CENTER FOR DEMOCRACY & TECHNOLOGY

Workplace Privacy: State Legislation & Future Technology Questions

Ali Lange, Katie McInnis, & Michelle De Mooy
Center for Democracy & Technology
June 1, 2016

Introduction

Digital technology has fundamentally and forever changed the way we share information about ourselves. New formats like Instagram, Twitter, and Facebook create opportunities to instantaneously share our experiences and create community, but they can also blur the boundaries between our private and public lives by creating digital records that can be aggregated, copied, shared, or otherwise disseminated and taken out of context. This has raised many complicated questions about the definition of privacy generally, and it has diminished our ability to keep separate personas at work and at home, "IRL"[1] versus online. The boundaries between work and home have been further muddled by incentives for employers to monitor employee health, a growing culture of Bring-Your-Own-Device (BYOD) workplaces, and affordable innovations in monitoring and tracking technology. This creates a need for us to define what it means to have privacy in the relationship between employers and their employees, and to create a culture of workplace privacy, which state legislators are now attempting to do.

Creating a regulatory framework for employee privacy that sufficiently addresses the variety of workplace settings equitably and comprehensively is a difficult task. Businesses face complex risks as a result of employee behavior—from monetary losses to legal liability—and technological monitoring is a tempting way to mitigate some of these risks. In addition to the tremendous variety of business practices and workplace cultures, some businesses have legal reporting requirements that necessitate the monitoring of employee communications.[2]

[1] Internet slang for 'In Real Life.'

[2] Financial institutions involved in selling securities are required to keep records of employees phone calls and emails in order to be responsive to fraud investigations. The Financial Industry Regulatory Authority (FINRA) prescribes procedures (approved by the Securities & Exchange Commission) for this recordkeeping: "incoming and outgoing written (including electronic) correspondence to properly identify and handle in accordance with firm procedures, customer complaints, instructions, funds and securities, and communications that are of a subject matter that require review under FINRA rules and federal securities laws." FINRA Manual. *3110. Supervision.*

But workplace privacy protections can benefit both individuals and employers. The freedom to have private lives outside of work and private thoughts at work is critical to supporting a creative and diverse workforce built on respect for individual dignity. There are clear risks for employees if their employer learns private, sensitive information, including termination or other forms of retaliation. Sensitive information in this context includes anything about the employee's health, job search, plans to unionize, or attempts at whistleblowing. But there are risks to employers in learning this information as well. For example, if an employer learns an employee's religious affiliation and subsequently fires them, the employee might be able to claim their termination was the result of discrimination. And privacy in the workplace plays a bigger role than protecting against these relatively straightforward harms. Workplace privacy protections grant employees the freedom to ruminate on new ideas, to act without second guessing their decisions, and to solve problems in diverse ways. This can contribute to the health of an organization and encourage innovation.

The benefits and risks of employee privacy have been recognized by policymakers working to re-establish boundaries. With limited guidance in federal law, state legislatures and interested stakeholders have begun to propose and institute legislation regarding employee rights in the workplace. These proposed pieces of legislation have some promise for improving the state of employee privacy, but the dynamic nature of technology requires flexible and creative solutions from employers and technology companies.

This paper first describes the current legal landscape of employee privacy at the state level, followed by a synopsis of three efforts to create a unified state law. We then use three case studies of workplace technology trends to demonstrate the privacy risks posed by current and future technology, and examine how the current proposals fall short. Finally, we propose methods to mitigate some of these threats through policy, innovation, and legal expectations.

Current State Law and Proposals

Adoption of new workplace technology has not been accompanied by corresponding protections for employee privacy. Employers can request access to personal accounts and devices, even to those not associated with work or the real identity of the employee, without facing legal consequences. They can essentially monitor and track any behavior on-site and sometimes keep monitoring while employees are off the clock. However, states have started to

http://finra.complinet.com/en/display/display_main.html?rbid=2403&element_id=11345 (last accessed May 16, 2016).

address the inherent imbalance accentuated by technology by codifying privacy protections for employees.

