AUTONOMOUS IMAGING AND SPOTLIGHT SECURITY SYSTEM
BALANCING BETWEEN DATA PRIVACY AND THE NEED FOR VIDEO SECURITY

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Engineering

By
Kiki Wong
October 27, 2023

Technical Team Members:
Ethan Cha
Minsol Kim
Kousuke Tapia
Josh Yu

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS
Adam Barnes, Department of Electrical and Computer Engineering
Rider Foley, Department of Engineering and Society

INTRODUCTION

Security systems are essential for safeguarding people, property, and information from various threats. They deter and detect potential dangers such as theft, vandalism, or emergencies. In both residential and commercial settings, security systems play a crucial role in enhancing peace of mind, reducing risks, and maintaining a secure environment. The pandemic and the accompanying restrictions had a multifaceted impact on crime rates. During the initial outbreak of the COVID-19 pandemic, there was a concerning upswing in criminal activities, with a pronounced increase in both violent and property crimes (Grawert, 2022). The economic strains resulting from lockdowns and business closures, leading to financial instability for many individuals, and the emotional and psychological stress of the pandemic, coupled with isolation from lockdowns, may have contributed to both a rise in property crimes, driven by increased economic hardship, and an increase in violent crimes (World Health Organization, 2022). These complex factors highlight the interplay between social, economic, and public health factors, making it essential for governments and communities to consider holistic strategies to address these challenges during times of crisis.

As crimes become more complex, security systems need to continuously evolve and incorporate advanced technology and strategies to effectively detect, deter, and respond to these increasingly sophisticated threats. The need to protect sensitive data, critical infrastructure, and individual privacy has escalated in the digital and interconnected world (Alawida, 2022). Environmental threats, supply chain vulnerabilities, and strict regulatory requirements also underscore the significance of security measures in safeguarding both physical and digital assets. The driving force behind the project, Radiance, is the paramount goal of enhancing safety and security in various settings. This project will be a surveillance and intruder detection system that

uses thermal imaging to detect any life with a heat signature within a designated perimeter, automatically illuminating the entity and tracking its position as it moves. It also allows the user to directly interact with the target by toggling the spotlight that will automatically follow the target's movement. This project is an example of computer vision and autonomous robotics in security, a field that has expanded into the consumer market from military technology (Sage, 1999).

AUTONOMOUS IMAGING AND SPOTLIGHT SECURITY SYSTEM

The central component of this automated searchlight system, Radiance, is the Raspberry Pi that directly interfaced with the thermal camera and microcontroller. A Raspberry Pi is a small, affordable single-board computer that allows one to control electronic components for physical computing. And a microcontroller is a compact integrated circuit designed to govern a specific operation in an embedded system. The cameras are infrared (IR) which work by shining a short wavelength IR light over the entire field of view and detecting reflections off objects (Rogalski, 2002). The Raspberry Pi processes the real-time video feed from the camera and instantaneously transmits signals to the controller upon subject detection. These signals trigger the movement of motors through acquired drivers that regulate the electricity supplied to the motors, adjusting both speed and torque. Simultaneously, either the Raspberry Pi or the microcontroller initiates a signal to activate the light switch, which is hardwired to the flashlight, allowing power flow upon activation. This operation continues until no heat signature is detected. To power the system, a DC power supply will be acquired and integrated into a custom-designed power distribution PCB, which will furnish the requisite voltages to the Raspberry Pi, motors, and flashlight (Eaton 2023). Both the camera and microcontroller draw

power from the USB ports in the Raspberry Pi. If time permits, a backup power source will also be incorporated to address utility outages. This will involve equipping the system with a battery and the design of appropriate switching circuitry to enable automatic utilization of battery power when required. The system's performance is contingent on various external and internal factors, which impose limitations.

