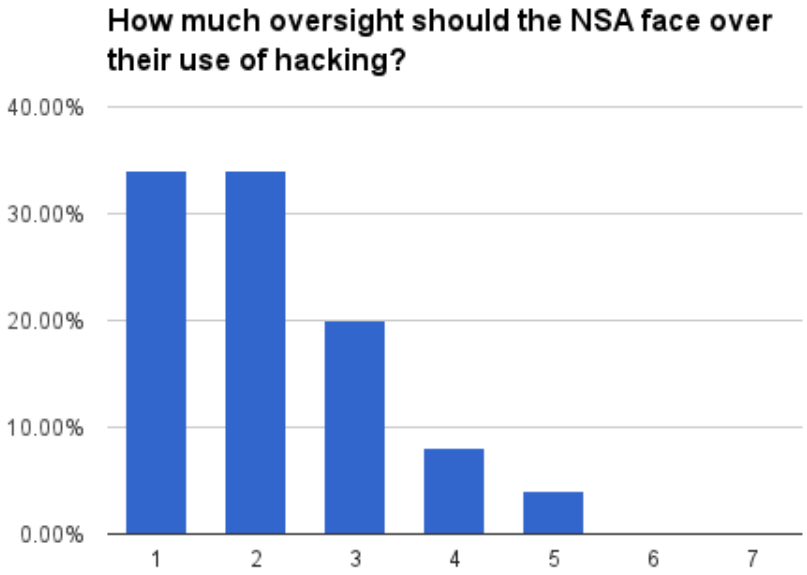

Figure 7 This graph displays the spectrum of responses regarding the amount of oversight people believe the NSA should face over their use of hacking. On the x-axis, 1 represents needing a warrant for every attack, and 7 represents not needing oversight.

activating the indicator light. 83% of people said they felt that the FBI should have to reveal this information. However, when asked if the FBI should still have to disclose this information given that they use the capability infrequently and uses it to deal with terrorism threats, only 56% of responders said that they should still have to. Knowing that the FBI is attempting to use hacking for good purposes made many people reconsider their first choice, showing the importance of transparency and trust. Finally, when asked how permissible it was that the FBI use this technology, given that they have not been successful in catching terrorists, the results were all over the spectrum, in Figure 8. Thus approval of the use of these techniques is not clearly correlated to the accuracy, which is an interesting note.

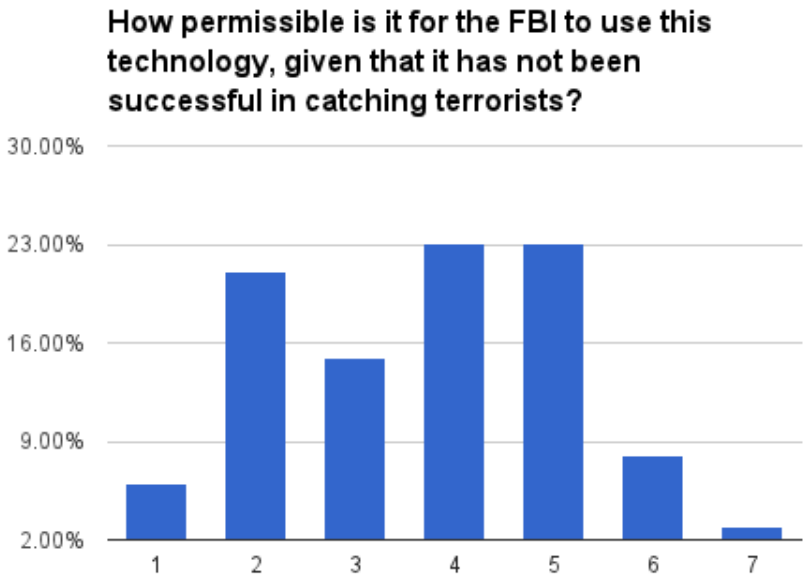

Figure 8 The graph above displays the spectrum of responses regarding how permissible people thought it was for the FBI to use hacking, given that it has not been successful in catching terrorists. On the x-axis, 1 represents that the technology should never be used, and 7 represents that it should be used according to existing policies at any time.

