Undergraduate Thesis Project

# Developing a Comprehensive Network Traffic Monitoring System; Approaches, Challenges, and Solutions

(technical research project in Computer Science)

# The Balancing Act: Navigating the Tight Rope of Online Privacy

(sociotechnical research project)

by
Caleb Stoltz
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.

*Caleb Stoltz*

*Technical Advisor:* Rosanne Vgrutman, Department of Computer Science

*STS Advisor:* Peter Norton, Department of Engineering and Society

**General Research Problem**

*In the face of increasing cyberattacks and the emergence of Artificial Intelligence, how will cybersecurity effectively protect critical infrastructure?*

As cyber threats grow increasingly more common, especially within the growing use of artificial intelligence, the demand for reinforced cybersecurity measures for critical infrastructure increases. Not only does this provide a technical problem, but also a social dilemma. The illumination of the dual complications, reinforcing cybersecurity, and grasping ethical boundaries of privacy are vital in finding a further solution.

**Proposal and Development of a Network Traffic and Control System**

*How do current network monitoring systems maintain security levels with exponential growth in cyberattacks?*

Over the summer, I will be working closely with a mentor of mine in the cybersecurity field on a proposal design for a network traffic monitoring system. In relation to my STS work, the constant need for updated network security is vital in protecting personal online information. Rosanne Vgrutman in the UVA Department of Computer Science is also my technical advisor for my independent project with my mentor. Project goals include a proposal and possible development of a network traffic and control system. To get a leg up in my proposal, I have been looking into current systems involving network monitoring and filtering data packets. This proposal will benefit my future career in computer science and cybersecurity by broadening my knowledge on current systems and practices.

**The Balancing Act: Navigating the Tight Rope of Online Privacy**

*How do e-commerce enterprises, data collectors, and privacy advocacies compete to draw the line between legitimate and verboten collection of personal data online?*

With the rapidly evolving digital landscape, the fight for personal data collection between companies and users has reached an all-time high. The United States Census Bureau released that "in 2013, 74.4 percent of all households reported Internet use, with 73.4 percent reporting a high-speed connection (File, Ryan, 2014)." That number has only vastly increased in today's connected society with personal data-driven marketing. Mckinsey & Company, one of the most prestigious consulting firms, found that "data-driven campaigns are poised to increase sales in a core product by more than 10 percent (Bibby, Gordon, Schuler, & Stein, 2021)." Where the line falls between necessary online privacy and appropriate corporate data collection is a matter of major controversy.

E-commerce enterprises and data collections have many ways to collect data including the most common form, cookies, and pop-ups. Wagner states that "using third-party cookies, the third party learns the browsing history of users for all websites that its content is included on. (Wagner 2022)" Ad blockers commonly shut down for third-party tracking, but blockers cannot cut out everything. Wagner (2022) states that ad-blockers can only run as well as the system allows, meaning the operating system and web browser and their privacy standards.

Pham (2022) speaks on *Surveillance Capitalism*, the targeting of online user interests for company monetization. Company monetization of user search patterns has been one of the biggest markets for personal data collection since the early years of the Internet. “Marketing has been repeatedly carved out as an exception to strong privacy protection and the early commercialization of the web has resulted in more consumer rhetoric, debate, and laws—all of which serve a surveillance capitalism. (Lauer, Lipartito, 2022)” This is where the line between legitimate and verboten data collection becomes more ambiguous. While companies are required to give notice to any user of what data is being collected, notices often come in text-dense pop-ups that many will not read.

Participants involved in the debate on personal data collection include the United States Government Accountability Office. The U.S. GAO is a reputable office that specializes in providing Congress and other executive agencies that can be used to “improve the performance of the government, ensuring transparency and saving money (U.S. GAO, n. d.).” They state that since the U.S. does not have a full Internet Privacy Law, the Federal Trade Commission leads efforts on personal data collection. The US GAO was critical of the FTC claiming that they lack “regulations for Internet privacy other than ones protecting the privacy of children.” They also are looking for an implementation of an “overarching Internet privacy law” soon to enhance consumer protection (U.S. GAO, n.d.).

