Advancing the Design of Non-Contact Vital Sign Measurement Technology

Government Use of Technology in Surveillance

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 Biomedical Engineering

By
Matthew T. Beyer

October 27, 2022

Technical Team Members:

Alec Figler, Hugh Thorner

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

Dr. Kent Wayland, Department of Engineering and Society

Dr. Timothy Allen, Department of Biomedical Engineering

General Research Problem: Advancing measurement technology to be affordable and mass-producible

How can surveillance technology be developed and implemented without overstepping ethical bounds?

Surveillance technology "has spilled out of its old nation-state containers to become a feature of everyday life, at work, at home, at play and on the move" (Lyon, 2003). Rather than serving political espionage purposes, surveillance technology has boomed into everyday life—baby monitors help parents provide tender care to their children, home security systems allow families to live in peace, and Apple Watches detect irregular heart rhythms before doctors get the chance. With the rise of internet and expanding technology, surveillance has sprung into the present before much legislative action could be passed to regulate how these new technologies are used. While the non-contact vital sign measurement technology that is being developed for my technical research problem is intended for medical or military use, the technology has the potential to be used for law enforcement purposes by cheaply and effectively picking up signs of life inside a building without anyone knowing. This could be used by law enforcement to surveil buildings when searching for a suspect, delivering a warrant, or even just to look for suspicious activity—a searching technology that has not yet been regulated by legislative acts. The Fourth Amendment to the United States Constitution states that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." Interpretations of "unreasonable searches" have varied since the inception of the United States, and emergent technology coupled with globalized threats of terrorism have resulted in passage of the "Patriot Act," which has given governmental agencies such as the NSA permission to comb through Americans' online data and communications in the interest of societal safety in specific cases, although whistleblowers allege that this technology is being used in situations that are outside the scope of permissions granted by the act. For this reason, the American public is skeptical of surveillance technology as a whole. Given recent growing distrust in law enforcement and the federal government to behave with the best interests of the American people at their hearts, the introduction of such technology and growing permission to monitor civilians raises the question: how far can governmental powers ethically extend their use of technology for surveillance and law enforcement purposes?

Technical Research Problem: Advancing the Design of Non-Contact Vital Sign Measurement Technology

How can non-contact vital sign measurement technology be altered to allow cheap, customizable production?

Human heart rate and respiration rate are biomarkers that provide physicians insight on patient health status. These biomarkers are called “vital signs,” as the absence of a heart rate or respiration indicates catastrophic organ failure. Since the mid-1980s, the United States Air Force has been using prototypes of non-contact vital sign measuring doppler radar devices to measure vital signs of fallen soldiers from up to 100 meters away (Matthews, 2000). While non-contact vital sign measurement (NCVSM) has been developed for military use, a plethora of potential non-military commercial users do not have NCVSM available to them. Trauma center patients such as burn victims for whom electrodes would be infeasible could greatly benefit from a cheap, commercially available NCVSM system. Radio-frequency directional horn antennas in the millimeter wave band (~60GHz) can be used for NCVSM using signals beamed to and reflected from a human subject at a distance of a few meters (Owen, 2022). These horn antennas are subject to interference, which may compromise signal to noise ratio and the ability to accurately determine heart rate or respiration rate, but can detect the presence of a heartbeat or respiration regardless–critical to emergency response and medical care in “life or death” situations. While frustum shaped horn antennas are currently available on the market, they tend to cost between $1500 and $2000 per copper horn. Currently, our advisor has developed a 2D PCB Flex Circuit which folds, like origami, into a 3D frustum horn. This PCB circuit, layered with copper, only costs $500 to produce– 33% of the cost of the cheapest existing horns on the market. The goal of our project is to advance the “origami” horn prototype to a stage where it is market-ready.