Some states have already passed laws concerning employee privacy. California, Colorado, Connecticut, New York, and North Dakota prohibit the discipline of employees for off-duty activity on social networking sites, unless the activity damages the company in some way.[3] Twenty-two states[4] have laws protecting employees or job applicants from employers who require them to provide a password or username to personal social media accounts.[5] Connecticut, Delaware, and Rhode Island[6] recently signed different versions of the same model legislation published by American Legislative Exchange Council (ALEC)[7] in 2013. Many states, including Colorado, Connecticut, Delaware, and Tennessee[8] have laws requiring employers to create a policy on the monitoring of employee access times and usage of electronic devices, as well as detailing any intercept of employee electronic communications.

These laws protect employees by prohibiting the discipline of an employee for social media posts that are unrelated to work, prohibiting coerced access to employees' personal social media accounts, and requiring employers to institute an employee-monitoring policy. Other states have proposed legislation to increase employees' legal rights to privacy where the federal government does not provide protection.[9] These proposals are largely based on model legislation authored by external bodies, if not entirely drawn from them. The bills are narrowly

[3] Generally, if the off-work social media activity is related to work it can be found damaging to the company. However, certain forms of communication cannot be prohibited by a workplace social media policy. For instance, discussion of working conditions or wages among employees is protected by federal law. *Workplace Privacy and Employee Monitoring*, Privacy Rights Clearinghouse (Oct. 2015), https://www.privacyrights.org/workplace-privacy-and-employee-monitoring.

[4] Arkansas, California, Colorado, Connecticut, Delaware, Illinois, Louisiana, Maryland, Michigan, Montana, Nevada, New Hampshire, New Jersey, New Mexico (applies only to job applicants), Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Virginia, Washington, and Wisconsin. *State Laws About Social Media Privacy*, Nat'l Conf. of State Legislatures (June 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.

[5] *Workplace Privacy and Employee Monitoring*, Privacy Rights Clearinghouse (Oct. 2015), https://www.privacyrights.org/workplace-privacy-and-employee-monitoring.

[6] 2015 Conn. Acts 15-6 (Reg. Sess), Del. Code §19-7-709A (2016), R.I. Gen. Laws § 28-56-1 to -6.

[7] Employee Online Privacy Act – as amended, Amer. Legislative Exchange Council (Aug. 5, 2013), http://www.alec.org/model-legislation/employee-online-privacy-act/.

[8] Colo. Rev. Stat. §24-72-204.5 (2015), Conn. Gen. Stat. § 31-48d (2015), Del. Code §19-7-705 (2016), Tenn. Code §10-7-512 (2016).

[9] *Access to Social Media Usernames and Passwords*, National Conference of State Legislatures (Feb. 2, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

crafted, responding largely to reports of employers asking employees or applicants to provide login credentials (username and password) for their online accounts, but more is needed to create a culture of workplace privacy. Asking for login information is a clear violation of employee privacy and a natural starting point for establishing workplace norms. That said, the vast majority of employment applications currently do not request this information, and very few employers report that they would ask their employees for social networking or other personal online account details.[10] Even in reported cases, the employer typically accessed social media content via a third party connected to their employee, not by compelling direct access.[11]

Proposed Legislation and CDT's Workshop

Several institutions are writing model bills to unify state law nationwide and provide employees with some statutory privacy protections. The Uniform Law Commission (ULC),[12] the American Civil Liberties Union (ACLU),[13] and the State Privacy and Security Coalition each drafted models that represent their point of view on how to navigate some employee privacy issues.[14]

While all three models are focused on establishing statutory privacy protections for employees, there are variations in the details as a result of the interests and approach of each group. First, the ULC drafting committee tends to consider a broad range of stakeholder input, motivated by the desire of members to produce legislation that is responsive both to existing legal precedent and the current cultural climate. The legislation produced by this committee process is typically very detailed and technical, as far as model laws go. In this case, the model produced by the ULC (which is not yet in its final format) attempts to balance business interests while establishing concrete employee privacy protections. In comparison, the State Privacy and Security Coalition is more narrowly focused and, in general, represents the view of its member