One of the most vital pieces in personal privacy and data protection is dependent on the web browser like Google, Firefox, etc. DuckDuckGo, an independent company, was founded in 2008 and made it their mission to not track the personal data of their users. DuckDuckGo (2023) does not save IP addresses, unique identifiers with searches, or any visits to websites. While other search engines use this data to sell to data collectors and e-commerce companies,

DuckDuckGo can profit from private search ads, instead of selling user information. DuckDuckGo looks to create a standard that other web browsers should follow, in protecting the user.

Advocacies in personal data collection like the Electronic Frontier Foundation and Privacy International are heavily involved as participant groups. They advocate for similar interests like digital privacy rights by engaging in legal battles and monitoring the actions of governments worldwide. Their approach aims to safeguard individual privacy in the digital realm (EFF, n.d.; PI, n.d.). The EFF (2022) and the Asian American Liberation Network filed a lawsuit against the Sacramento Municipal Utility District and the City of Sacramento due to the police unlawfully searching private data of energy usage per home for mass surveillance of neighborhoods to find cannabis cultivation prospects. They also avoided predominantly white neighborhoods and removed non-Asian names before running the energy analysis. (EFF, 2022) "National governments must put legal checks in place to prevent abuse of state powers, and international bodies need to consider how a changing technological environment shapes security agencies' best practices (EFF, n.d.)." Being founded in 1990, the EFF has participated in hundreds of legal battles in fights for personal data privacy and aims to draw the line between legitimate and verboten personal data collection.

## References


Bibby, C., Gordon, J., Schuler, G., & Stein, E. (2021, March 25). *The big reset: Data-driven marketing in the next normal*. McKinsey & Company. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-big-reset-data-driven-marketing-in-the-next-normal

DeWoody, Jillian. (2020). *CONNECTING AT-HOME NURSES WITH PATIENTS ONLINE; A COST to CONVENIENCE: HOW CONSUMERS MANAGE PRIVACY VALUES ONLINE*. Charlottesville, VA: University of Virginia, School of Engineering and Applied Science, BS (Bachelor of Science), 2020. University of Virginia Library

DuckDuckGo. (n.d.). *DuckDuckGo: Privacy Policy*. DuckDuckGo. https://duckduckgo.com/privacy

Electronic Frontier Foundation(EFF). (n.d). *Issues: Privacy*. Electronic Frontier Foundation. https://www.eff.org/issues/privacy

Electronic Frontier Foundation. (2022, November 3). *Asian American Liberation Network V. Smud, et al.* Electronic Frontier Foundation. https://www.eff.org/cases/asian-american-liberation-network-v-smud-et-al

File, T., & Ryan, C. (2014, November). Computer and Internet Use in the United States: 2013. US Department of Commerce.

Lauer, J. & Lipartito, K. (2022). *Surveillance Capitalism in America*. Philadelphia: University of Pennsylvania Press. https://doi-org.proxy1.library.virginia.edu/10.9783/9780812299946

Pham, Steven. (2022). *Design of a Prioritization Methodology for Equitable Infrastructure Planning; Examining the Ethical, Practical, and Societal Implications of Data Monetization*. Charlottesville, VA: University of Virginia, School of Engineering and Applied Science, BS (Bachelor of Science), 2022. University of Virginia Library

Privacy International(PI). (n.d.). *About Us*. Privacy International . https://privacyinternational.org/about

United States Government. (n.d.). *Critical Infrastructure Sectors*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

U.S. Government Accountability Office. (n.d.). *What GAO Does*. U.S. Government Accountability Office. https://www.gao.gov/about/what-gao-does

U.S. Government Accountability Office. (2019). *Your Internet Privacy*. U.S. Government Accountability Office. https://www.gao.gov/blog/2019/02/19/your-internet-privacy#:~:text=Information%20resellers%3A%20No%20overarching%20federal,legislation%20has%20not%20been%20enacted.

Wagner, Isabel. (2022). *Auditing Corporate Surveillance Systems: Research Methods for Greater Transparency*. Cambridge: Cambridge University Press. Cambridge University Press.