Creating Protocols for Spyware

Ashlyn Pope
Justin Fugiel
Sebastian Wagoner

Lake Forest College Public Policy Challenge 2023

Contents

I. Introduction

With COVID-19 in our near past and the increase in using online programs for work, employers are turning to different forms of surveillance including camera tracking and keyboard tracking to monitor their employee's activities. The goal of surveillance is to uphold employee accountability along with job productivity to make sure the employee is doing efficient work. While this holds potential benefits, this type of surveillance brings up important privacy, legal, and ethical questions about the balance between accountability and the employer's right to privacy.

80%

of major companies monitor the internet usage, phone and email of their employees. *(American Bar Association)*

II. Executive Summary

Working from home has allowed many Americans to conveniently support themselves and their families. As technology continuously progresses, this becomes more desirable. Particularly since the beginning of the COVID-19 pandemic, individuals heavily prefer working from the comfort of their home, perhaps alongside loved ones. This creates a more enjoyable environment compared to the discomforting office cubicle in which many Americans report to forty hours per week. Everyone has to earn their dollar, but recent times have proven the effectiveness of remote employment. Why not create a simpler life?

While the simplicity of remote work has proved wonderfully for many Americans, it has ruined others. Alongside progressive technology, employers have implemented strategies to ensure effective surveillance of employees. This includes, but is not limited to, access to personal information, search history, and even the camera. Employers may also implement keylogging software to measure productive work. This surveillance, often unauthorized, has actually made American workers more uncomfortable and unmotivated in their setting.

Creating Protocols for Spyware explains what is meant by "employee surveillance," including a definition of the controversial action. This paper concerns harm done to individual privacy, productivity, and well-being. Following is each the legislative, judicial, and regulatory approaches to combatting employee surveillance demonstrated visually. In

conclusion, a solution will be presented as to what should be done.

Employee surveillance comes in two forms, intrusive and non-intrusive. The former is an extreme version of this, highlighted by software that provides access to personal information. This information is undoubtedly at risk in the hands of the employer, who may utilize it however they please. Regardless of the type, each has proven to negatively affect worker productivity. Despite the goals of these actions, the typical result is actually distraction and anxiety. Because of this, a bill has risen in Congress and many states have taken matters into their own hands. However, the lines are often blurred as to what is and is not allowed.

Combatting employee surveillance requires serious regulatory measures. *Creating Protocols for Spyware* will lay these out. Invasive monitoring is not warranted in the workplace regardless of the reasoning. This surveillance, often unconsented, creates a discomforting environment for workers who are simply earning a living.

While invasive monitoring requires regulation, this paper will also present permitted, non-intrusive forms of monitoring. It is understood that employers are concerned with the level of productivity from their employees. *Creating Protocols for Spyware* will bridge this gap in order to create policy allowing for effective remote working in the United States.

III. What do we mean by employee surveillance?

Employee Surveillance

We believe there to be a place for an appropriate level of employee surveillance in the workplace. The main issue that arises is the invasion of privacy. Non-intrusive workplace surveillance includes tracking screen time, idle time, and keeping track of attendance. Even some more aggressive monitoring can be appropriate on workplace devices. For example, government employees or high-profile companies that handle sensitive information can and should use software to identify any concerning emails or phone calls via work devices. Unfortunately, the most common surveillance comes in the form of key stroke logging, screen recording, GPS tracking, and even biometric timekeeping (Mitchell 2022). While some companies choose to purchase and install bossware onto devices in the workplace, major providers like Google and Microsoft are now coming with bossware built in (Timmerman 2023). For example, Microsoft Teams, one of the most popular workplace sites, uses a status tracker to show the owner of the page how frequently they visit the page and if they are currently active or not.

Intrusive Surveillance

Bossware is on a spectrum and the more extreme forms become invasive and violate worker privacy. For example, keystrokes can be used to simply identify screentime and track amount of time working, but they can also log what keys are used and what words are typed (Timmerman 2023). An extreme example of intrusive bossware is camera and/or audio tracking. Built in cameras on work devices have been utilized to take images or videos of employees to ensure productivity.

IV. Detailed look at the harms, section by section

a. Legal

The legality of employee monitoring and surveillance is not at all black and white because of next to no federal or state regulations. As of current, the only states with legal protection for the employees regarding workplace surveillance are Connecticut, New York, and Delaware (cite). Outside of these states, the only regulations protecting the monitoring privacy of employees are regarding recording in private spaces such as restrooms and locker rooms (cite). Expanding the definition of these private spaces to simply, "outside the workplace" would allow for more protection for the employees.

