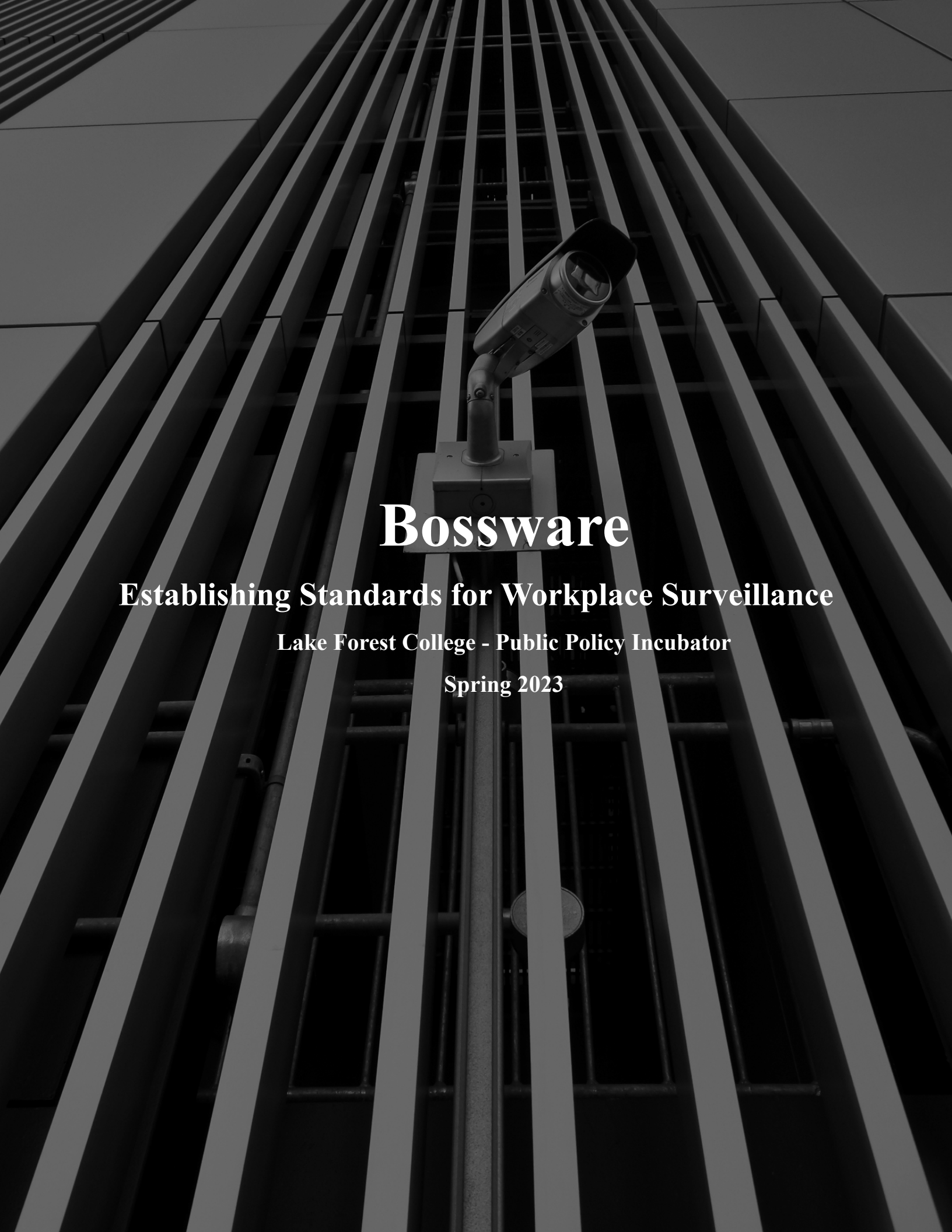


Bossware

Establishing Standards for Workplace Surveillance

Lake Forest College - Public Policy Incubator

Spring 2023

Contents

Foreword

Lake Forest College is a center of learning designed to help guide and foster the next generation of thinkers, with a large focus on both domestic and international talent. Within it, the Public Policy Incubator is an initiative designed to emulate the work taking place at NGOs, think tanks, and political offices. This program is focused on helping students hone their analytical skills in ways that allow for real-world consideration and practical policy making.