4.7 General Policies

Finally, we looked at laws and general policies potentially relevant to these cases. The first question asked the participants how strongly they thought the Fourth Amendment applied to cyberspace. In general, people felt that clearly applied to cyberspace, with 83% of people on the upper half (5-7) of the scale. Finally, we asked if the participants felt since government agencies often need approval from a judge or court to hack, that this is due process of law. The results for this question were all over the map, shown in Figure 9, but did tend towards the middle of the spectrum. This is another area where further clarity could help with public opinion.

5 Policy Recommendation

This study was motivated with the goal of creating a policy recommendation. With such striking results, there are several recommendations we can make. Because the civilian and government sectors are treated

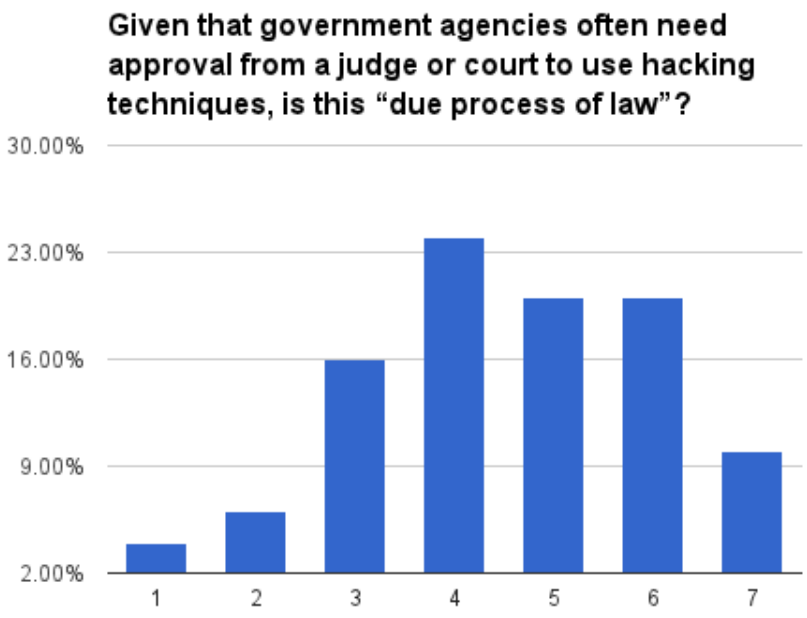

Figure 9 This graph displays the spectrum of responses regarding whether people believe it to be due process of law if government agencies often need to get approval from a judge or court before using hacking techniques. On the x-axis, 1 represents it not being due process, while 7 represents it definitely being due process.

differently, our policy recommendation handles each case separately.

5.1 Civilian Sector

The most striking result through this survey is that public opinion often believes in much harsher penalties than those that currently exist, potentially helping create a stronger deterrent against future attacks. Below are specific recommendations based on the cases we used as examples.

5.1.1 Miss Teen USA Case

The judicial system rulings were moderately well aligned with public opinion in this case, though more lenient. This case did not generate any specific policy recommendations, though similar cases should also consider a fine or more jail time as a stronger deterrent.

5.1.2 Lower Merion School District Case

The school district should have faced much harsher penalties. This crime should have faced a larger fine. In addition:

1) If an organization is employing webcam hacking techniques, individuals should also be held accountable.

Many people wanted to see the individuals involved with this scandal to be fired or jailed. The crime was committed by individuals through an organization, thus they too should be held accountable.

5.1.3 Trevor Harwell Case

In this case, Harwell took pictures of people in various states of undress and was sentenced to 1 year in jail. He was not required to register as a sex offender. Based on our survey results, we have three recommendations to make:

1) True to existing policy, if a company takes reasonable measures to prevent employees from misusing their positions to exploit customers from hacking attacks, the company should not be punished for employee actions. This is based on the strong response against punishing Rezitech Inc. for giving Harwell access to the machines.
2) Abusing a professional position to hack into machines and take illicit images and videos deserves a punishment of at least one year in jail. This was the popular opinion.
3) A perpetrator who uses webcam hacking to take images of people in various states of undress should be required to register as a sex offender.

Each of these recommendations is based on popular opinion but ties to existing policy. The first is already installed. For the second, it suggests that current punishments are too lax. Perhaps by making them more stringent, not only will the punishment seem more fitting for the crime, but potential adversaries will be deterred by the worse prospects if caught. The third recommendation is actually an extension of many existing laws. Currently covertly taking pictures of an individual undressing is considered a tier 1 sex offense, yet this case showed that the crime is treated differently if pictures are taken through cyberspace. This rule could clarify the existing definitions for tier 1 sex offenses.