Personal Data and Health Information
Since there are few regulations and legal measures protecting employees in this regard, employers get away with invading privacy. For example, employers do not have access to employee's health information under the protection of HIPAA (cite), with invasive screen monitoring and/or recording as a form of employee surveillance, employers can pick up private information and personal health data from employees. Since it is under the guise of workplace surveillance, this creates a legal grey area. Similarly, data like passwords and banking information are at risk of exposure.

Union Busting
According to the National Labor Relations Board (NLRB), "it is unlawful for an employer to interfere with, restrain, or coerce employees in the exercise of their rights", (NLRB). There are employers who are scanning employee emails, phone calls, and

other private conversations on workplace devices to look for signs of hostility or resentment, "Employers are charged with making threats, engaging in surveillance activities, or harassing workers in nearly a third of all union election campaigns," (McNicholas 2019). It is illegal to reprimand employees for these conversations but because of the underregulating of monitoring and surveillance, employers are getting away with it.

b. Productivity

Research continues to show time and time again that increased surveillance and monitoring does not fully benefit workplace productivity. Dr. Chase Thiel from the University of Wyoming conducted two studies to understand the effects of monitoring on employee behavior and productivity. What they found was that monitored employees were more likely to cheat on tasks, damage property, steal office equipment, work at a slow pace, and other poor behavior (Thiel 2022). An ExpressVPN survey shows that 38% of the 2,000 employees sampled feel more pressure to be online than doing actual productive work (ExpressVPN 2021). An explanation for this behavior is that, according to the study, employees who are monitored are more likely to blame their behavior on their supervisors where those who are not monitored take greater responsibility for their behavior (Thiel 2022). The results of the study concluded that when employees feel they are treated with fairness then they are less likely to act immorally and therefore are more productive (Thiel 2022). At the end of the day, moral, mental health, and attitude towards the supervisor plays a larger role in productivity than intense monitoring.

c. *Mental health and wellbeing*

Surveillance of employees is thought to increase anxiety in workers due to the worry that they might be caught doing something wrong even if they are exemplary workers. Anxiety can distract and lead to reduced job satisfaction and productivity. ExpressVPN conducted a survey of 2,000 remote and hybrid U.S. employees, revealing that 59% feel anxious about being monitored by their employers and 83% believing this to be an ethical concern (ExpressVPN 2021). From the research done by Dr. Thiel, an unhappy or anxious employee is less likely to produce good work due to the moral levels in the workplace and feelings toward supervisors (Thiel 2022).

V. What can be done/is being done to stop these harms?

a. Legislative approach

Moving forward with this solution, one step forward is to get a bill passed at the state level, specifically in Illinois. Using this SWOT analysis, we can conclude that this is a good step moving forward. Strengths for passing a bill with this solution at a state level would be that it may be easier to pass at a state level as well as Illinois being an influential state due to the financial impact a big city like Chicago has. Therefore if it was passed in Illinois, we would potentially be able to build traction to continue our solution further. Also, Senator Bob Casey is currently supporting an act called the "Stop Spying Bosses Act". (Stop Spying Bosses Act One Pager) This act outlines many similar ideas that we believe in. Continuing, as mentioned, an opportunity of passing this at a state level would allow the bill to be seen by other states and potentially allow for greater traction. A weakness of passing this at the state level is that besides the "Stop Spying Bosses Act" on a federal level, there is not much of a push for this specifically at the state level. A threat to our solutions is big corporations and big tech. Big tech and other bigger companies naturally look for surveillance and control over their employees to collect data and to understand how to improve their company. Limiting and controlling surveillance from these bigger corporations would be difficult because of their stance of influence and opposition. They will oppose and try to have our proposition not be passed.

b. Judicial approach

ACLU

A potential avenue for achieving better employee rights in terms of surveillance would be going through labor rights groups and unions in order to reach the courts. This can consist of a few different actions and lead to a variety of pathways. One possible route is to go through the American Civil Liberties Union. This could still be narrowed in even farther and specified to the state ACLU, like the Illinois ACLU. The ACLU can litigate cases where a person has their civil rights violated. In order for this method to be successful the ACLU would need to find people who have faced discrimination or scrutiny because they were being watched/listened to. For example, if someone was expressing workplace grievances over email to another employee and that email was being tracked and monitored by a supervisor and then the employee was apprehended for retaliation, the ACLU would be able to step in and consider this a free speech violation. It might be more successful to go through the Illinois ACLU rather than attempting to reach the national ACLU simply because of the volume of complaints the ACLU receives day to day. This avenue would require pretty specific situations where other groups that specialize in labor rights would reach a wider audience.