The image analysis algorithm for this system will be written in the Python programming language, with a primary focus on leveraging the capabilities of the OpenCV library. OpenCV, a versatile and powerful computer vision library, will enable the system to perform a wide range of image processing tasks crucial to our system's functionality. To facilitate seamless communication between the software and the MSP432 microcontroller, we will employ the pySerial library, ensuring efficient data exchange and control. The code that drives the motors and light on the MSP432 microcontroller will be written in embedded C, a low-level programming language, using Code Composer Studio, a reliable integrated development environment. Furthermore, our project involves the development of a custom-designed printed circuit board (PCB) to streamline and optimize the hardware aspects of our system. To accomplish this, we will rely on EasyEDA, a user-friendly PCB design tool, to create a tailored PCB layout and order the necessary components. EasyEDA's intuitive interface and powerful design features will enable us to bring our hardware vision to life while ensuring precision and reliability in the manufacturing process. This project encompasses both software and hardware, underscoring the technical depth and integration that our project embodies.

As for performance objectives, when monitoring a 5m x 5m x 5m area, the system is designed to illuminate and track a subject moving at a top speed of 2.8 m/s in any direction with a precision of ± 0.15 m in either direction under worst-case conditions, a speed classified as 'fast'

according to a study on human running speeds (Zhao, 2022). In the event of multiple subjects, the system prioritizes the first recognized subject but offers a user-friendly toggle functionality for switching focus. Moreover, users can access the thermal camera feed remotely with ease. Lastly, the system includes a feature to avoid activation during daylight conditions when used outdoors.

In the context of this project, usability considerations are paramount, emphasizing inclusivity for individuals of diverse ages and abilities. This involves the incorporation of multiple languages and visual aids in the user interface to ensure accessibility. The availability of necessary components, including electrical parts, circuit boards, cameras, and power systems, is currently confirmed. Economic considerations revolve around a $500 budget, with the thermal camera constituting a notable expense. To address environmental concerns, the system is engineered with sustainability in mind, featuring low-power and repairable components. Safety measures involve regular system checks and the capacity to distinguish potential threats. Ethical considerations pertain to continuous system operation and suggest the use of user-generated signage to inform passersby of surveillance within specific areas, thereby fostering transparency and consent. These multifaceted considerations ensure that our system aligns with various constraints and stakeholder requirements.

BALANCING BETWEEN DATA PRIVACY AND THE NEED FOR VIDEO SECURITY

Bijker's article, *Constructing Worlds: Reflections on Science, Technology, and Democracy (and a Plea for Bold Modesty),* introduces the Social Construction of Technology (SCOT) framework as a valuable lens through which to scrutinize the development and impact of your automatic spotlight security system. Within the SCOT framework, various facets come into

play, with data privacy emerging as a prominent concern. Firstly, the SCOT framework underscores the pivotal role of different social groups or stakeholders in shaping technology. In this project, stakeholders, including homeowners, apartment complexes, businesses, and law enforcement, each possess unique interests and needs concerning security (Bijker, 2017). These diverse groups profoundly influence the design and features of the automated spotlight system, with a particular focus on data privacy. Secondly, the SCOT framework highlights the importance of interpretative flexibility. In the context of my project, this aspect is evident as the system employs image detection with a thermal camera to identify potential security threats. Divergent interpretations of what constitutes a threat among various user groups directly impact data privacy concerns. For example, homeowners and a prison facility might hold differing criteria for defining a threat. Such variations could lead to adjustments in the system's algorithms and alert mechanisms, thereby raising substantial questions about data privacy and consent.

The integration of Ethnography of Infrastructure principles into the development of a new alarm video security system presents a holistic approach to system design. This approach entails a meticulous examination of how users interact with existing security systems, the identification of their challenges, and a deep understanding of the cultural and organizational contexts within which these systems operate (Star, 1999). By closely observing user behaviors and challenges, the new system can be tailor-made to enhance user-friendliness, adapt seamlessly to diverse environments, and operate with ease, requiring minimal training. Ethnographic research is also likely to unearth unexpected uses and innovative applications of such systems, fostering a more versatile, user-centered design. Furthermore, it accentuates the significance of feedback mechanisms for continuous improvement and the incorporation of features allowing users to report issues or provide input.