5.2 Government Sector

Throughout these questions, it seemed that there was clear dissatisfaction with many existing policies and oversight procedures.

5.2.1 Changing Policy

The NSA should be much more conservative with its webcam use:

1) Webcam hacking should be used as a last resort, thus with less frequency
2) The NSA should need a warrant in order to hack into any webcam

Overall, people feel that the NSA has too broad a reach with too little oversight. Making these two changes will help address a wide array of concerns held by the public.

5.2.2 Changing Public Opinion

While we have outlined potential ways to better align public opinion and policy, we realize there is a large amount of information not available that will influence these decisions. In the event that policies cannot

change, we recommend that policy makers attempt to be more transparent about any of the reasoning behind existing policy. More generally:

1) Have clear and transparent guidelines for the use of personal information such as covertly obtained pictures and videos.

The importance of transparency and oversight was clear through answers to the FBI questions. Without much background information, people wanted the FBI to be more transparent about its use of this techniques. However, when informed that the FBI uses webcam hacking sparingly, the number of people who wanted disclosure from the FBI dropped a full 17 percentage points. In addition, even with the added information that it has not always been successful, people were very divided whether or not these techniques should be allowed. This stands in sharp contrast to the way that overwhelmingly the NSAs use of this technology was voted against. Thus without compromising security, public opinion and government practices can become better aligned.

6 Conclusion and Future Work

In summary, this project raised awareness about webcam security issues and designed a security protocol based on public opinion to deal with webcam hacking in both the civilian and governmental sectors. A survey was used to gather public opinion regarding webcam hacking and the security policies surrounding several high-profile cases that involved webcam hacking. Using the data from the survey, we proposed several policy recommendations that can be used to design a webcam security policy that can effectively protect the privacy of the community and deter webcam hacking at large.

Webcam hacking is a phenomenon that is beginning to capture many recent headlines as webcam vulnerabilities are being exploited by both individual attackers as well as governmental agencies. Whether webcam hacking is used to achieve good or evil deeds, it is certainly important to have a strong security protocol in place that clearly outlines the restrictions on governmental hacking and the consequences of unauthorized hacking by any individual, organization, or governmental agency. In addition, the security protocol must be stringent enough to not only detect but also deter future webcam hacking.

Although our security recommendations are aligned with public opinion, there is still much work to be done before a strong protocol is in place. In the future, we aim to further stratify the results from our initial survey based on demographic information in order to design a security protocol that better meets the needs of every individual. In addition, we aim to improve the structure of our survey in order to elicit more accurate and unbiased responses from the survey respondents. Furthermore, we can include more diverse case studies in the survey in order to better understand the motivating factors behind the results and cross-reference the results from a single respondent for consistency purposes. Nonetheless, we believe that our security protocol is well-aligned with public opinion and that the results from this project lay the foundation for the future design of security protocols that can protect the security and privacy of the community in the face an ever-expanding threat against webcams.

7 References

1) Brocker, M and Checkoway, S. iSeeYou: disabling the MacBook webcam indicator LED. Dec 2013.

2) Online: http://articles.economictimes.indiatimes.com/2013-07-22/news/40727952_1_webcam-lapse-mac-app

3) Online: http://robertsiciliano.com/blog/2010/03/02/rats-are-committing-identity-theft-via-webcams/

4) Online: http://technet.microsoft.com/en-us/library/dd632947.aspx#EDAA

5) Rydstedt, G, Bursztein, E, Boneh, D, and Jackson C. Busting frame busting: a study of clickjacking vulnerabilities on popular websites. 2010.