NLRB

The NLRB protects the rights of employees in the private sector, regardless of union status. This is important because majority of the established labor rights laws are hard to get through to private companies or organizations. The NLRB is where people can form or join a union as well, a good place to start if the workplace is unfair. The NLRB enforces the National Labor Relations Act (NLRA) which means if a citizen believes their rights have been violated, they can file a charge through the NLRB. Just recently, the General Counsel Jennifer Abruzzo released a memo regarding bossware and the violation of labor rights in terms of predatory employee surveillance. The memo suggests that the Board work to amend/adapt the NLRA to account for 'changing patterns of industrial life' as times are changing quickly with the new

capabilities of technology. Abruzzo mentions interference and potential violation of Section 7 and 8 of the NLRA which promises, "the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representations of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection". Section 8 solidifies that employers may not interfere, restrain, or coerce employees in regards to Section 7. Majority of Section 7 calls for protection of active union employees but can also be stretched to protect potential unions, much like the example earlier with workplace grievance conversations. Any specific language added to the NLRA and specifically Section 7 and 8 that would consider new technology, bossware, and surveillance of employees would provide better protection for employees and open the door for more employee complaints.

A strength for opting for change through independent agencies would be that these groups can apply pressure through lobbying as most are powerful and well-established groups. Lawsuits and complaints through these agencies can be a good shoo-in for entering the court system, especially with the legal resources these large groups have access to. In terms of weaknesses, it would be difficult to challenge companies and organizations that do not already have unionized employees or employees attempting to unionize. It is also definitely a slow process once the complaint gets to the courts. Most of the civil liberties groups prefer those complaints just be settled without the court's involvement, maybe preventing a vaster progress. Opportunities include potential amendments to the NLRA which would create national change and provide widespread rights to employees regardless of what state they work in. Any progress in the courts or with these civil liberties groups can serve as good backing for the Stop Spying Bosses Act as well. Unfortunately, success in this realm is limited by good lawyers and poorly specified laws. A different group but still in labor rights, the Equal Employment Opportunity Commission sees retaliation complaints more than anything but only 2% of complaints result in penalties. This is not a surefire

avenue but one to be considered and one that can help in gathering personal statements.

c. Regulatory approach

Another room for change is within the Illinois specific workers' rights amendment. The Illinois Workers' Rights Amendment essentially codifies Section 7 of the NLRA stating employees have the fundamental right to organize and bargain collectively. Adding language to consider the privacy of the employees would strengthen workers' rights in Illinois and lead the way for potential nationwide changes.

STOP SPYING BOSSES ACT OF 2023

U.S. Senators Bob Casey (D-PA), Cory Booker (D-NJ), and Brian Schatz (D-HI)

The Stop Spying Bosses Act of 2023 would:

- Require any employer engaging in surveillance and collecting data on employees or applicants to disclose such information in a timely and public manner;
- Prohibit employers from collecting sensitive data on workers (i.e., off-duty data collection, data collection that interferes with organizing, etc.);
- Create rules around the usage of automated decision systems to empower workers in employment decisions; and
- Establish the Privacy and Technology Division at the Department of Labor to enforce and regulate workplace surveillance as novel and emerging technologies.

Stop Spying Bosses Act is

- cosponsored by U.S. Senators John Fetterman (D-PA) and Elizabeth Warren (D-MA)
- supported by the Economic Policy Institute, National Employment Law Project, the Athena Coalition, the Communications Workers of America, the SEIU, and the AFL-CIO
- introduced to the senate and referred to the Committee on Health, Education, Labor, and Pensions

“American workers are like the backbone of our country, and they deserve to be treated with basic dignity at work.”

