Undergraduate Thesis Prospectus

A Safer Web: Analyzing Cyber Risk

(technical research project in Computer Science)

Employee Surveillance: A Fight Against Undue Workplace Monitoring

(sociotechnical research project)

by

Matthew Walsh

November 2, 2020

technical project collaborators:

Emily Studtmann

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.

Matthew Walsh

Technical advisor: Jack W. Davidson, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

Matthew Walsh

STS 4500 (2:00)
November 2nd, 2020
Word Count: 1203

Prospectus

General Research Problem

Where is the appropriate line between privacy and security in a cyber-environment?

According to Statista (2020), there are 4.66 billion active internet users globally. Companies collect online user data to study their customer base and to develop targeted advertising campaigns (Clement 2020). Among American internet users, most report they "have very little or no control over the data that government (84%) or companies (81%) collect about them" (Auxier et al., 2019). To thwart cyberattacks, companies and government agencies collect online data, but most Americans report that the risks of such data collection outweigh the benefits (Auxier et al., 2019). Data collectors and privacy advocates compete to draw the line between necessary and invasive data collection.

A Safer Web: Analyzing Cyber Risk

Can machine learning tools accurately predict and prevent cyberattacks?

In order to prevent cyberattacks, programmers must fully understand how an attack works and what it does to a victim host in order to effectively dispel the harmful code. Using the Caldera cybersecurity interface, our research group will implement attacks and monitor the damage they cause in order to form usable countermeasures. The data from these attacks will be

collected and stored for use in machine learning algorithms so that antivirus software can be updated to use these algorithms to predict and prevent attacks of similar nature.

Microsoft's Windows Defender and Advanced Threat Protection platform and Amazon's Cloud Services platform are among many that use machine learning to analyze data for enhanced protection against attacks. This project aims to find similar methods for protection against specific attacks we create. Unfortunately, though not surprisingly, much of the specifics regarding current cybersecurity platforms are not available due to security concerns that would arise from any transparency in a security system. One main issue with using machine learning to scan for harmful code is that the algorithms must be trained on attacks that are known, yet many successful attacks are only successful because the method of attack is new. Currently, we are setting up our platform and working on specific attacks with the plan of expanding to more attacks for a broader collection of data. We will start by analyzing more common attacks, then move to newer, harder to detect attacks. Upon each attack, relevant data will be collected and fed into algorithms for training, and these algorithms will then be tested to see if, when given input code, they can detect that a threat is present. The goal of this project is to create a system that can identify the threats for which it is trained, and to learn more about new styles of hacking or malware implementation. Professor Jack Davidson in the Computer Science Department will be overseeing the group of graduate and undergraduate students working on the project.

Employee Surveillance: A Fight Against Undue Workplace Monitoring

How do employers and employees determine the line between justified employee surveillance and unwarranted invasions of privacy?

In March 2020, quarantines and lockdowns to prevent coronavirus transmission contributed to the biggest single-month increase in unemployment in the U.S. since 1975 (BLS, 2020). Many workers who kept their jobs shifted to remote work. According to the U.S. Bureau of Labor Statistics, 22.7 percent of laborers were working from home in September 2020; 37 percent of jobs may eventually shift to fully remote work (BLS, 2020). To monitor employees working from home, many employers now require access to workers' keystrokes, screens, and electronic communications. To many employees, however, such practices are invasions of privacy.

Among employees, about 70 percent suspect their employers "routinely monitor their behavior at work" (Wronski, 2019). To many employers, however, surveillance is necessary to prevent data breaches, which cost companies an average of 3.86 million dollars each (IBM, 2020). About 57 percent of these employees perceive monitoring as more harmful than beneficial (SHRM, 2020). Vendors of workplace surveillance systems, however, contend that employers must determine whether employees are "working hard or hardly working," and "who is accessing sensitive files or participating in risky activities" (InterGuard, 2020). Such companies promise their clients that with such systems, they can "monitor and control user activity to ensure compliance with internal security policies and regulatory requirements" (Teramind, 2020).

Employers must comply with the Electronic Communications Privacy Act of 1986, which limits workplace surveillance. Many state laws require employers to inform their employees of any monitoring policies (Mehl, 2020). Delaware and Connecticut require employers to inform workers when their email accounts are monitored (Laird, 2020). Employees generally lose such rights, however, when they use their employer's devices or accounts (PRC, 2019). For example, in *U.S. v. Hamilton* (2012), the court found that because an employee "did not take any steps" to

protect his email on a company computer, he had abandoned his right to privacy (EPIC, 2012). In *Bărbulescu v. Romania,* an employee who had used a work account for personal correspondence contended that his company had "unjustly prioritized the employer's interest over his right to privacy." However, the European Court of Human Rights found that because the employer had disclosed its surveillance policies in the employee's contract, they were well within their rights (Columbia, 2017). U.S. courts are still determining the legal limits of employer surveillance of personal devices that employees use for work (Laird, 2020).