6) Online: http://ha.ckers.org/blog/20081007/clickjacking-details/

7) Online: http://blog.guya.net/2008/10/07/malicious-camera-spying-using-clickjacking/

8) Hansen, R and Grossman, J. Clickjacking. Sept. 2008. URL: http://www.sectheory.com/clickjacking.htm

9) Online: http://feross.org/webcam-spy/

8 Appendix

8.1 Miss Teen USA Case

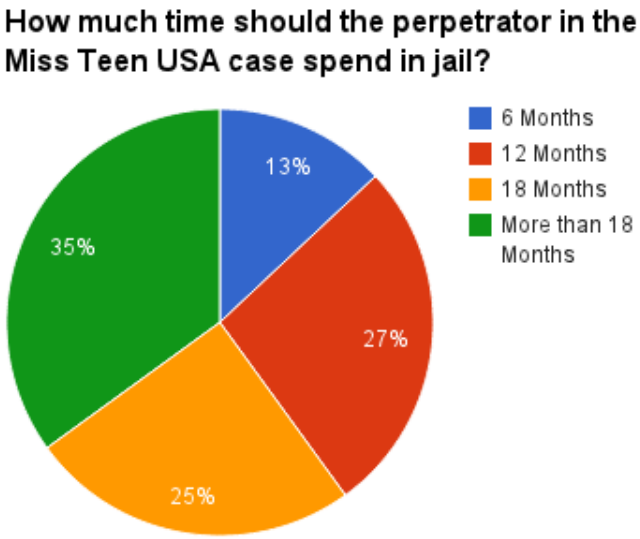

Figure 10 This pie chart displays how long people felt the Miss Teen USA perpetrator should have spent in jail.

8.2 Lower Merion School District Case

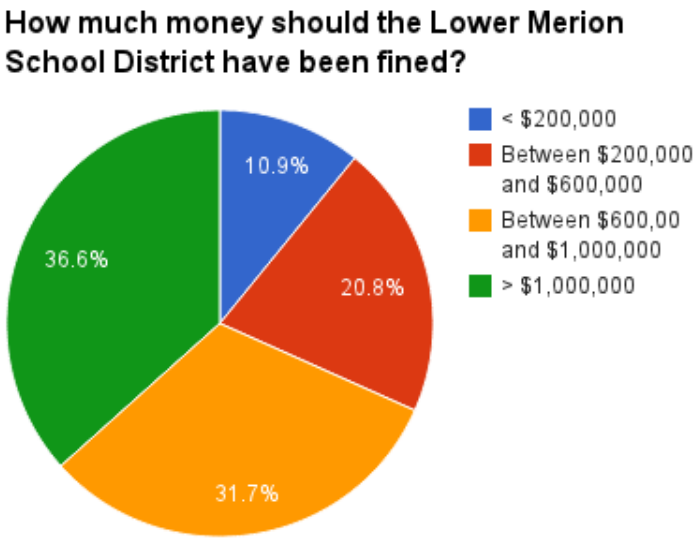

Figure 11 This graph displays how much money people felt the Lower Merion School District should have been fined for their crime.

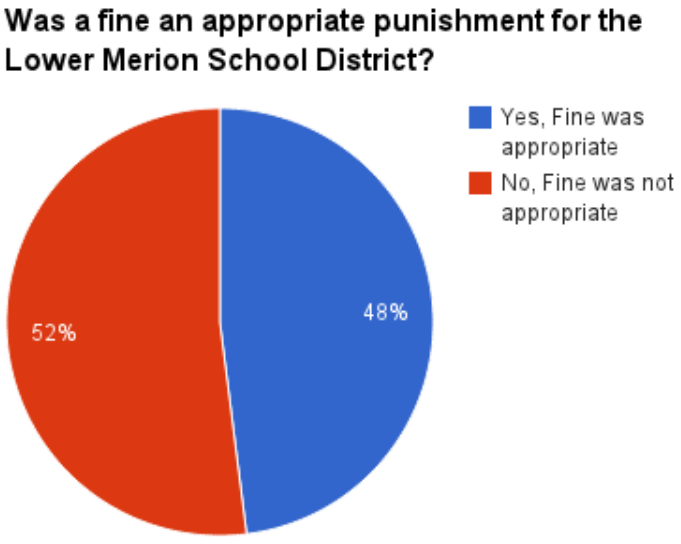

Figure 12 This graph shows the percentage of people who believed that a fine was an appropriate punishment for the Lower Merion School District.