— **U.S. Senator Casey (D-PA)**

FROM THE STATES

Connecticut

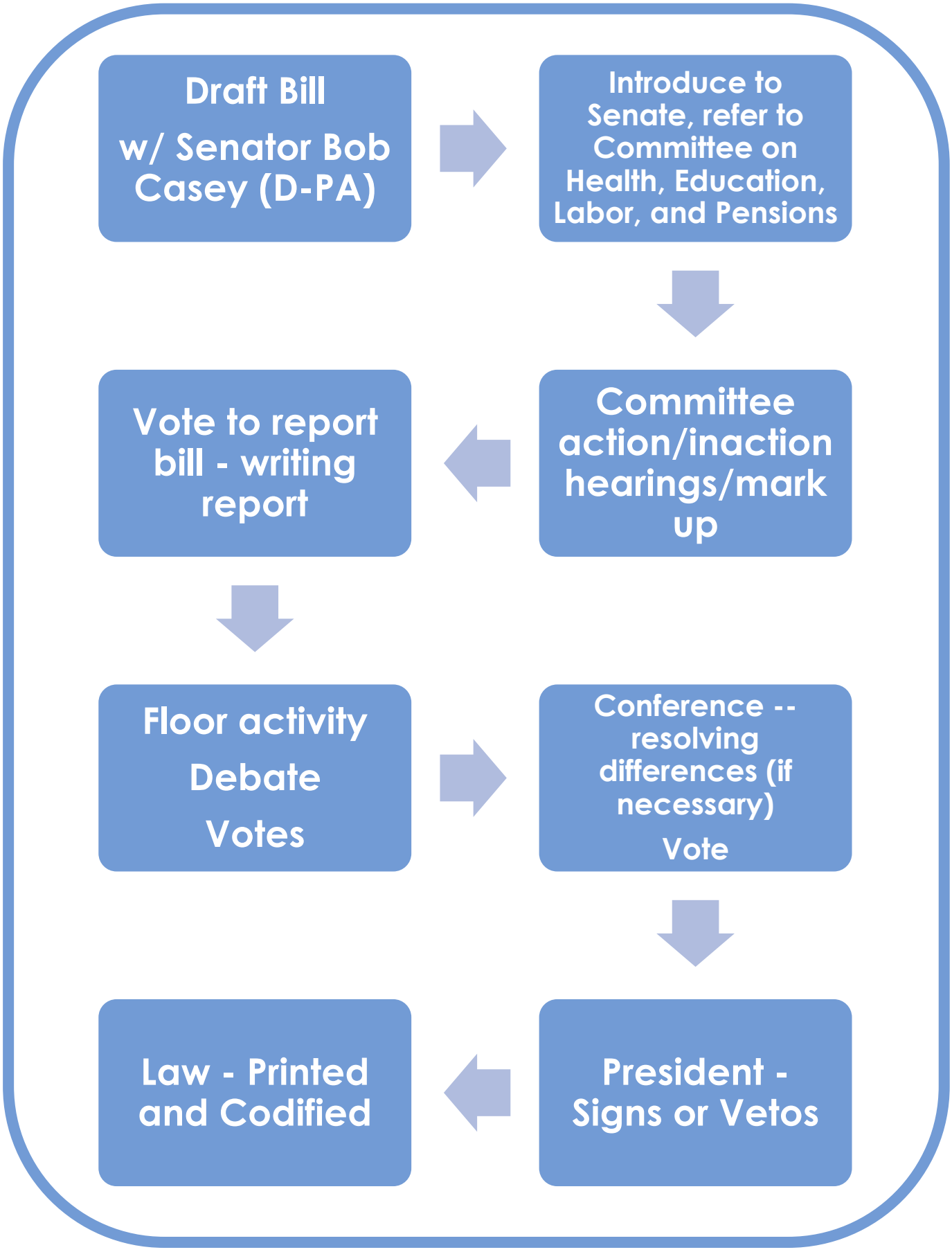
- employers engaged in electronic monitoring required to give prior written notice to employees
- CT Gen Stat Section 31-48d (2012)

New York

- Requires every private-sector employer to provide notice of its electronics monitoring practices to all employees up on hiring and in a "conspicuous place"
- New York Senate Bill S2628 (2021)

Delaware

- Notice of monitoring telephone transmissions, electronic mail and internet usage.
- monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer provided email or internet access services
- Del. Code tit. 19, Section 705 (2010)


Draft Bill
w/ Senator Bob Casey (D-PA)
Introduce to Senate, refer to Committee on Health, Education, Labor, and Pensions
Committee action/inaction hearings/mark up
Vote to report bill - writing report
Floor activity
Debate
Votes
Conference -- resolving differences (if necessary)
Vote
President - Signs or Vetos
Law - Printed and Codified

VI. What should be done? What is our plan?

Regulations surrounding workplace monitoring are either nonexistent or out of date – an amendment to an already proposed bill would protect both the workplace and the worker. Our proposal combines both new regulative measures as well as an amendment to already proposed federal legislation. With the Stop Spying Bosses act as our template, we would like to make it more specific to not allow for any loopholes. We would also pull from the state legislation and include fines as consequences for companies that are found guilty for not following regulation, Ideally, smaller businesses would have a lower fine based on their yearly intake.