The American Civil Liberties Union (ACLU) contends that employer surveillance "often goes well beyond proper management concerns and becomes a tool for spying on employees in furtherance of no legitimate business interest" (ACLU, 2018). ACLU resists such excesses, in part by ensuring that employees have access to legal counsel. The ePolicy Institute consults with companies to "maximize compliance, manage behavior, and minimize risks—including litigation and regulatory investigations—through best-practices-based policies and employee training programs" (ePolicy Institute, 2020).

Researchers have studied the effects of the pandemic on workplace surveillance, and the risks and benefits of monitoring employees. Shoebrige (2020) contends that until a covid vaccine is widely available, employers must track and trace employees to limit workers' exposure. As remote work proliferated from April to June 2020, demand for remote employee tracking tools rose by 10 percent; now 45 percent of employees who work remotely believe that their employers monitor them.

Surveillance can compromise employees' trust of their employers. Accenture (2019) found that monitoring diminishes trust among 52 percent of employees, estimating the consequences may cost companies 3.1 trillion dollars globally. Zhang and Bock (2006) found

that strict policies may limit job satisfaction as well. Fichtner, Strader and Scullen (2013) argue that non-work related computing (NWRC) policies must be well defined and explicitly enforced via a "comprehensive written policy" to ensure that employees are held accountable for inappropriate use of company technology.

Workplace surveillance is not new. McParland and Conolly (2020) note that Jeremy Bentham's 1791 prison design, the panopticon, featured "an observation unit" from which a warden could "observe any inmate in the unit at any time." The prisoners, however, could not tell when or if the warden was watching. Similarly, remote workers may be unaware that companies "observe their employees and collate data on them" (McParland and Conolly, 2020).

References

Accenture. (2019, January 21). More Responsible Use of Workforce Data Required to Strengthen Employee Trust and Unlock Growth, According to Accenture Report. https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.html

ACLU (n.d.). American Civil Liberties Union. The Rise of Platform Authoritarianism. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/rise-platform-authoritarianism

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bărbulescu v. Romania. (2017, Oct 16). https://globalfreedomofexpression.columbia.edu/cases/case-barbulescu-v-romania/

BLS (2020, June 1). U.S. Bureau of Labor Statistics. Ability to work from home: Evidence from two surveys and implications for the labor market in the COVID-19 pandemic : Monthly Labor Review. (2020, June 01). https://www.bls.gov/opub/mlr/2020/article/ability-to-work-from-home.html

Clement, J. (2020, October 29). Internet users in the world 2020. https://www.statista.com/statistics/617136/digital-population-worldwide/

Electronic Communications Privacy Act of 1986 (ECPA). (2019, April 23). https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

EPIC (2012, Dec. 13). Electronic Privacy Information Center. United States v. Hamilton. https://epic.org/amicus/hamilton/

ePolicy Institute. (n.d.). Welcome to The ePolicy Institute. http://www.epolicyinstitute.com/

Fichtner, J., Strader, T. J., & Scullen, S. E. (2013). *Creating, Clarifying, and Enforcing an Effective Non-work Related Computing Policy: A Legal Perspective* (Rep.). Penn State University Press. JSTOR

IBM. (2020). Cost of a Data Breach Study. https://www.ibm.com/security/data-breach

Interguard. (2020) Remote Employee Monitoring & Productivity Tracking Software.

(2020, October 06). https://www.interguardsoftware.com/?utm_campaign=brand

Laird, L. (2020, June 23). What Are Your Privacy Rights When You Work From Home? https://www.legalzoom.com/articles/what-are-your-privacy-rights-when-you-work-from-home

McParland, C., & Connolly, R. (2020). *Dataveillance in the Workplace: Managing the Impact of Innovation* (Rep.). Dublin, Ireland: Dublin City University Business School.

Mehl, B. (2020, August 13). The State of Employee Privacy and Surveillance in 2020. https://www.getkisi.com/blog/state-employee-privacy-surveillance

PRC (2019, June 27.) Privacy Rights Clearinghouse. Somebody's Watching Me: Employee Surveillance. https://privacyrights.org/resources/somebodys-watching-me-employee-monitoring

Provision Living. (2020, June 25). Smartphone Screen Time: Baby Boomers and Millennials. https://www.provisionliving.com/news/smartphone-screen-time-baby-boomers-and-millennials

Shoebridge, M. (2020). *Returning to work during the pandemic: Testing, surveillance, apps and data as our near term future* (Rep.). Australian Strategic Policy Institute. JSTOR

Teramind. (2020, November 01). https://www.teramind.co/?utm_source=Google

Wronski, L. (2019, October 25). Axios poll: Workplace surveillance. https://www.surveymonkey.com/curiosity/axios-poll-workplace-surveillance/

Zhang, C., & Bock, G. (2006). *Why Employees Do Non-Work-Related Computing: An Investigation of Factors Affecting NWRC in a Workplace* (Rep.). Pacific Asia Conference on Information Systems. JSTOR

Zielinski, D. (2020, August 08). Monitoring Remote Workers. https://www.shrm.org/hr-today/news/all-things-work/pages/monitoring-remote-workers.aspx