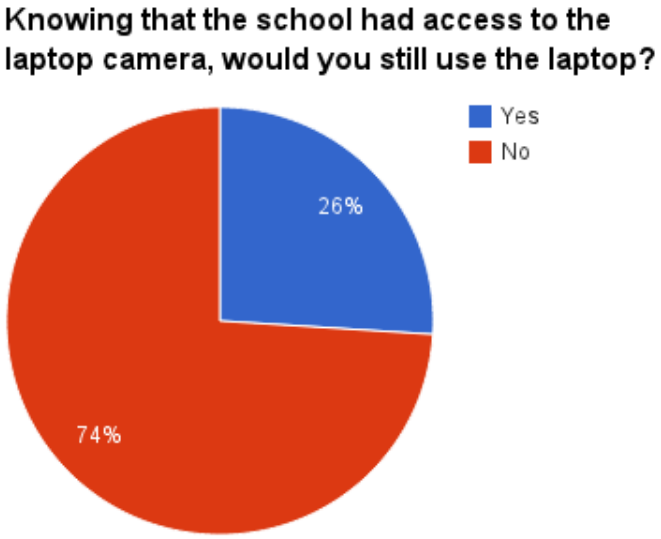

Figure 13 This graph displays the percentage of people who would still agree to use a laptop given to them by the school district, knowing that the school had access to the camera.

8.3 Trevor Harwell Case

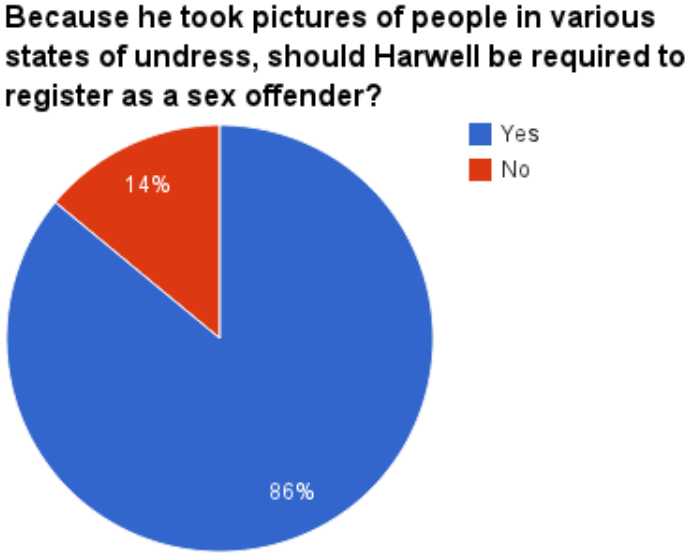

Figure 14 This graph shows the percentage of people who believe that Trevor Harwell should be forced to register as a sex offender.

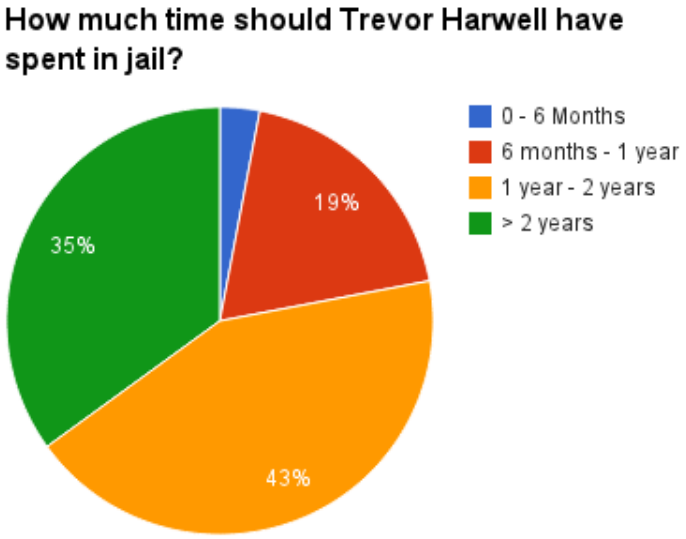

Figure 15 This graph displays how long people felt that Trevor Harwell should have spent in jail for his crime.