Regulations:

- No camera or audio access, no access to keystrokes, no access to personal data UNLESS clearly disclosed and consented by employee. Any kind of monitoring must be disclosed in the application process.
- Permitted: non-invasive monitoring on work devices: can track the screen time, idle time, tracking attendance, mouse strokes, activity status
- Creating an agency to check businesses and companies – perform audits regularly and respond to employee concerns and complaints regarding surveillance under the dept. of labor.

VII. Conclusion

As technology continuously advances, many American workers will need to utilize it in order to secure employment. Perhaps they seek a more comfortable environment. While technology will not go away, neither will these powerful employers. *Creating Protocols for Spyware* outlines the necessary compromise. Otherwise, the problem of workplace surveillance will persist.

Remote American workers are vulnerable and subject to unnecessary surveillance under the guise of ensuring productivity. While this claim is valid, employees are often unaware they are monitored in such a way. This includes the collection of personal information, keylogging, and access to microphones and/or cameras.

This sharp increase in remote employment did not occur until the beginning of the COVID-19 pandemic. Since then, many Americans have either been forced or chosen to work remotely. Regardless, employers have powers capable of endangering these individuals. Unfortunately, there has been no legislation or regulation introduced to combat this growing issue.

Creating Protocols for Spyware lays out regulations necessary to help the problem of workplace surveillance. Employers will not be allowed to access camera and audio. Additionally, keylogging will not be allowed and access to any personal information must be consented by the employee. Non-invasive monitoring of any kind must be disclosed to the employee. Employers, however, will be allowed to track screen time, idle time, mouse strokes, activity status, and record attendance. Additionally, proposed is a committee that will perform regular auditing to ensure company cooperation. The committee shall also respond to employee concerns.

These regulations will ultimately combat the issue of intrusive workplace surveillance. This team is eager to work hard in order to help.

Citations

"CleverControl." *Microphone Sound Recordings*, https://web.archive.org/web/20201206004528/https://clevercontrol.com/microphone-sound-recordings.

Cyphers, Bennett, and Karen Gullo. "Inside the Invasive, Secretive 'Bossware' Tracking Workers." *Electronic Frontier Foundation*, 13 June 2022, https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers.

Hunter, Tatum. "Here Are All the Ways Your Boss Can Legally Monitor You." *The Washington Post*, WP Company, 4 Oct. 2021, https://www.washingtonpost.com/technology/2021/08/20/work-from-home-computer-monitoring/.

West, Darrell M. "How Employers Use Technology to Surveil Employees." *Brookings*, Brookings, 9 Mar. 2022, https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/.

Zarook, Ruqaiyah. "Senate Democrats Are Taking Companies to Task over Invasive Workplace Surveillance." *Mother Jones*, 7 Feb. 2023, https://www.motherjones.com/politics/2023/02/workplace-surveillance-stop-spying-bosses-act/.

"Advantages and Disadvantages of Monitoring Employees." *Business.com*, https://www.business.com/articles/pros-and-cons-of-monitoring-employees/.

"Casey, Booker, Schatz Introduce Bill to Protect Workers from Invasive, Exploitative Surveillance Technologies: U.S. Senator for Pennsylvania." *Senator Bob Casey*, 2 Feb. 2023, https://www.casey.senate.gov/news/releases/casey-booker-schatz-introduce-bill-to-protect-workers-from-invasive-exploitative-surveillance-technologies.

"ExpressVPN Survey Shows Widespread Surveillance on Remote Workers." *Home of Internet Privacy*, 1 Dec. 2021, https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce/#mental.

"How Much Employee Monitoring Is Too Much?" *Americanbar.org*, https://www.americanbar.org/news/abanews/publications/youraba/2018/january-2018/how-much-employee-monitoring-is-too-much-/.

McNicholas, Celine. "Unlawful: U.S. Employers Are Charged with Violating Federal Law in 41.5% of All Union Election Campaigns." *Economic Policy Institute*, https://www.epi.org/publication/unlawful-employer-opposition-to-union-election-campaigns/.

Thiel, Chase. "Monitoring Employees Makes Them More Likely to Break Rules." *Harvard Business Review*, 27 June 2022, https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules.