Undergraduate Thesis Prospectus

How a Required Cyber Security Course Prepares CS Students for the Future

(technical research project in Computer Science)

Balancing the Scale: Finding Common Ground on Internet Privacy

(sociotechnical research project)

by

Aaron Alem

October 27, 2023

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.

Aaron Alem

STS advisor: Peter Norton, Department of Engineering and Society

General research problem

How can we find the optimal blend between digital privacy and digital utility?

Digital data has become an integral part for businesses in many industries. Whether it comes to marketing, transportation, or health, digital data has become a part of our day to day life. With this increase in data collected also comes a privacy risk. In 2023 alone there were 4.5 billion compromised records worldwide (Ford 2023) and millions of dollars paid out due to privacy violations. With the growth in digital data collection, digital privacy also needs to be taken into consideration.

Preparing CS Students for the Future

How can a required Cyber Security course better prepare undergraduate CS students for the demands they will face, regardless of their specific field?

The project department is Computer Science, and the project will likely be the CS 4991 proposal option. This project will likely be about enhancing the value of the uva CS program.

Balancing the Scale: Finding Common Ground on Internet Privacy

In the US, how do e-commerce enterprises, data collectors, and privacy advocacies compete to draw the line between permissible and impermissible collection of personal data online?

About 62 percent of US adults accept daily data collection as a fact of life; 81 say they have no control over data collection (Auxier 2019). With user data, companies can offer free services and improve their products and services, however consumers do not alway feel these benefits are worth it. When user data is directly used to make these improvements, consumers believe that they are getting a fair trade. For example, when Netflix collects data to recommend shows or when Apple records user location to automatically keep track of where they parked

their car, consumers feel that they are getting value for the loss of their privacy. When it comes to data used for target marketing, consumers believe they should be getting more value out of the data being collected (Morey 2015). The concerns have been noticed with multiple states having implemented laws that try to increase online privacy by allowing consumers to opt out of sales of their data and target advertising. However, with 81% of Americans believing that the potential risks of collecting data on them outweigh the benefits (Auxier 2019), there's still a big disconnect between companies and consumers on digital privacy. How can we work towards bridging the gap?

Scholarly Exploration

Hallam and Zanella (2016) observed that despite expressing concerns for privacy, people constantly share sensitive information online using social networking sites. This creates something they call a "privacy paradox". From researching this "privacy paradox" they found that when using social networking sites, the viewed privacy risks are seen as abstract while social rewards are seen as concrete. Construction level theory tells us that abstract ideas are associated with distant-future outcomes and concrete ideas are associated with near-future outcomes. Since distant-future outcomes tend to be discounted for near-future ones, online privacy is discounted for social rewards. Liu and Pavlou (2021) looked to improve privacy policies for consumers using information technology. They prototyped an "active-recommendation" app which uses customer service agents to allow consumers to customize their own privacy policies. To test its effectiveness, Liu and Pavlou looked at the acceptance rate of three apps with three ways of displaying the privacy statement. App 1 had a link to the statement and had users select "agree" or "disagree", App 2 allowed consumers to select their privacy settings before agreeing or disagreeing, and App 3 implemented the "active-recommendation". App 1 turned out to have the

highest acceptance rate, but this seemed to be due to users accepting without reading the privacy policy. App 3 gave users the best experience by reducing their cognitive load and allowing them to fully understand the level of privacy they were giving up. Nget, Cao, and Yoshikawa (2018) set out to find a balance between money and protection of personal data through a data market. After taking a survey to estimate the type and value of information that will be sold, pricing for different sorts of data were made. Using this pricing, they were able to create a framework for a personal data market that more fairly compensates people for the loss of their privacy. Chong Wang, Cong Wang, and Zhang (2021) explored digital privacy from different perspectives and narrowed it down to three main ideas. These ideas are privacy as a psychological need, privacy as an economic tradeoff, and privacy as a technical artifact. In the psychological need for privacy, a new construct, "peer privacy concern," was found. This idea was that people feel that it is impossible to maintain their privacy due their peers being online. When exploring privacy as an economic tradeoff Chong Wang, Cong Wang, and, Zhang found the same "privacy paradox" as mentioned earlier. When looking at privacy as a technical artifact, a possible solution was found where using machine learning models were used to send masked results and ensure privacy of the user.

Participants

Participants include people who buy data and like Digital Advertising Alliance (DAA). This is an organization of big advertisers who together self-regulate online advertising (YourAdChoices 2023). Mr. Signorelli, counsel for the DAA explains how they want to "Provide standards and transparency for digital advertising," (Signorelli 2018). To do so, the DAA has developed tools that can help protect privacy like the ability to opt out of targeted advertising. Other participants include the consumers and people who protect them. The Electronic Privacy

Information Center (EPIC), is a non-profit organization who helps maintain Americans' right to privacy (EPIC 2023). EPIC Board Chair Zuboff says, “the fight for privacy as a fundamental right and an essential condition of a democratic society, has never been more urgent.” EPIC sees data brokers as “the hidden engine of the surveillance economy,” and a threat to Americans' privacy. To combat this, EPIC has pushed for restrictions on the data broker industry and protections for the consumers to help end data being “commercially exploited by brokers,” (EPIC 2023). The Federal Trade Commission (FTC) is a government agency that also works towards protecting online security. FTC Chairman Joe Simons explains that, “The Department of Justice is committed to protecting consumer data privacy,” and “ensuring that social media companies (...) do not mislead individuals about the use of their personal information,” (FTC 2019). Data collectors and social media companies like Meta are also involved. Meta strives towards growing their business and increasing their number of users of their services. To do so, they created social media platforms they believe are “inherently personalized,” and see that “providing ads tailored uniquely to users is a necessary and essential part of the service,” (Bushard 2023). To create this personalization, Meta collects large amounts of personal data. Twitter is another social media account that strives to increase its revenue and users, while also creating a “global town square” (CNBC 2023). In doing this though, twitter has also collected a significant amount of data. Twitter has collected phone numbers and email addresses, and used this information to help target users with ads.

References

Signorelli, F. A. (2018, May 23). *Campaigns & Elections quotes Michael Signorelli in an article about the digital advertising industry's transparency initiatives*. Venable LLP. https://www.venable.com/about/news/2018/05/campaign-election-mike-signorelli-ad-indust-transp

Electronic Privacy Information Center. (2023, January 16). *PRESS RELEASE: EPIC Announces Organizational Updates for 2023*.
https://epic.org/press-release-epic-announces-organizational-updates-for-2023/

Electronic Privacy Information Center. (2023, July 17). *PRESS RELEASE: EPIC Urges CFPB to Take Decisive Regulatory Action Against Data Brokers.*
https://epic.org/epic-urges-cfpb-to-take-decisive-regulatory-action-against-data-brokers/

Digital Advertising Alliance. (n.d.). *Integrate with DAA's CCPA Opt-Out Tool.*
https://digitaladvertisingalliance.org/integrate-webchoices-ccpa

Bushard, B. (2023, January 4). *Meta Fined Over $400 Million By EU For Alleged Personal Data Collection Violation*. Forbes. https://www.forbes.com/sites/brianbushard/2023/01/04/meta-fined-over-400-million-by-eu-for-alleged-personal-data-collection-violation/?sh=459bdfff5592

Ford, N. (2023, October 6). *List of data breaches and cyber attacks in 2023*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#:~:text=According%20to%20our%20research%2C%20there,total%20to%20over%204.5%20billion

Federal Trade Commission. (2022, January 27). *FTC imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook.* https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Auxier, B. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information.* Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Morey, T., Forbath, T., & Schoop, A. (n.d.). *Customer data: Designing for Transparency and Trust*. Harvard Business Review. https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

YourAdChoices (n.d.) *About the Digital Advertising Alliance*. https://youradchoices.com/about#:~:text=The%20Digital%20Advertising%20Alliance%20(DAA,solutions%20to%20online%20consumer%20issues.

Electronic Privacy Information Center. (n.d.). *About Us*. https://epic.org/about/

Meta (n.d.). *NOTICE OF Annual meeting and proxy statement. In META PLATFORM INC, NPCS 2023.* https://materials.proxyvote.com/Approved/30303M/20230406/NPS_535694/INDEX.HTML?page=1

Fair, L. (2023, September 15). *Updated FTC-HHS publication outlines privacy and security laws and rules that impact consumer health data.* Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2023/09/updated-ftc-hhs-publication-outlines-privacy-security-laws-rules-impact-consumer-health-data

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68*, 217-227 https://doi.org/10.1016/j.chb.2016.11.033

Liu, B., Pavlou, P. A., & Cheng, X. (2021). Achieving a Balance Between Privacy Protection and Data Collection: A Field Experimental Examination of a Theory-Driven Information Technology Solution. I*nformation Systems Research, 33*(1), 203–223. https://doi.org/10.1287/isre.2021.1045

Nget, R., Cao, Y., & Yoshikawa, M. (2017). How to Balance Privacy and Money through Pricing Mechanism in Personal Data Market. https://doi.org/10.48550/arxiv.1705.02982

Wang, C., Zhang, N., & Wang, C. (2021). Managing privacy in the digital economy. *Fundamental Research, 1(5),* Fundamental Research. https://doi.org/10.1016/j.fmre.2021.08.009 (Web of Science)