STS 4500 Thesis Prospectus

Leo Bashaw

5 November 2023

Introduction

Data acquisition, analysis, and transmission compose a central part of our everyday lives. From making a phone call to putting a rover on Mars, fantastically complex applications of big data are happening in real-time everyday. In my mechanical engineering capstone class (Spacecraft Design), myself and a team of 30 other students are designing a high powered rocket that will carry a payload of ~10 pounds to an altitude of ~5000 feet. Within our class, I am the lead engineer for our four person data acquisition and transmission (DAQT) subteam. Our principal goal is to design a reliable, secure, and accurate DAQT system for use during every stage of the rocket's flight (ascent, parachute deployment, descent, etc). Failure to meet this goal could result in a number of things: a 50 pound rocket falling over a populated area from 5000 feet with no parachute, the waste of countless man hours and thousands of dollars invested in the rocket, or, in a more hypothetical situation, a foreign adversary being able to interfere with our mission and hack our rocket's digital systems (assuming our goal of security is not met).

The complex nature of my capstone project pushed me to think about the applications of DAQT to my everyday life, and naturally I began to ponder the topics of social media, marketing, and targeted content-delivery. Within this global socio-technical system of DAQT, the abuse of privacy by both government and corporate institutions is generally public knowledge. For example, Edward Snowden is arguably a household name and Facebook/Meta's privacy lawsuit recently ended in a near $750 million settlement (NPR). As both a provider and consumer of big data through my life as an American and my work as an engineer, I realize that I straddle opposing sides of the heated discussion over digital privacy; this led me to choose digital privacy as my STS research topic. My STS research will focus on the integrity of privacy during the everyday acquisition, transmission, and analysis of our personal data. More specifically, I will argue that it is unwise to leave your privacy in the hands of the agencies that handle your data. I will then attempt to evaluate the types and efficacy of the extra precautions that non-institutional actors can take to safeguard their privacy.

Overall, both my technical and STS research projects are centered around handling and processing data safely and efficiently to produce meaningful results from which greater insights can be gleaned. In the case of my capstone project, we are attempting to gather and analyze data to determine when we have reached 5000 feet, deploy our parachute, and ensure that the rocket returns to ground safely. From the results of our project, we will propose plans for improvement that future classes of UVA students can act on. In the case of my STS research, I will gather information about the current state of personal digital privacy in America to determine why one should take extra security measures to protect their data, and how they can do so. The "greater insights" in this case will be conclusions about whether or not it is even possible to adequately protect your data, or if to participate in the modern digital world (as it currently exists) one must forgo a certain degree of privacy.

Technical Topic

In my capstone class, Spacecraft Design II, myself and a team of 30 other students are working to build a high powered rocket that will bring a 10 pound payload to a height of 5000 feet. Our rocket will be about six inches in diameter, roughly six feet tall, and will weigh about 50 pounds. The payload, where the bulk of my engineering efforts are focused, consists of two separate parts. The first is a telemetry module that incorporates all of our sensors, flight computers, and radio transmitters (this will stay attached to the main body of the rocket for the whole flight). The second and experimental part of the payload is a deployable glider that has an onboard camera and a few sensors. Once our telemetry module senses that the rocket has reached its maximum altitude, the rocket will separate into three pieces with the help of explosive charges. Then, the parachutes will deploy and the glider will be ejected from the body of the rocket to begin its own descent.