The Privacy Act of 1974, HIPAA, and the Gramm-Leach-Bliley Act, alongside an array of state-level data privacy laws, collectively play a significant role in the realm of video security systems. These regulations collectively address the protection and handling of personal data, a category often captured and processed by video security systems. The Privacy Act of 1974 dictates how federal agencies handle individual data, placing a premium on the need for consent and privacy protection. The United States does not appear to have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FERPA, ECPA, CCPA, and VPPA (Klosowski, 2021). HIPAA primarily focuses on the privacy of personal health data, which becomes relevant when video surveillance encompasses healthcare settings (Murray, 2023). State-level data privacy laws, exemplified by the CCPA in California, add an additional layer of protection and rights for individuals regarding their data. It's incumbent upon video security systems to adhere to these regulations to ensure compliance while diligently safeguarding the privacy of individuals captured by these systems.

The data that will be recorded from our project comprises of sensitive details like facial features, license plates, and biometric information (Intozi, 2023). While video security systems are essential for safeguarding individuals, properties, and public spaces and providing critical evidence for investigations, ethical and legal concerns surrounding data privacy, especially with AI video analytics, cannot be ignored. The potential misuse of such data, from identity theft to harassment, necessitates a comprehensive framework of laws, regulations, and best practices to govern data collection, storage, and dissemination. Unfortunately, obtaining consent for audio recordings necessitates written authorization. It's often mistakenly believed that displaying window decals or yard signs is adequate for obtaining consent, assuming that visitors will notice and understand them (“The Legal and Ethical Considerations of Video Surveillance in the

Workplace", 2016). However, in a residential setting, the acceptability of home camera usage ultimately depends on the person's intentions and actions concerning the recordings.

The implementation of automated security systems like this project raises substantial concerns, necessitating a thorough review of existing data privacy laws and the development of new policies to address the ethical and legal implications tied to this technology. In this era of expanding digital surveillance and data collection, it becomes imperative to strike a harmonious balance between security and the safeguarding of individuals' personal information. The evolving landscape of data privacy regulations and ethical considerations will play a central role in shaping the development and deployment of your security system.

RESEARCH QUESTION AND METHODS

In contemplating the constant surveillance of areas beyond personal property and its intersection with the possible misuse of data acquired through AI video analytics, a critical query arises: Could the integrity of data privacy be compromised in the context of video security systems? The intricate nature of data privacy becomes particularly challenging when recording on private property inadvertently capturing others in the footage. Questions regarding the safety and permissibility of retaining such recordings emerge. Can legal consequences arise from these scenarios? Guiding inquiries will serve as the foundation for my research question, acknowledging the absence of a straightforward answer.

To address this research question, an extensive review of data privacy and cybersecurity laws, including the Privacy Act of 1974, HIPAA, and the Gramm-Leach-Bliley Act, will be conducted. This legal analysis aims to uncover the regulatory landscape governing data

collection, especially when private property intersects with public spaces. Simultaneously, an examination of relevant legal cases and rulings will be undertaken to glean insights into the intricacies of data privacy in the context of constant surveillance through AI video analytics. This exploration of legal precedents seeks to illuminate the ramifications and potential complexities associated with the use of video security systems.

In addition to the legal analysis, qualitative research methods will be employed to capture perspectives from individuals inadvertently recorded on private property. This may involve conducting interviews or surveys to understand public perceptions, concerns, and expectations regarding the privacy implications of unintentional surveillance. Additionally, I will compare practices and policies in various places to uncover differences in how laws handle the balance between data privacy and the use of video security systems. This global viewpoint aims to help us better grasp the issues and possible answers where technology and privacy meet. By combining legal study, personal perspectives, and a look at different approaches, this research method aims to thoroughly explore how data privacy might be at risk in video security systems.

CONCLUSION

This project encompasses the development of an advanced automatic spotlight security system that addresses the evolving landscape of safety and security needs. It is designed to enhance user-friendliness, adaptability, and effectiveness while considering data privacy and ethical concerns. The project acknowledges the multifaceted challenges posed by modern threats, emphasizing the importance of security systems in safeguarding both physical and digital assets, individuals, and critical infrastructure. Additionally, the project underscores the Social Construction of Technology (SCOT) framework's relevance, particularly concerning data privacy

and the influence of diverse stakeholder groups. It also recognizes the significance of existing data privacy laws and ethnographic insights in the project's development. As we move forward, it is essential to continuously adapt security systems to meet the dynamic and complex challenges of our times while upholding the principles of privacy and ethical operation.