[10] Brittany Dancel, *The Password Requirement: State Legislation and Social Media Access*, 9 FIU L. Rev. 119, 154 n. 170 (2013), http://ecollections.law.fiu.edu/lawreview/vol9/iss1/31/.
[11] *Id.* at 125 n. 41, 126.
[12] National Conference of Commissioners on Uniform State Laws, *Employee And Student Online Privacy Protection Act*, February 26-27, 2016 Drafting Committee Meeting Redline Draft (most current draft as of writing), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016FEB_ESOPPA_Mtg%20draft_Redline.pdf.
[13] American Civil Liberties Union, *Employee User Name and Password Privacy Protection Model Bill*, https://www.aclu.org/legal-document/employee-social-media-passwords-bill (last accessed Apr. 10, 2016).
[14] Uniform Law Commission, *February 2016 Committee Meeting - Comparison Chart*, (Feb. 23, 2016), http://www.uniformlaws.org/shared/docs/social%20media%20privacy/2016feb23_ESOPPA_Comparison%20Chart.pdf.

companies.[15] In particular, workplace privacy questions implicate social media companies, which are largely caught in the middle of wanting to provide opportunities for individuals to connect and network without their services being used to coerce access to private information. Finally, and relatedly, the ACLU model is focused on employee social media privacy specifically. The ACLU's reputation as a staunch advocate for the privacy and constitutional rights of individuals is reflected in their model's strong positions and framework, which proposes, for example, equal privacy protections to domestic employees.[16]

CDT invited representatives of each institution to a workshop that convened a broad group of stakeholders, including representatives from the Employee Equal Opportunity Commission, the National Consumers League, the AFL-CIO, and employment attorneys. The group gathered in an effort to discuss and standardize the protections afforded to employees in these models. Workshop participants discussed both the privacy expectations of employees and the needs of employers to protect their brand as well as ensure internal security. The diversity of situations, tools, and products relevant to the discussion (even before attempting to anticipate future technologies) speaks to the difficulty of writing legislation to address all possible workplace environments. However, most participants agreed that the following were the most important questions in writing legislation:

- What kinds of access do employers need to reasonably protect their proprietary interests and mitigate legal liability for employee actions conducted through business property?

[15] Comments filed with the National Telecommunications and Information Administration in 2010 state: "State Privacy & Security Coalition ("the State Coalition") members include a broad cross-section of the US technology and media industries – companies and trade associations who are vitally concerned with barriers to innovation posed by conflicting state privacy, security and e-commerce regulation: Amazon.com, AOL, AT&T, Cisco, Comcast, HP/EDS, Facebook, Fox Interactive, Google, Monster.com, Reed Elsevier, Skype, TimeWarner Cable, Verizon, and Yahoo!, the Entertainment Software Association, Internet Alliance, the NAi, NetChoice, Technology Association of America, and TechNet." National Telecommunications and Information Administration US Department of Commerce, *Comments of the State Privacy & Security Coalition on Information Privacy and Innovation in the Internet Economy*, 2 (June 16, 2010), https://www.ntia.doc.gov/files/ntia/comments/100402174-0175-01/attachments/State%20Privacy%20Security%20Coalition%20Comments.pdf.

[16] While the original ULC model specifically excepted this group, the ACLU successfully advocated at the February 2016 drafting meeting for the committee to modify their model's language and the current ULC draft now protects this class of employees as well.

- How should access be defined? For example, does an employer have a right to request to see the complete contents of a personal account as part of an investigation, or should they be limited by their capability to define specifically relevant pieces of content?
- What interests do businesses have in accessing content of devices or accounts that they support, monetarily or technically?