Hannah Tarshis

A junior at Lake Forest College majoring in English Literature with a minor in Asian Studies concentration in Chinese. She is from Chicago and enjoys video games, reading, and petting cats.

Shang Chen

A senior student at Lake Forest College, who is majoring in International Relations and minor in Asian Studies : concentration in Japanese. She comes from Shenzhen, a southern seaside city in China. She has spent a lot of fun time with snow and lake here.

Thomas Russell

A senior at Lake Forest College, currently majoring in Politics with a Legal Studies minor. He has been a local resident of the Lake County area for over twenty years, having moved to Lincolnshire from the United Kingdom as a child.

Executive Summary

Bossware is a relatively recent development that will continue to have long reaching consequences for many employees today. It exists as a constant invasion of their privacy and peace of mind. Especially so when such actions are taken without their consent or knowledge. The term Bossware is the usage of workplace monitoring systems by the employer targeted at the employees. This can range from webcam usage and keystroke tracking, in targeted circumstances, to that of surveillance cameras for general observation. A key concern is that in some circumstances, depending upon the depth of the surveillance, it is comparable to spyware, which is how the terminology was coined. Through the examination of three states, Connecticut, Delaware, and New York, that currently have such anti-Bossware laws, we propose legislation for Illinois that will likewise attempt to curb Bossware surveillance by requiring employers to notify employees of any such activities. Through the combination of different ideas from each, we will seek to provide a comprehensive proposal that covers the weaknesses of the three aforementioned. Such as New York's exemption of its governmental jobs from such protections. This proposal analyzes how Illinois should enable greater protections for its workforce, balanced with the security for corporations against liability risks that come from an unlegislated environment. Key ideas are mandating that employees must be informed, prior to the occurrence, of all forms of monitoring done at the workplace or on work devices, and that the retention and scope of data collected be kept to a reasonable level.

Introduction

The history of employment has always been one riddled with strife, centuries of slavery and serfdom have shown us this much. It is from this strife that great progress has been made towards the protections and rights of the working people. In 1945, Electronic Numerical Integrator and Computer (ENIAC), the first Turing complete computer was created (Weik, 1961). 29 years later, in 1974, with the development of Transfer Control Protocol, the first instance of the internet was born (Cerf, 1974). Two decades later, the first webcam, known as "Trojan Room coffee pot" was developed (Gordon). The rise of the internet in the past forty years is but a blink of an eye on the calendar of humankind, and the subsequent electronic workplace developed from it is still in its infancy, especially so when it comes to the relevant legislation designed to shape and protect those who reside within. This paper seeks to discuss "Bossware": what it is, how it has affected the workplace, and what are some possible regulations that might bring positive impact to those most affected by it.

The collective term for surveillance tools designed to keep track of employees, bossware seeks to provide managers with a constant stream of information about the productivity of their employees. Residing in the same vein of technology as spyware and malware, which garner attention for being illicit practices, bossware gains legitimacy from the self-induced nature of it by the employer onto their own property. However, recent history with the COVID-19 pandemic and the rapid shift of the workplace from the corporate environment to that of employees' private homes, has brought to bear questioning of this supposed legitimacy. With the inability of managers to maintain surveillance through physical proximity, and the preconceived notion that without existing in a corporate environment workers will slack off, the implementation and invasiveness of employer surveillance (bossware) has seen a drastic increase throughout the entire corporate sphere. A key factor to the questionability of bossware legitimacy, when talking about the implementation of tools that can potentially surveil an employee in their private residence, is the duality of it to that of other surveillance devices such as Google Voice, Siri, and Alexa. While these have their own contentions, specifically with how the subsequent data is recorded and potentially abused, they are a product that the employee has consented to of their own volition. Bossware, however, carries the power imbalance of the employer to employee hierarchy, in which it can be perceived that the act of denying or circumventing the employer's surveillance could lead to citation and possibly termination. Therefore any intrusion by the employer into the employee's life, must be upfront and transparent, with contractual consent.