There are a number of different types of sensors that will be incorporated in our telemetry module to ensure that we can accurately detect when an altitude of 5000 feet is reached. First, we use temperature and atmospheric pressure sensors, since these quantities both decrease as the rocket gains altitude. The way that temperature and pressure vary with altitude is well understood, so these quantities provide a reliable means of determining altitude. Second, we will have multiple accelerometers which are used primarily to detect abrupt changes in speed and direction (this is one of the ways that cars determine whether or not to deploy airbags). When the rocket reaches its maximum height, its velocity will change from positive (moving upward) to negative (moving downward). Our accelerometers can detect that change, and when combined with the temperature and pressure sensors, we should be able to accurately predict when we've reached 5000 feet and/or our maximum altitude (it is not guaranteed that our maximum altitude is exactly 5000 feet). More temperature sensors will be used in certain "hotspots" within the rocket (such as near the engine or large groups of electronics) to monitor the health of the rocket during flight. Strain gauges, electronic sensors that detect deformations in materials, will be used on critical frame components to provide a secondary way of monitoring the health of the rocket during flight. Finally, an off-the-shelf GPS unit, similar to a Garmin that you would use for hiking or boating, will be included in the rocket to aid in tracking and locating it after it has reached the ground.

All of this data is useful to the team for post-flight analysis, but it becomes exponentially more useful when it can be transmitted back to the ground and monitored in real time. For this task, we use radio transmitters to send the data to a receiver operated by the team on the ground. In case the radio is unreliable or damaged during flight, we will also gather the data and store it on an SD card that can be retrieved from the rocket once it reaches the ground.

This capstone project is useful for a number of reasons. For one, it provides our young team of engineers with practical, applied experience in solving complex problems that one cannot gain from problem sets or attending lectures. The project will help prepare students to enter the workforce, where they will need to adapt to changing project budgets, requirements, team structures, and deadlines. Moreover, this year is the genesis of the rocketry capstone class, so the students involved gain invaluable experience in building and organizing large-scale engineering teams from the ground up. Finally, this capstone sets the stage for future UVA capstone students to improve on our designs, project management methods, and augment our deployable glider into something more robust.

STS Topic

To restate, my work will focus on the current lack of personal privacy protection during the everyday process of personal data acquisition, transmission, and analysis. Following the position that modern digital privacy is in a poor state, I will conduct an analysis of the countermeasures that individuals can use to protect their data and the effectiveness of said countermeasures. Ultimately, I will draw some conclusions about whether or not it is currently possible to adequately guarantee digital privacy, and if not, why a certain amount of freedom must be given up to participate in the modern digital world.

A general consensus among scholars today is that digital privacy is not guaranteed. For example, even in 2012 researchers at leading universities such as Georgetown and the University of Sydney argued that there “are serious issues involved in the ethics of online data collection and analysis…[and that] the research ethics cannot be ignored simply because the data are seemingly public" (Boyd, Crawford). Moreover, a 2023 study of over thousands of online privacy policies from 1996-2021, conducted by Swiss and English scholars, found "several concerning trends, including the increasing use of location data, increasing use of implicitly collected data, lack of meaningful choice, lack of effective notification of privacy policy changes, increasing data sharing with unnamed third parties, and lack of specific information about security and privacy measures" (Wagner). With several high profile privacy scandals occurring in recent decades (think Edward Snowden, Mark Zuckerberg, just to name a couple), it is alarming that the current state of digital privacy is still viewed as generally compromised.

To build off of this, many Americans today are ill-equipped to make informed decisions about digital privacy. A joint focus group study conducted by researchers at the University of North Carolina and the University of Zurich found that "participants viewed privacy violations as inevitable and social media use as necessary," and that "virtually no-one grasped the extent of data-mining" (Marwick, Hargittai). These researchers reference other studies with highly similar findings, and one would not need a source to postulate that a vast majority of Americans do not completely understand the electrical, algorithmic, and institutional nature of the systems that handle their data. Not only should we understand how we can protect our own privacy, we should also understand how we can protect our dependents' privacy. For example, many young children use and are even famous on social media, which shows a ripe opportunity for ethically ambiguous data collection. It is known that children are easily impressionable and generally less capable of rational decision making than adults, making them easy targets for data collection and marketing. As proof that this type of abuse already occurs, know that in 2022, the Irish Data Protection Commission "fined Instagram a record 405 million euros… for alleged mishandling of teens' data" (Li). With such a gap in between the public's knowledge of and protection by privacy standards, my research aims to plug the holes of modern privacy ignorance and abuse by answering the questions of "what needs to be done, why, and how do we take things into our own hands?" I will research grass-roots, individual, and communal methods of ensuring privacy in digital ecosystems, but the work does not end there. I believe that reducing our dependence on these digital ecosystems is also entirely possible. For example, instead of keeping up with friends via social media apps, simply texting peers in group chats already offers a more private way to share information about your personal life.