Workshop participants had a lively discussion of what level of employer access should be afforded through legislation. The legislative models are each premised on codifying broad employee privacy protections, defining exceptions to privacy protections rather than providing extensive access by default.[17] As a result, the drafts necessarily implicate the interests and expectations of employers, beginning with defined legal requirements for employers in some sectors to monitor their employees' activities, in order to carve out exceptions for these activities.

The group agreed that any burden on employees to maintain a complete separation of work and personal correspondence, connections, or even devices would be unrealistic. Alternative proposals included creating a technical mechanism that divides employee work and personal content, considering who pays for or otherwise sponsors an account, and requiring that an employer's request for access be limited to a narrowly described piece of information, such as an email sent within a particular time period.

The group additionally debated whether the rules should provide employers with one-time or ongoing access. While the ULC and industry models provide exceptions that allow employers to access content of an employee account under some circumstances, the ACLU takes a more protectionist stance by allowing only requests that ask "to share specific content that has been reported to the employer, without requesting or requiring an employee or applicant to provide a username ... password, or other means of authentication that provides access to a personal social media account."[18]

[17] All the models allow narrow exceptions for employers to gain access to their employee's personal online accounts, though the question of what constitutes a personal account varies. "Both [the ULC model] and the Industry model define a personal account in terms of requiring log-in credentials. The ACLU model does not address log-in credentials. It also applies more narrowly to social media accounts involving certain user-generated content." Uniform Law Commission, *supra* note 14 at 4.

[18] *Id*. at 13.

In CDT's view, a framework based on real world situations can be helpful in answering these questions, making a distinction between *situational* and *ongoing* access questions in particular. Situational access is one-time and should be in response to a specific investigation involving bullying, harassment, fraud, misuse of company technology and information, or similar scenarios where an employee's action could incur employer's liability. On the other hand, an employer may have legitimate interests in ongoing monitoring of activity on a personal account or device that is directly affiliated with the employer or business activities (described in the model legislative language as "sponsored by," "provided by," or "created by"). For example, an employer who pays for an employee to upgrade their personal LinkedIn account to the Premium version might subsequently request to see the messages and connections made through this account. Despite the legitimate business needs that evoke monitoring, ongoing access to personal information poses tremendous privacy concerns. CDT believes that a general framework around situational and ongoing access adds important nuance to the debate around appropriate levels of access based on business needs and individual privacy.

Bringing together these three institutions while they were drafting their models helped unify their policy positions, though they still have important differences. The discussion is ongoing and will continue throughout the state legislative process in the coming legislative seasons.

These model bills, and the debate hosted by CDT, demonstrate the potential power and limitations of using legal regulatory efforts to establish employee privacy protections. This perspective informs the policy recommendations CDT makes in response to the case studies we highlight and examine in the next section.

Technology Trends in the Workplace

Proposed model legislation focuses on the most egregious and familiar privacy violations, but technology moves fast and some policy decisions have accelerated the degradation of boundaries between employees and employers. While the legal debate continues to unfold, employees continue to experience the increasing possibility of being watched, quantified, and/or ranked by technology in their workplaces.[19] The following three case studies highlight key privacy risks and challenges that point to larger concerns with current workplace technology trends. For each case, we have described the technology being used, explained the

[19] Don Peck, *They're Watching You at Work*, THE ATLANTIC (Dec. 2013), http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

interests of employers and employees in its deployment, and concluded with a discussion of CDT's proposed policy recommendations.

Employee Wellness Programs (EWP) and Wearables

Many employers have added or expanded employee wellness programs (EWP) in response to regulations in the Affordable Care Act (ACA). The ACA allows employers to provide financial incentives to employees who participate in an EWP, in part because Congress, the White House, and many employers believe that these programs encourage a healthy lifestyle and reduce overall healthcare costs. Setting aside the question of whether these programs are effective,[20] one result of their use is the creation of a health data pipeline between employers and employees that was previously restricted by other regulations (primarily the Americans with Disabilities Act (ADA) and the Genetic Information Nondiscrimination Act (GINA)).