Modern Workplace Surveillance

Modern society is a technological and digitized world. Within it, people have become accustomed to living with digital surveillance and constant data collection. Russo and colleagues once predicted there will be more than 200 billion sensor devices internet connected by 2020 (2015). Where those sensor devices can be found in “home electronic systems, health monitoring equipment, cars, and smartphones” (Russo, 2015). If there was a question of whether technology has been good or bad for humanity, it would be reasonable that most people would say the development of technology has been more beneficial than harmful for human life. Mackenzie Adams also points out, societal functioning has highly depended on information and communication technology, known as “big data”. According to him, “big data” and its relevant products have made great achievements in the field of medicine, transportation, and education (2017). GPS enables people to travel farther, faster, and more conveniently. For example, People can request a ride through Uber or order food from DoorDash without ever having to leave the comfort of their living room. This constant stream of data collection can serve the customer too. Apps can show the location of your scheduled driver or the progress of their meal. Such services would not be able to exist without this omnipresent data acquisition system. Ever since such electronic tracking technologies have significantly improved the average person's quality of life, more and more people have subconsciously grown accustomed to the electronic tracking and data collection functions, even going so far as to start enjoying these electronic tracking technologies, bemoaning when certain products don’t have a to the minute tracking of delivery products. But what if those electronic traces found their way into your work environment?

Originally, companies started installing software and hardware on their computers that could track their location, with the aim of preventing the loss of company property. But soon, the practices were expanded so that employers could: show worker location, record interactions with co-workers, and monitor worker’s smartphone activities through surveillance software. Bossware began to collect all the employee data it could get its hands on. Depending upon the invasiveness of the software, it could even collect employees’ chat information from no matter which app or electronic device used. Even though in most cases, managers need to have a good reason and the consent of IT and HR to get access to employees' private chat messages, technically speaking with them already holding it, it is not very difficult for them to get access to your personal information.

What bossware uses is not a newly invented technology or concept. It has simply reached new heights at the right time - the outbreak of COVID-19 - and expanded on a large scale without being fully understood or restricted by most people. Prodoscore was founded in 2018 as an employee monitoring software company. Although this company focused on developing bossware products, it was not specifically designed for COVID-19. However, the unexpected increase in the number of remote workers has made the development of this technology far beyond what people imagined. According to data from Global Workplace Analytics, the epidemic has caused the number of remote workers to increase by 140% since 2005. Moreover, given the pushback to returning to the office post-pandemic, the number of these remote workers

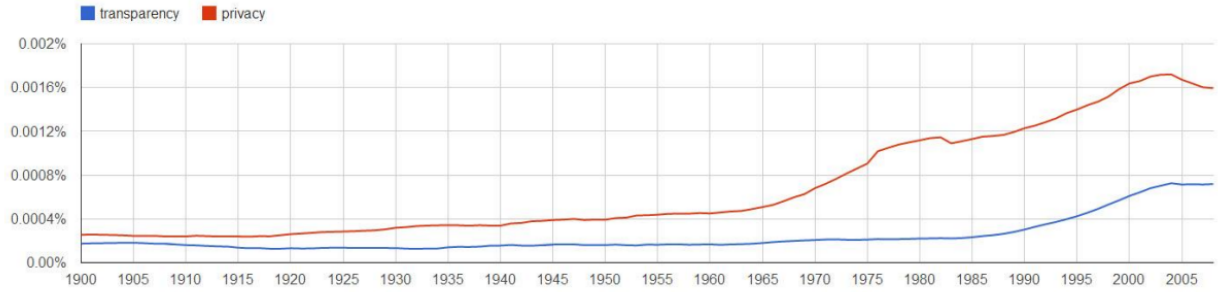
may not decrease in the future. Therefore, more and more employers are choosing to use bossware to supervise their employees to ensure the efficiency of remote work. InterGuard reported that its customer base grew by over 300% in just the first few weeks after the outbreak. Time Doctor claims to have big companies, such as Allstate, Ericsson, and Verizon, among its 83,000 users. ActivTrak is used by more than 6,500 organizations, including many universities, while StaffCop and Teramind serve clients from various industries, such as healthcare, banking, fashion, manufacturing, and call centers.

This is far from over. Two years after the outbreak of COVID-19, a report from Coworker.org shows that more than 500 new technologies have been developed to monitor employees and their work in 2022 (Davis, 2022). At the same time, Digital.com put out a survey of 1250 employers in the US, which shows that 60% of employers across the country tell their employees that they will use surveillance software. Meanwhile the survey also shows that 88% of companies will fire employees based on information collected from bossware (2023). Moreover, in addition to the visible monitoring part, these software also have invisible monitoring parts. Employees may not even know that they are being monitored and their personal data is collected. This is resulting in an awakening for people to think whether the data collected by these software goes too deep into the field of personal privacy.