The current horn antenna prototype consists of several overlapping layers of PCB and copper, folded into a frustum and soldered together, fixed at the narrow end to a millimeter-wave transmitter/receiver device and circuit board. While this device can effectively record heart rate and respiration rate on a stationary target placed at its focal depth, more development is necessary to make this prototype effective in the field and as a commercial product. First, our group intends to parametrize an existing program that feeds dimensions for 2D horn printing into kiCAD software. This parameterization will use geometric formulas for beam pattern to feed kiCAD optimal dimensions to print the 2D PCB and copper sheet so that it folds into a frustum which conducts a beam to a requested input focal depth. Next, our group needs to physically design and assemble a testing apparatus. This will be used to determine how accurate horns of each focal depth are at measuring vital signs from a range of distances. This will allow the commercialized product to guarantee a degree of accuracy within a specific range of distances. Finally, our group will use AutoCAD to design multiple physical scaffolding components for the device. First, we will develop a clamp which can fix the small end of the horn to the circuit board after the horn is soldered into a frustum shape. Next, we will design scaffolding to protect the circuit board and keep the device sleek, portable, and durable. Once these objectives are met, the new device should be market-ready for commercialization, allowing it to improve the quality of life of medical users and military personnel.

STS Research Problem: Government Use of Technology in Surveillance

How far can governmental powers ethically extend their use of facial recognition technology for surveillance and law enforcement purposes?

Globalization and advances in technology have led to amazing socioeconomic phenomena, but have also allowed for radicalization, terrorism, and the ability to steal from millions at the press of a button. As a result, law enforcement agencies across the globe have been scrambling to modernize and develop cutting-edge technology. Unfortunately, as technologies arise, they are often put to use before their implications are fully understood and before legislation is enacted to regulate their ethical use. The purpose of my research is to analyze the actants and social groups involved in this progress and provide insight into their positions on how artificial intelligence, specifically facial recognition, can be regulated for ethical use by the government to efficiently enforce rule of law and ensure that said technologies are not used to oppress, endanger, or infringe upon the rights of civilians, but rather protect them.

Newly available technologies are being used by governments worldwide to help law enforcement carry out their jobs efficiently. A 2022 study by Priyosantoso et al. found that in Indonesia, the main challenges for law enforcement are “lack of resources, changes in the scope of law enforcement, and information that is not integrated” (Priyosantoso, 2022). Due to Indonesia’s archipelago geography, high population, and cultural diversity, local and regional law enforcement agencies have struggled to streamline information on criminals and missing people, especially between regions that are well developed and regions that are underdeveloped. With crime on the rise, the Indonesian government has adopted a new database system to distribute criminal records uniformly and help law enforcement agencies do their jobs. This database system has successfully aided them in upholding the rule of law.

In the United States, law enforcement have adopted technologies aimed at protecting the lives of those who are in the line of duty. A 2020 conference on wearable sensor technology found that officers who were given sensors would be able to have their vital signs checked from a central headquarters, leading to safer encounters and quicker backup dispatch if an officer was in danger (Goodison, 2020). However, during this conference, police leaders voiced their concern for the applicability of the technology, as long-time officers prefer to maintain the protocols they were trained with and have been using for years. In both of the above cases, the national government has implemented technological changes in an effort to preserve rule of law and safety for individual officers, however officers are sometimes reluctant to accept these changes. These indicate that national governments choose to implement technologies that support their goals and hope that their employees can adapt to these changes. However, in other scenarios, the government implements technologies of concern to the public. The public—from whom the government's power is derived—are expected to adapt to these technologies, yet are sometimes concerned with the implied power which these technologies give the government. A critical issue wherein the public is wary of technology's potential usage by the government is facial recognition: a subcategory of artificial intelligence.

Artificial intelligence (AI) "deals with all aspects of mimicking cognitive functions for real-world problem solving and building systems that learn and think like people" (Holzinger, 2019). This is often personified by the development of computer programs which can learn to classify and identify things based on provided datasets and discover correlations that humans otherwise would not draw. In a 2019 paper, Dick pointed out that "attempts to produce intelligent behavior in machines often run parallel to attempts to make human behavior more machine-like" (Dick, 2019). While artificial intelligence can be used for good, it can and has resulted in humans being profiled and minimized to data points, opening the door to oppression and misclassification, as context and social phenomena are often neglected in analysis of "machine-like" human behavior. Artificial intelligence has expanded into the realm of facial recognition technology: programs which "(create) a 'template' of (a) target's facial image and compare the template to photographs of preexisting images" from a database with the goal of determining the target's identity (Andrejevic, 2020).

This facial recognition technology can be used for all kinds of purposes, ranging from employers tracking who is at work to advertisers targeting ads and governments using facial recognition to identify threats. A Pew Research Center study found that while more than half of US adults trust law enforcement to use facial recognition responsibly, whereas a far smaller percentage of adults trust technology companies or advertisers to use the same technology responsibly (Smith, 2019). While a slight majority of American adults seem to trust the government using facial recognition, it seems that this may be in error, as a 2020 study by Lynch argued that facial recognition technology poses significant risks to civil liberties, including by disproportionately affecting people of color (Lynch, 2020). This disparity has resulted in minority groups having special interest in the means of development and regulation of facial recognition. When the public sees that the power they vested in the government to protect them may be used to harm them, it becomes their responsibility to elect or lobby leaders that will enact legislation that regulates such power. While we do not yet have substantial federal regulation of facial recognition technology in the United States, other areas of the world are considering regulation and being lobbied with suggestions from several groups.

A 2022 convention highlighted several positive uses of facial recognition before making policy demands for its regulation. This discussion revealed that certain human rights groups, such as the European Convention of Human Rights, Fair Trials, and 114 civil society organizations urge caution in the development of facial recognition and urge for legislation in the EU to regulate facial recognition in an effort to ensure that it is trustworthy and adheres to the ethical principles of "respect for human autonomy, prevention of harm, fairness, and explicability" (Roksandić, 2022). These demands form several policy suggestions that could be used to regulate AI and facial recognition in an effort to continue progress within ethical bounds, not just in the EU, but as a template for regulation in the United States.

I plan to gather more ethical papers and statistics on the impacts of facial recognition technology on minority groups to truly understand the risks of facial recognition technologies. I also plan to find more information on state-level regulation of facial recognition, as well as any academic perspectives on the tangible increase in safety that facial recognition has provided the general public against terrorism and other crime. I intend to use the Social Construction of Technology framework to analyze how the federal government, marginalized groups within the public, and the overall United States public can interact to form a legislative plan that aims to prioritize the societal values of safety, human autonomy, racial equality, rule of law, and anti-authoritarianism in the presence of facial recognition technology.

Conclusion

From my STS research, I hope to provide context toward what the relevant social groups of the United States Government, the minority population of the United States, and individual legislators feel and choose to do regarding regulation of facial recognition technology. From my technical research, I hope to bring a non-contact vital sign measurement device to the stage at which it can be produced and sold on a large scale to aid with enforcement of law, military procedures, disaster relief, and medical treatment. Overall, I hope to use the sociotechnical context of surveillance to ethically evaluate the potential uses of my technical project, allowing me to behave as a conscientious engineer who is mindful of the sociotechnical impact that unintended, unethical uses of my device may cause.

References

Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*, *45*(2), 115-128.

Dick, S. (2019). Artificial Intelligence. *Harvard Data Science Review*, *1*(1). https://doi.org/10.1162/99608f92.92fe150c

Goodison, S. E., Barnum, J. D., Vermeer, M. J., Woods, D., Sitar, S. I., Shelton, S. R., & Jackson, B. A. (2020). *Wearable Sensor Technology and Potential Uses Within Law Enforcement: Identifying High-Priority Needs to Improve Officer Safety, Health, and Wellness Using Wearable Sensor Technology*. RAND.

Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(4), e1312.

Lynch, J. (2020). Face Off: Law Enforcement Use of Face Recognition Technology. *Electronic Frontier Foundation. Available at SSRN 3909038.*

Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Psychology Press.

Matthews G, Sudduth B, Burrow M. (2000). A non-contact vital signs monitor. Crit Rev Biomed Eng. 2000;28(1-2):173-8. doi: 10.1615/critrevbiomedeng.v28.i12.290. PMID: 10999382.

Owen, Kevin. (2022). Origami Horn Antenna Capstone Project Description. *University of Virginia School of Engineering and Applied Sciences*. Rivanna Medical.

Priyosantoso, R., Aminanto, M. E., & Fadilah, F. (2022). Citizen Data Integration as the Backbone of Law Enforcement Implementation in Indonesia. *International Journal of Multicultural and Multireligious Understanding*, *9*(1), 695-703.

Roksandić, S., Protrka, N., & Engelhart, M. (2022, May). Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?. In *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1225-1232). IEEE.

Smith, A. (2019). More than half of US adults trust law enforcement to use facial recognition responsibly. *Pew Research Center*, *5*.