The underlying goal for many workplaces that participate in wellness programs is the reduction of skyrocketing healthcare costs through preventative care. Wellness programs create a perverse incentive to penalize individuals whose data suggests that they are in a health risk category that may incur costs to the company. Employers are able to access health information about employees in aggregate since many programs require participants to fill out a detailed health risk assessment or undergo genomic testing. Those who refuse may incur large increases on their yearly premiums.[21] This shifts the cost of care onto the shoulders of employees, rather than representing a true cost savings.

Wellness programs are increasingly using fitness tracking devices ("wearables") to monitor and report employee health metrics like the number of steps a person has taken or their heart rate. Wearable devices come with some legal concerns for employers, including accusations of spying if the device has a recording function that is not turned off when the employee is off the clock.[22] Employees are typically asked to provide information from their job-issued activity trackers as a part of an EWP. Data from wearables can reveal incredibly sensitive health information, including pregnancy[23] and emotional distress,[24] which can be used to infer

[20] Al Lewis, *10 Most Dangerous Wellness Programs*, Insurance Thought Leadership (Jan. 19, 2016), http://insurancethoughtleadership.com/10-most-dangerous-wellness-programs/.
[21] *2014 Employer Health Benefits Survey*, Kaiser Family Foundation (Sept. 10, 2014), http://kff.org/report-section/ehbs-2014-summary-of-findings/.
[22] Patience Haggin, *As Wearables in Workplace Spread, So Do Legal Concerns*, Wall Street Journal (Mar. 13, 2016), http://www.wsj.com/articles/as-wearables-in-workplace-spread-so-do-legal-concerns-1457921550.
[23] Mary Brophy Marcus, *Fitbit fitness tracker detects woman's pregnancy*, CBS News (Feb. 9, 2016), http://www.cbsnews.com/news/fitbit-fitness-tracker-tells-woman-shes-pregnant/.

diagnoses, treatments, and future health issues. The Health Information Privacy and Accountability Act (HIPAA) protects health information that flows to and from "covered entities," which includes healthcare providers, health insurance exchanges, and health insurance plans, as well as the business associates of these entities. Unless an employer deploys a wellness program through their existing health insurance plan, any health data collected, used, or shared through the EWP would not be covered by HIPAA. For example, if an employer administers a wellness program through a third party vendor, though the vendor is beholden to some of the ACA's guidelines, most of the data sharing practices are governed solely by the vendor's privacy policy.

Tracking devices are also being used in workplaces outside of employee wellness programs. For example, insurance giant Aetna gives its employees Fitbits to track their sleep; if they average seven or more hours of sleep a night for 20 days, they are given monetary rewards of up to $300. The company claims that this focus on sleep has improved their health of their workforce, with the underlying force behind this program being the increase in productivity and profit. While the concept of a business experimenting with ways to maximize its profit is nothing new, collecting and using employee biometrics to achieve this aim certainly is.

CDT Policy Recommendation

The temptation for employers and wellness vendors to broadly collect vast amounts of employee health data (including electronic health records, which may include genetic testing information) without a clear and immediate purpose should be mitigated through formal policies and practices.

As more companies participate in wellness and other biometric-related programs, a growing body of commercial vendors is collecting more and more health and lifestyle data about individuals. This puts employers directly in a position to make significant public policy decisions. As they decide which vendors to work with, employers should require that wellness programs and other vendors that they contract with are in compliance with the full set of protections offered by HIPAA's Privacy and Security Rule, including: clear and actionable notice requirements, the ability to obtain copies of all personal information collected as part of the program, the ability to challenge completeness and accuracy of such information, the right to obtain a listing of all parties to whom such information was disclosed, robust security protocols

including de-identification standards, and the ability to request confidential communication with providers. Employers should require that these protections cover all health information and wellness data, including genetic information, data collected via fitness trackers and mobile apps, and data about the level of individual's participation in a wellness or other lifestyle program. Legislators, unions, or others representing the interests of employees should also demand that data generated by wellness program be afforded HIPAA-like protections.