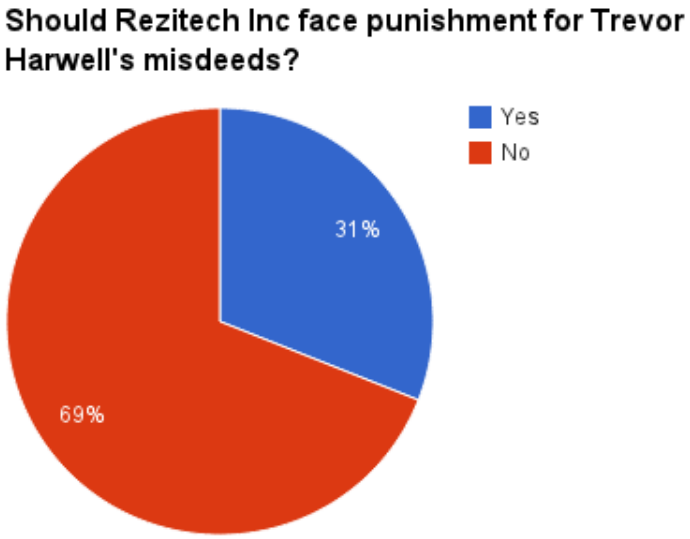

Figure 16 This graph shows the percentage of people who believe that Rezitech Inc, the company Trevor Harwell worked for, should face punishment because of his crimes.

8.4 Governmental Agencies

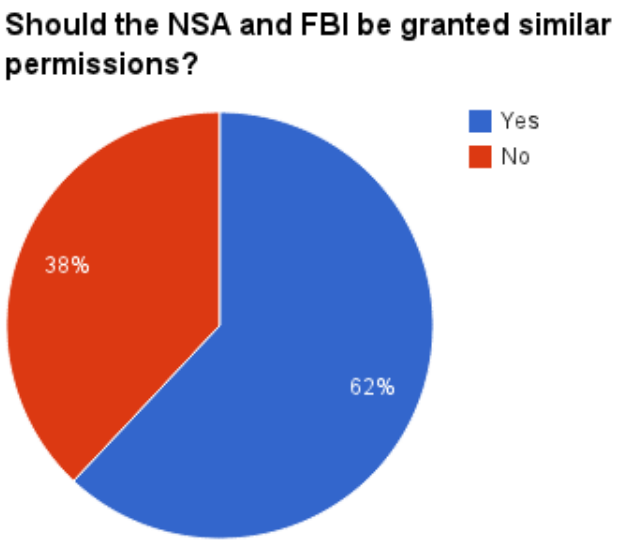

Figure 17 The graph shows the percentage of people who believe that the NSA and FBI should be granted similar permissions.

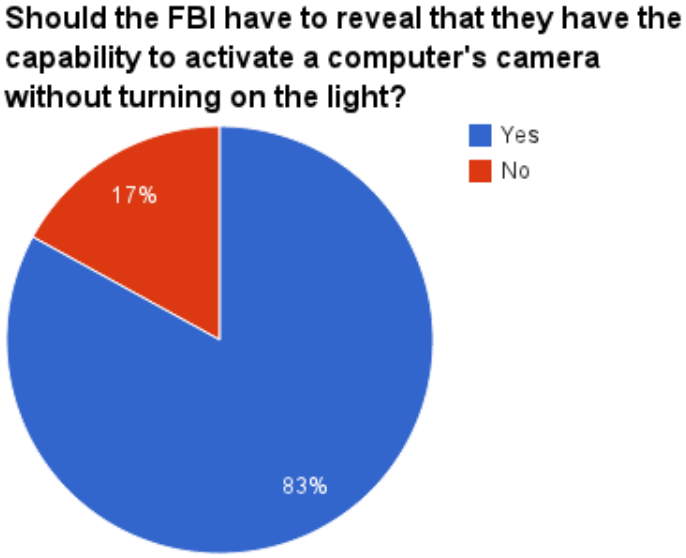

Figure 18 The graph displays the percentage of people who feel that the FBI should have to reveal that they have the capability to activate a laptops camera without turning on the indicator light.

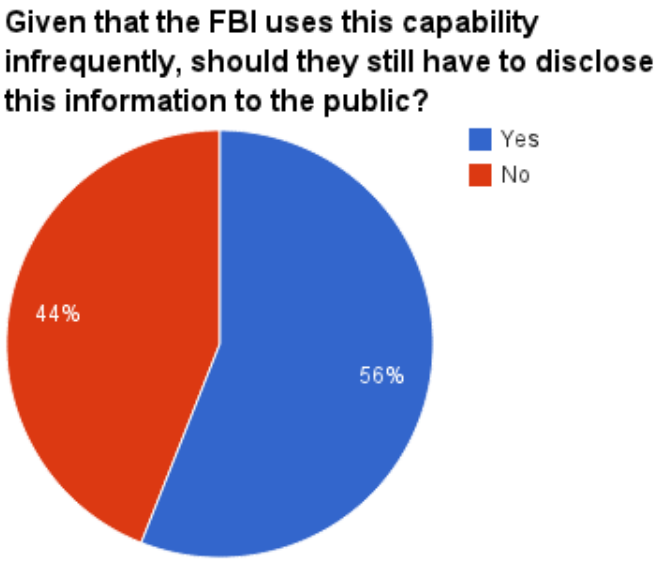

Figure 19 The graph displays the percentage of people who feel that the FBI should have to reveal that they have the capability to activate a laptops camera without turning on the indicator light, after knowing that FBI uses this capability infrequently and uses the method in an attempt to deal with terrorist threats.

8.5 General Policies

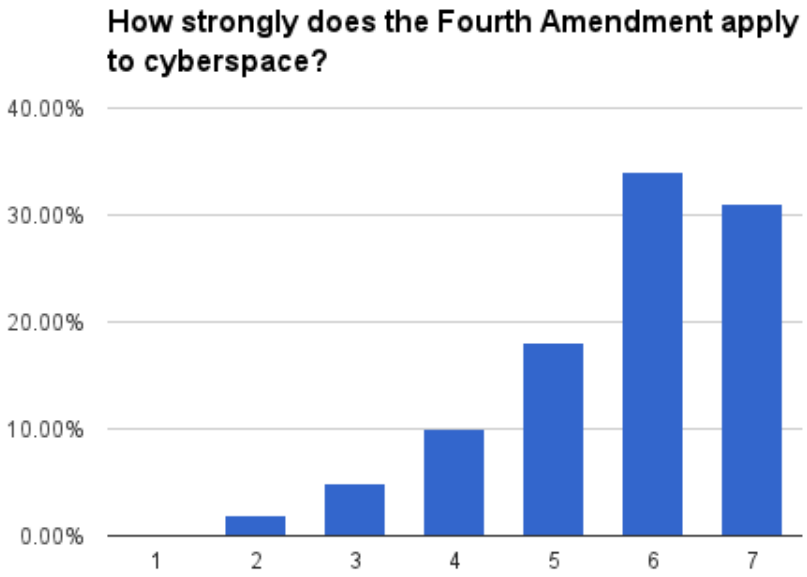

Figure 20 This graphs shows the spectrum of responses regarding how strongly people feel that the Fourth Amendment applies to cyberspace. On the x-axis, 1 represents not applying to cyberspace, and 7 represents very strongly applying to cyberspace.

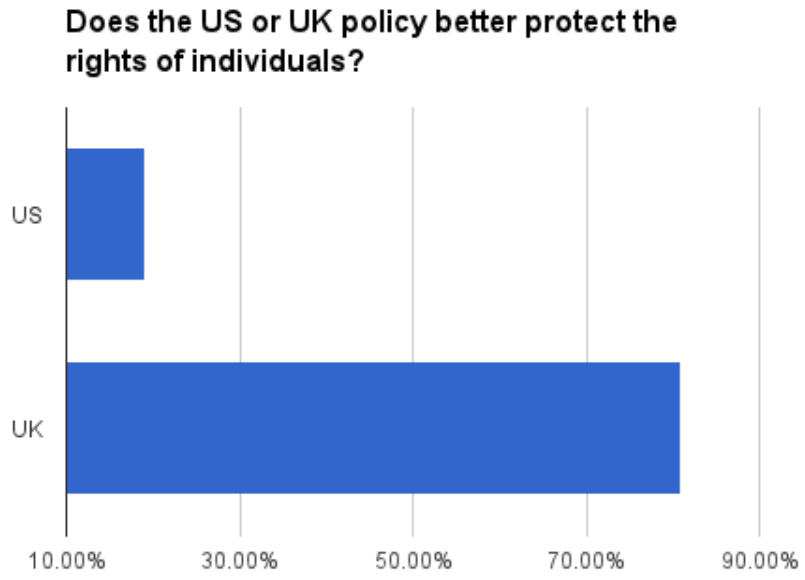

Figure 21 This graph displays the percentages of people who favor the US vs. UK data collection policy.