Based on the data presented, it is evident that the use of bossware is increasingly prevalent in today's work environment. However, being common doesn't mean it is always right. Bossware enhances employers' power and tears a big hole in the harmonious work relationship between employees and employers. Although the majority of employers in the Digital.com survey confirmed bossware is positive and useful in helping them to manage the company and the business (2023), there are many voices from workers who say they are suffering from bossware at work. Many employees feel that they are not trusted after knowing that they have been monitored while working, which dampens their enthusiasm for work and hurts their personalities. Besides, bossware visualizes the employees' efforts into various numbers, which also gives employees a sense of being a tool. What's more, there will always be something that can't be simply calculated from the time used on the computer, like how much effort an employee has spent on a group idea. It is unfair to adjust someone's effort by the number on the surveillance tool. We can change the situation before the cruel and heartless working society walks from a science fiction movie into reality.

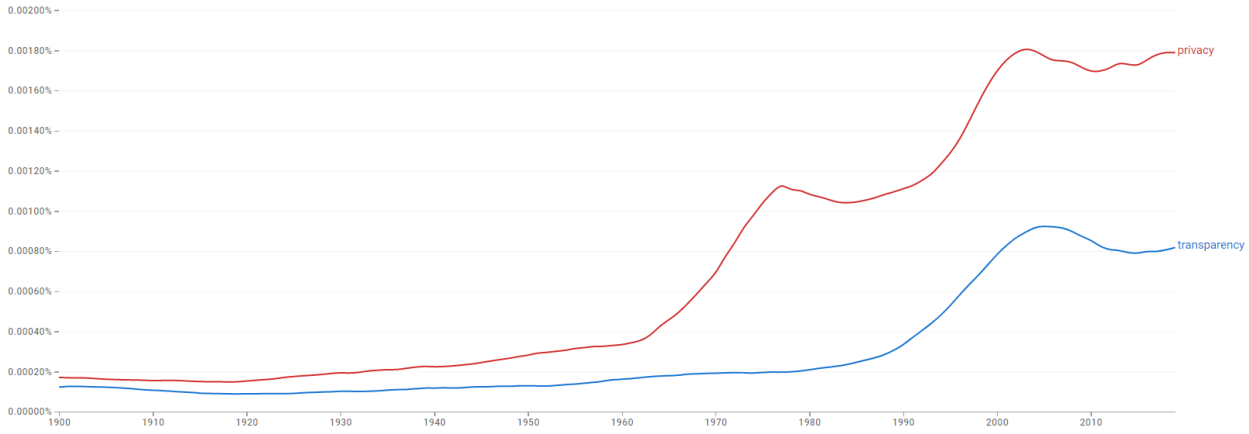
In his work, *Making Transparency Transparent: The Evolution of Observation in Management Theory*, Ethan S. Bernstein compares the terms privacy and transparency. Asking "Why has privacy had so little impact on management and organizations scholarship while transparency has had so much?" (Bernstein 40). To which he answers that it is due to the lack of legislation. That the "Constitutional privacy protections apply only in the case of "state action"; that is, they apply in the workplace only if the employer is the government" (Bernstein 40). The following chart was generated by Bernstein to highlight that while the practical use of the term "privacy" has risen, along with an increase in "transparency", he states that its "use as a scholarly concept, unlike that of transparency, has actually narrowed." (Bernstein 39).

Figure 6: Privacy and Transparency Appearances in Text



Source: Google Books Ngram Viewer (http://books.google.com/ngrams/)

If this is then compared to a recent generation of the same terms, with the end-date of 2019, building off Bernstein's 2007 trends. It can be seen that the rise and fall of both terms are becoming synchronous, indicating a modern day relationship between the two within the public mindset.



Concerns for Workers' Privacy and Rights

If it is true that the growing use of electronic surveillance is due to the work environment changes caused by the pandemic, then will the work environment eventually change back to what it was before? In that case, the issues caused by bossware may no longer be a major concern. Judging from some survey data, people's enthusiasm for returning to offline work is far from that great. With the outbreak of the new crown epidemic in 2020, most people had to leave the company's office building and go home to work. In the spring of 2020, about 60% of the total number of American employees went home to work remotely. This figure expanded again to 71% in October 2020. Although the impact of the epidemic has gradually diminished since mid-2021, the number of telecommuters has not decreased as rapidly as everyone imagined. As of January 2022, 59% of people still work from home all the time, and 18% will go to the company for a few days from time to time in a week. Among those who work remotely, 78% said they would continue to work from home post-pandemic if given the choice (Parker, Horowitz and Minkin, 2022). So it can be said that job monitoring software will be another technology that we will definitely coexist with in the future.

From a historical perspective, technological development sometimes reshaped the way people work and live, and then went on to cause more problems. As people's travel methods gradually changed from horse-drawn carriages to cars, people needed a new set of traffic rules to prevent car accidents. Surveillance software and technology in the field of electronic technology are developing, but workers' ability to defend their rights are getting weaker and weaker. At present, this problem mainly has two manifestations: first, the company does not have enough transparency about the monitoring of employees at work. Many employees don't even realize they're being watched, and even if they do, they don't quite know what information is being collected about them. According to a survey report from Digital.com, there are 14% of the majority of employees who don’t have any idea that their boss is watching them (2023). The concerning situation goes even further, as Electronic Frontier Foundation points out that these monitoring products usually don’t distinguish between work-related activity and personal account credentials, bank data, or medical information (Ascott, 2022). Which means, the high-level privacy information has the risk of leaking at any time. Second, there is still a lack of a clear definition of electronic monitoring intrusion into workers' personal privacy in law. This also makes employees lack any ability to defend their rights.

Kathryn Zickuhr, a labor market senior policy analyst at the Washington Center for Equitable Growth, claims the workplace surveillance behavior undermines the worker power by changing the structure of jobs and work in“*Workplace surveillance is becoming the new normal for U.S. workers*” (2021). According to Kathryn, lacking the legal protections or regulatory restrictions of workplace surveillance is the main reason for undermining worker power in the United States. She says the current legal framework for protecting privacy has a long way to go. In fact, America doesn't seem to have a privacy protection law for workers. The previous privacy protection protocol is more for customers. She points out if a company claims that there is a business-related reason for the surveillance, workers may have very fewer rights to privacy in the

workplace. When worker power becomes weaker, the intrusive and revealing surveillance will become more brazen and ultimately lead to worker exploitation.

State Implementation

In addressing potential solutions to the problems of Bossware, it is important to take note of what regulation has already been implemented by multiple legislations throughout the United States. Regarding the topic of digital surveillance and the resulting privacy laws, few states have enacted encompassing regulation, and those that have, mainly focus on the topic of awareness and consent of the target in question. The states in question are: New York, Delaware, and Connecticut. Each of which we will breakdown and analyze their approach in turn.

Overall, the current level of legislation in place in regards to digital surveillance and workplace privacy are severely lacking comparatively to GDPR, with all three states simply requesting prior notice and acknowledgement, not to mention the rest of the states that have no such requirements at all. As it stands, these operate as a baseline level of implementation that we know can and have been passed, thus anything more from here is what we seek to advocate for in this paper.

New York

Starting with the Laws of New York, *Chapter 6 Civil Rights Article 5 Right of Privacy Section 52-C*, titled "Employers engaged in electronic monitoring; prior notice required". Within, it is broken down into four points, the first addresses who this law encompasses, the second follows by addressing the stipulated restrictions, third what the punishments for being found in violation of this law are, and finally fourth a provision for what it does not protect against. For who it encompasses, that is any type of employer, be it an individual person, all the way up to a massive corporation, as long as it does business within the state. However, it does state that "It shall not include the state or any political subdivision of the state." (NY §52-c 1), which is interesting that it would exempt the governmental divisions from requiring prior notice. As for the stipulated regulation itself, it is broken down into two parts. First, that in the event where the employer will be monitoring or intercepting any form of telephone or internet access, a prior written notice must be given upon hiring an employee, and "acknowledged by the employee either in writing or electronically" (NY §52-c 2a). At the same time, a notice of electronic monitoring must be posted in a visible place. And secondly, that the employee must be made aware that such monitoring can happen at "any and all times and by any lawful means" (NY §52-c 2b). The violations for failing to adhere to the proper disclosure and awareness of workplace monitoring are a civil penalty maxing at $500 for the first breach, $1000 for the second, and then $3000 for every offense after. Finally, the law excludes monitoring that is "not targeted to monitor or intercept the electronic mail or telephone voice mail or internet usage of a particular individual" (NY §52-c 4), as in data that is volumetric in nature and operates "solely for the purpose of computer system maintenance and/or protection." (NY §52-c 4). Taken as a whole, the New York law can be understood to aim at curtailing unknown/hidden surveillance, with the approach that as long as the employee has understood they are to be monitored, it is permissible. What is of note is that the government, both at the capstone and down into the subdivisions are exempt from being required to give such notice.

Delaware

For the Delaware Code, *Title 19 Chapter 7 Employment Practices Section 705*, named "Notice of monitoring of telephone transmissions, electronic mail and Internet usage". The Delaware legislation starts off the same as the New York one, introducing who is defined as an employer, but unlike New York's there is no exclusion for the state government from being included "the State of Delaware or any agency or political subdivision thereof." (DE §705 a). Interestingly, they offer two modes of notice to be in compliance with monitoring. Either by providing "an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer-provided e-mail or Internet access services" (DE §705 b1), or that of a 1-time notice with employee acknowledgement, similar to that of New York's requirements. As for the penalty, each violation is only subject to $100, as such it can be seen as being considerably more lenient than New York. Finally closing out with the same provision giving exception to monitoring not of an individual, but the system at large for maintenance and/or protection processes. Observing the differences so far, the underlying message of employee awareness is consistent, and while Delaware takes a step forward in including state employment in the legislation, the cost of infringing on the law does seem low in comparison.

Connecticut

The third legislation is that of the Connecticut legislation, *Chapter 557 Employment Regulation Part II Protection of Employees Section 31-48d*, titled "Employers engaged in electronic monitoring required to give prior notice to employees. Exceptions. Civil penalty.". Acting the same as Delaware, Connecticut includes the state in their employer classification. When it comes to defining what "Electronic monitoring" is though, they specify that it is "the collection of information on an employer's premises" (CT §31-48d 3), whereas the prior two state legislations made no verbal declaration of premises. They also stipulate that any monitoring for "security purposes in common areas" (CT §31-48d 3a) does not fall under this monitoring status. However, the mode of informing the employees is similar, in that a prior written notice must be given to all affected employees, and that a notice about said monitoring must be posted in a visible location. Interestingly, it goes on to stipulate more exceptions to these rules, wherein as long as the employer believes an employee "(i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment, and (B) electronic monitoring may produce evidence of this misconduct" (CT §31-48d 2) then the employer is given the ability to conduct monitoring actions without having to provide a notice for informed consent. The Connecticut legislation then finishes with a penalty amount the same as New York's, starting at $500, followed by $1000, and then $3000 continued after that. Overall, the legislation in place by Connecticut has the most considerations for the employer's benefit, and it would be interesting to see just how terms such as "premise" and "hostile workplace environment" hold up, as they have a broad reach on just what they dictate.

Illinois State Legislative Proposal

Based on the current implementation format of previously mentioned state legislation, and the landscape of Illinois' corporate environment, the following proposal has been drafted as a potential solution for the current concerns and needs of both employer and employee alike.

1. For employers subject to Illinois law who engage in the act of electronic monitoring, prior notice for all actions is required.
2. Employer is defined as any individual, corporation, partnership, firm, or association that has a place of business within the state. The state, as well as any and all political subdivisions of the state are also included in such.
3. The act of electronic and digital monitoring includes in scope that of: intercepting telephone conversations, electronic mail, internet access or usage, of any employee by any electronic device, including but not limited to the use of computers, telephone, or radio systems.
4. Prior notice about such monitoring must be presented and acknowledged either in writing or electronically upon hiring any and all employees potentially subject to electronic monitoring.
    a. Further notice must be given and acknowledged upon access request to internal internet networks that are subject to monitoring.
    b. Further notice must be given at the start of any telephone conversations subject to recording or monitoring.
    c. Further notice must be given in disclaimer notice within any electronic mail that is subject to monitoring.
    d. For areas of the workplace that are under constant monitoring, a notice of such actions detailing the breath and content of monitoring must be physically posted in an easily visible position.
5. For the retention of data, it can be kept for up to 6 years after the last interaction.
6. Upon request of deletion of data, information must be removed after a formal request has been submitted.
7. Attorney general may enforce the provisions of this legislation. Any employer found to be in violation of this shall be subject to a maximum of $500 for the first breach, $1000 for the second, and $3000 for the third and each subsequent offense committed.
8. Exclusions for processes that manage volume, not targeted at the usage of any particular individual, that do not record data transmitted, for the sole purpose of internet system maintenance or protection.

Analysis of Solution Viability

Any solution would likely have to involve getting proper consent from all those involved and making sure everyone is properly informed of what all that might occur. But employees might feel pressured to agree with anything in order to get the job, so some of the more egregious methods of data collecting should be banned or limited, such as most things involving brain scanning technology, which is discussed in the Wall Street Journal article "*When Your Boss Is Tracking Your Brain"*.

A potential solution would likely involve pull and push reports for data gathering. With pull reports being data that an employer can look into at any time and pull information from, and push reports being self reported employee data. It could be said that push reports are more ethical due to the inherent consent and awareness involved in self reported data, but it will likely depend on individual jobs to decide what method is the best for efficiently gathering necessary information for the job. The meaning of "necessary information" might have to be determined or reviewed by an unbiased source due to companies probably wanting to say they need more information on their employees than they actually do.

Amazon said they were planning to display AI cameras around their drivers in 2021 (Stanley, 2021). The AI camera will uninterruptedly monitor the driver and report to the company if the AI thinks the driver did something wrong. Can AI really judge the state of employees reasonably? What information does the AI use to judge? Will employers know this information? Will the company collect and use this personal information? What if the AI gets it wrong? There are no answers to these questions right now. Although it can be discussed whether it is reasonable or not, but for now, it is legal to load AI cameras. Apparently, technology is ahead of all laws.

After analyzing the data and reviewing the relevant laws, it is clear that new legislation must be implemented quickly due to the rapid pace of technological advancement in modern society. Since the launch of ChatGPT in November 2022, it has undergone four iterations, which highlights the urgency of this issue. However, it is important to note that the law may not always keep up with technology. For instance, the use of Amazon's AI surveillance plan and the potential integration with other surveillance software in the future is unpredictable. As such, it is difficult to propose a feasible prevention plan at this time. Instead, a clearer legal basis and more stringent penalties are necessary to protect workers' privacy and rights. In her article, "Workplace surveillance is becoming the new normal for U.S. workers," Kathryn suggests establishing oversight and enforcement measures for workplace monitoring and requiring companies to transparently disclose surveillance behavior. This new standard should prioritize protecting workers and hold companies accountable for their surveillance practices.

During the Atlantic Council Discussion on Cybersecurity Strategy on April 6th, Jen Easterly, the director of the Department of Homeland Security in Cybersecurity and Infrastructure Security Agency, proposed a concept called the "burden shift." This idea suggests that greater responsibility should be placed on the provider of the big cloud, rather than placing the same high information security risks on users. Similarly, when it comes to bossware, the

transfer of responsibility should also be considered. Companies cannot simply rely on employees to protect their privacy and personal data by making their surveillance behavior public. Instead, they must take responsibility for any privacy violations. Workers should not be expected to be highly knowledgeable about privacy protection or to constantly worry about potential violations of their privacy.

Conclusion

Douglas Adams, an England science fiction novelist, once made three interesting principles to conclude people's relationship with technology: "1) Anything that is in the world when you're born is normal and ordinary and is just a natural part of the way the world works. 2) Anything that's invented between when you're fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it. 3) Anything invented after you're thirty-five is against the natural order of things" (Becher, 2014). Though Adams says that in a humorous way, he indicated the statement that technology is growing too fast and it can not always be controlled by people who invented it. No matter what good ambitions the technology holds, that product can be used in a dangerous and dark way. Same story happened with bossware issues.

Through previous analysis, bossware raises deeper concerns about worker privacy and worker power along with its function, which is workplace surveillance. Being a surveillance tool based on digital equipment, bossware is not well understood by many people, resulting in a significant gap in potential protection against harm. Researching those states with legislation already implemented, provided perspective for the standards necessary to protect employees from the wanton use of bossware related tools. While providing the companies with a set of guidelines to streamline management resources and alleviate liabilities.