Additionally, state lawmakers may reconsider the nature of the incentive structure that employees face when deciding whether or not to participate in an EWP. Specifically, CDT is concerned that under current ACA guidelines these programs are not truly voluntary because they can include significant financial repercussions for failure to participate. Requiring employees to "voluntarily" pay hundreds or thousands of dollars more for their health coverage does not represent real choice.

Some of these policy issues are being considered at the federal level, a process that might guide state legislators. For example, the Equal Employment Opportunity Commission's (EEOC) has proposed amendments to the Genetic Information Nondiscrimination Act of 2008 (GINA) as it relates to employer wellness programs. CDT believes collection of genetic information by wellness programs should be restricted to only the minimum necessary needed for these activities. Specifically, employees would benefit substantially if the definition of "wellness program" were changed from one "reasonably designed to promote health or prevent disease" to one that requires scientifically valid evidence that the data collected can be used to diagnose or prevent a specific disease or condition.

The proliferation of direct-to-consumer testing, along with government programs like the Precision Medicine Initiative, will create larger and more diverse streams of data containing genomic information. State lawmakers could consider prohibiting workplace wellness programs from accessing and appending genetic information from other sources, such as patient claims data and medical records data, as well as the sale of genetic data and of genetic data bundled with other health data, even if the the information is de-identified. For the public to trust commercial and government actors collecting their most sensitive and intrinsically personal data, these streams must be segmented and tightly controlled.

Finally, wearable device accounts should be included under the definition of a "personal account" in state model legislation. Regulatory agencies like the Federal Trade Commission and the Food and Drug Administration have mostly taken a hands-off approach to health and

wellness apps and devices, therefore the passage of state laws designed to protect personal accounts may be the most expedient path to protecting employee privacy in this context.

Bring-Your-Own-Device (BYOD) Workplaces and Dual-Purpose Accounts

The ubiquity of personal devices and efforts to reduce business costs has led some employers to conscript employee phones, tablets, and laptops into professional use. While it used to be common to have a separate phone for work, many individuals now have one device that serves multiple purposes, sometimes causing new complications in the employer-employee relationship. This is particularly interesting in the legislative context as some model bills include exceptions for devices or accounts that are paid for by the employer, even in part. Many mobile BYOD devices fall under this exception—for example, in the case of phone plans, an employer will sometimes offer a monthly stipend to offset costs of conducting business through a personal plan, giving the employer a small financial stake in the use of the phone.[25] While, sharing devices is often simpler for employees as well as more economical for employers, if employers do not allow for employees to use an employer-provided or otherwise separate device from their primary personal device, this could create significant privacy risks.

The same logic could apply to personal accounts, which can also be legitimately utilized for business purposes in some contexts. Sometimes an employee's personal social networking account can become the face of the business they represent. For example, employers might pay for an upgrade to a LinkedIn Premium account for the purpose of supporting an in-house recruiter's efforts to find talent for the company. In these cases, the employer has a formal stake in the employee's account, and might subsequently expect access on an ongoing basis. Much of the existing legal precedent relies on the idea that an institution owns the tools and devices used for work-related communication, providing a natural argument that the business conducted using those tools is subject to review by the employer.

Cost- and risk-shifting to employees through Bring-Your-Own-Device (BYOD) policies may serve both business and employee interests in some contexts, but it may also compromise the privacy of personal online accounts and personal devices. Personal computers and phones contain tremendous amounts of sensitive personal information, much of which is irrelevant to an employer. The number of communications an individual might conduct through a personal cell

[25] Some legislative language includes an exception that allows employers to access device stored on devices that are paid for 'in whole or in part' by the employer. *See e.g.*, American Legislative Exchange Council, *Employee Online Privacy Act* (approved by ALEC Board of Directors Aug. 5, 2013), https://www.alec.org/model-policy/employee-online-privacy-act/.

phone on a daily basis—including phone calls, texts, emails, photographs, social media posts, grocery lists, banking information, and health information—offers some perspective on the significant risk to an individual's privacy if an employer were able to access all of this content.