Conclusion

In conclusion, my research is centered on the critical issue of digital privacy, examining the everyday acquisition, transmission, and analysis of personal data and its profound implications for society. The relentless march of technology and the exponential growth of data-driven systems have placed our privacy at an unprecedented crossroads, where the choices we make today will shape the future of our society. In the course of my future research paper, I aim to unravel the complexities of this topic and present a comprehensive analysis. I anticipate shedding light on the vulnerabilities inherent in entrusting our data to institutions and corporations, offering a critical perspective on the risks they pose to our privacy. Additionally, I will explore the various extra precautions individuals can take to safeguard their personal data and assess their efficacy.

Ultimately, the expected results of my research will contribute to a better understanding of the state of personal digital privacy in contemporary America, highlighting the need for vigilance in protecting our data. My research will also provide valuable insights into the feasibility of maintaining one's privacy in the modern world. It is my hope that this study will empower individuals to make informed decisions about their data, promote discussions about digital privacy's broader societal implications, and encourage the adoption of practices that safeguard our privacy in an era of ever-expanding data acquisition and analysis.

References

1. Bishop, L. (2012). Using archived qualitative data for teaching: Practical and ethical considerations. *International Journal of Social Research Methodology*, *15*(4), 341–350. https://doi.org/10.1080/13645579.2012.688335
2. Boyd, D., & Crawford, K. (2012). CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, *15*(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878
3. Li, L. (2022, September 6). Ireland fines Instagram $400 million over handling of teens' data. *Washington Post*. https://www.washingtonpost.com/business/2022/09/06/ireland-instagram-fine-dpc-meta/
4. Li, S., Zhao, S., Gope, P., & Da Xu, L. (2023). Data Privacy Enhancing in the IoT User/Device Behavior Analytics. *ACM Transactions on Sensor Networks*, 32 (13 pp.). https://doi.org/10.1145/3534648
5. Mann, M., Wilson, M., & Warren, I. (2022). Smart Parenting? The Internet of Things, Children's Privacy, and Data Justice. *International Journal of Children's Rights*, *30*(1), 204–231. https://doi.org/10.1163/15718182-30010008
6. Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432
7. Prasanthi, K. N., Sekhara Rao Mvp, C., & Pallapothu, S. B. (2023). Boosted Hybrid Privacy Preserving Data Mining (BHPPDM) Technique to Increase Privacy and

Accuracy. *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2-4 Feb. 2023*, 378–384. https://doi.org/10.1109/ICAIS56108.2023.10073804

8. Silva, P., Amorim, V. J. P., Ribeiro, F. N., & Muzetti, I. (2015). PrivacyMod: Controlling and monitoring abuse of privacy-related data by android applications. *2015 Brazilian Symposium on Computing Systems Engineering (SBESC), 3-6 Nov. 2015*, 42–47. https://doi.org/10.1109/SBESC.2015.15
9. Wagner, I. (2023). Privacy Policies across the Ages: Content of Privacy Policies 1996-2021. *ACM Transactions on Privacy & Security*, *26*(3), 1–32. https://doi.org/10.1145/3590152
10. Witteborn, S. (2021). Data Privacy and Displacement: A Cultural Approach. *Journal of Refugee Studies*, *34*(2), 2291–2307. https://doi.org/10.1093/jrs/feaa004
11. Yong Jin Park, Jae Eun Chung, & Dong Hee Shin. (2018). The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. *American Behavioral Scientist*, *62*(10), 1319–1337. https://doi.org/10.1177/0002764218787863