References

Batiz-Lazo, B., & Maixe-Altes, J. A. (2002). Engineering, Social and Regulatory Issues in the Development of the EMV Smartcard Standards. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S1350449502001408

Bijker, W. (2017). Constructing worlds: Reflections on science, technology and democracy (and a plea for bold modesty). Engaging Science, Technology, and Society, 3, 315. doi:10.17351/ests2017.170

Brennan Center for Justice. (2023). Myths and Realities: Understanding Recent Trends in Violent Crime. https://www.brennancenter.org/our-work/research-reports/myths-and-realities-understanding-recent-trends-violent-crime

Eaton. (2023). USB charging and power delivery. Retrieved from https://tripplite.eaton.com/products/usb-charging

Ethics & Laws Of Home Surveillance. (2016). Retrieved from http://blog.securitycamexpert.com/2016/10/ethics-and-laws-of-home-surveillance/

Forbes. (2023). U.S. Data Privacy Protection Laws: A Comprehensive Guide. https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/?sh=79258e375f92

Hughes, Thomas P. 1987. The evolution of large technological systems. In The social construction of technological systems. New directions in the sociology and history of technology, edited by W. E. Bijker, T. P. Hughes and T. Pinch. Cambridge, Massachusetts & London, England: MIT Press, 51-82

Klosowski, T. (2021). What to Know About Data Privacy Laws in the US. LinkedIn. https://www.linkedin.com/pulse/privacy-data-protection-concerns-utilizing-ai-video-analytics/

The Legal and Ethical Considerations of Video Surveillance in the Workplace. (2023). Retrieved from https://pipl.systems/the-legal-and-ethical-considerations-of-video-surveillance-in-the-workplace/#:~:text=Legal%20Considerations&text=Depending%20on%20the%20jurisdiction%2C%20there,the%20use%20of%20hidden%20cameras.

National Center for Biotechnology Information. (2021). Research on Energy Cost of Human Body Exercise at Different Running Speed. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9367180/

An Overview of Video Analytics in Security. (2022). Retrieved from https://www.ifsecglobal.com/video-surveillance/overview-video-analytics-security/

Raspberry Pi 3 Model B. (2023). Retrieved from https://datasheets.raspberrypi.com/rpi3/raspberry-pi-3-b-plus-product-brief.pdf

Sage, K., & Young, S. (1999). Security applications of computer vision. IEEE Aerospace and Electronic Systems Magazine, 14(4), 19-29.

Security Industry Association. (2020). Data Privacy Code of Practice for Video Surveillance. https://www.securityindustry.org/report/data-privacy-code-of-practice-video-surveillance/#:~:text=Implement%20appropriate%20processes%2C%20policies%20and,encryption%20during%20transmission%20and%20storage

STAR, S. L. (1999). The Ethnography of Infrastructure. American Behavioral Scientist, 43(3), 377-391. https://doi.org/10.1177/00027649921955326

StudyCorgi. (2022). Ethical Issues in CCTV and Biometrics Technologies. Retrieved from https://studycorgi.com/ethical-issues-in-cctv-and-biometrics-technologies/

Touhy, J. (2023). Why Get a Home Security System? U.S. News. Retrieved from https://www.usnews.com/360-reviews/services/home-security/why-get-a-home-security-system

The World Health Organization. (2022). The Impact of COVID-19 on Mental Health Cannot Be Made Light Of. https://www.who.int/news-room/feature-stories/detail/the-impact-of-covid-19-on-mental-health-cannot-be-made-light-of#:~:text=A%20great%20number%20of%20people,affected%20much%20more%20than%20others

Wieczorek, A. (2019). Constructing Worlds: Reflections on Science, Technology, and Democracy (and a Plea for Bold Modesty). STS Infrastructures. https://stsinfrastructures.org/content/constructing-worlds-reflections-science-technology-and-democracy-and-plea-bold-modesty-1

Zhang, J. (2020). Understanding People's Privacy Attitudes Towards Video Analytics Technologies. https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-zhang.pdf