References:

Adams, Mackenzie. “Big Data and Individual Privacy in the Age of the Internet of Things.” Technology Innovation Management Review, 7(4): 12-24. April 2017. http://doi.org/10.22215/timreview/1067

Ascott, Emma. "Bossware: 14% Of Remote Employees Are Unaware They’re Being Monitored." AllWork.Spance. March 4, 2022 https://allwork.space/2022/03/bossware-14-of-remote-employees-are-unaware-theyre-being-monitored/

Becher, Jonathan. “Douglas Adams' Technology Rules”. Forbes.com. July 7, 2014. https://www.forbes.com/sites/sap/2014/07/07/douglas-adams-technology-rules/?sh=7a824c2153e6

Bennett Cyphers and Karen Gullo. Inside the Invasive, Secretive “Bossware” Tracking Workers. June 30, 2022. https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers

Bernhardt, A., Kresge, L., & Suleiman, R. (2023). The Data-Driven Workplace and the Case for Worker Technology Rights. ILR Review, 76(1), 3–29. https://doi.org/10.1177/00197939221131558

Bernstein, E. S. Making transparency transparent: The evolution of observation in management theory. Academy of Management Annals, 11(1): 217-266. https://www.hbs.edu/ris/Publication%20Files/BernsteinE-MakingTransparencyTransparent-AMA2017HBS_1ffde6a8-90b5-4dcb-8014-c2eea12b78bf.pdf

Cerf, V., Dalal, Y., & Sunshine, C. “SPECIFICATION OF INTERNET TRANSMISSION CONTROL PROGRAM” December 1974 https://datatracker.ietf.org/doc/html/rfc675

Connecticut, *Chapter 557 Employment Regulation Part II Protection of Employees Section 31-48d* https://www.cga.ct.gov/current/pub/chap_557.htm#sec_31-48b

Davis, Jerry. “No hiding place: ‘bossware’ is spying on you in the home, office and car”. Audio articles. October 24, 2022. https://www.imd.org/ibyimd/magazine/no-hiding-place-bossware-is-spying-on-you-in-the-home-office-and-car/

Delaware, *Title 19 Chapter 7 Employment Practices Section 705*
https://delcode.delaware.gov/title19/c007/sc01/index.html

Digital.com Staff. “6 in 10 employers require monitoring software for remote workers.” Digital.com. Updated February 22, 2023.
https://digital.com/6-in-10-employers-require-monitoring-software-for-remote-workers/

Glass, Ashley. “'Bossware' here to stay, experts predict, as employers monitor their workers.” December 12, 2022.
https://www.wptv.com/news/science-tech/bossware-here-to-stay-experts-predict-as-employers-monitor-their-workers

Gordon, Daniel “Trojan Room Coffee Pot”
https://www.cl.cam.ac.uk/coffee/coffee.html

Journal, A. O. T. W. S. (2023, February 16). *When your boss is Tracking Your Brain*. The Wall Street Journal. Retrieved March 9, 2023, from
https://www.wsj.com/articles/brain-wave-tracking-privacy-b1bac329

New York, *Chapter 6 Civil Rights Article 5 Right of Privacy Section 52-C*
https://www.nysenate.gov/legislation/laws/CVR/52-C*2

Parker, Kim, et al. "COVID-19 Pandemic Continues To Reshape Work in America." Pew Research Center, 20 Oct. 2021,
www.pewresearch.org/social-trends/2021/10/20/covid-19-pandemic-continues-to-reshape-work-in-america/

Russo, G., Marsigalia, B., Evangelista, F. et al. “Exploring regulations and scope of the Internet of Things in contemporary companies: a first literature analysis.” J Innov Entrep 4, 11. November 14, 2015.
https://doi.org/10.1186/s13731-015-0025-5

Segundo, El. “More companies using Bossware to monitor employees.” Inside The Issues. September 23, 2022.
https://spectrumnews1.com/ca/la-east/inside-the-issues/2022/09/23/more-companies-using--bossware--to-monitor-employees

Stanley, Jay. “Amazon Drivers Placed Under Robot Surveillance Microscope.” Aclu.org. March 23, 2021
https://www.aclu.org/news/privacy-technology/amazon-drivers-placed-under-robot-surveillance-microscope

Weik, Martin H. “The ENIAC Story” 1961
https://web.archive.org/web/20110814181522/http://ftp.arl.mil/~mike/comphist/eniac-story.html

Zickuhr, Kathryn. “Workplace surveillance is becoming the new normal for U.S. workers.” Equitablegrowth.org. August 18, 2021.
https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/