Employee use of personal accounts in performing professional duties creates additional unique challenges to privacy, particularly if employees simultaneously use these accounts for personal purposes. While any single account will contain less personal information than an entire device, this might be some of the most sensitive information when it comes to employee privacy. For example, an employee may use a personal account for communications related to job searching. Employers who have access to such communications might retaliate against employees who are actively seeking new employment, putting employees at risk of either losing their job or missing out on using a productive tool to help identify new positions. Additionally, even when employers aren't directly involved with the employee's conduct on a social networking site, they sometimes request that employees endorse, share, or otherwise promote content on behalf of the employer. While this may not, perhaps, pose a risk to privacy per se (assuming that the employer does not force an employee to reveal pseudonymous accounts), it can create significant tensions between employer and employee around the employee's own speech. If endorsing or promoting the employer's content through an employee's personal social media account is a key responsibility of a particular role, employers should make this clear, up front, in the job description. Generally, employees should be able to preserve their personal accounts for the expression of their own thoughts, ideas, and opinions and should not be compelled to express the views of their employers.

CDT Policy Recommendation

Increased privacy for employees should accompany the benefits to employers of BYOD policies. Or, at least these policies should not undermine the sovereignty of personal data and accounts on an employee's device.

These situations would be difficult to address through specific legislative requirements due to the diversity of scenarios that arise. However, at a minimum, legislation should require employers who are planning to recruit personal property or accounts to have a policy that states boundaries and expectations for both parties. This policy should be known to applicants and employees, and be binding for both parties, making it a versatile policy tool by giving the employee some options if their privacy is violated without requiring legislators to describe a one-size-fits-all solution. Employers could consider these policies a selling point to attract top

talent (as well as establishing values-based workplace norms) by creating clear and protective guidelines for employee privacy. At a minimum, BYOD policies should incorporate Fair Information Practice Principles, such as data minimization and purpose specification, requiring that data collected and used on an employee's device be limited to the minimum amount necessary, and subject to a specified purpose. Policies should also be bounded by a defined length of time (for example, the duration for which the company pays for an employee's service or device or limited to the amount of time the professional relationship exists), and access should be limited to reasonable work hours so that the employee is able to use their personal account, device, or other technology for personal purposes off the clock.

Although legislation can provide some solutions, many technology companies who build these products can and should directly provide tools and settings to help individuals protect their privacy. For example, LinkedIn is aware that their users are often using a personal account for professional or business reasons but also may want to conduct a job search. LinkedIn has a number of features and recommendations that individuals can take advantage of to preserve their privacy.[26] This type of innovation is a great example of privacy-preserving technology that respects the dignity of users while promoting business interests. This example demonstrates a best practice for companies who are building technology that could inadvertently compromise employee privacy.

Finally, there are technical solutions that allow for data to be segregated within a particular device such that it allows business-related data to be maintained separately within a personal device (referred to as a segregated data container).[27] This has benefits for both parties; employers can ensure that the data related to their business interests is secure and encrypted, and employees have some assurance that the employer does not capture their personal lives.

Emerging Employee Surveillance Technologies

Predictive analytics and wearable sensors are the frontier of employee surveillance technology. New technologies allow employers to observe and record employees' behavior in real-time and analyze data in order to draw inferences not only about their current and future productivity, but also about personality traits and soft skills like leadership. Examples of these new and emerging technologies include RFID tracking in ID badges that enables the tracking of office

[26] Lindsey Pollak, *The Stealth Job Search: How to Job Hunt Privately on LinkedIn*, LinkedIn Official Blog (Sept. 19, 2013), http://blog.linkedin.com/2013/09/19/the-stealth-job-search-how-to-job-hunt-privately-on-linkedin/.

[27] *See e.g.*, Check Point Capsule Workspace, https://www.checkpoint.com/products/capsule-workspace/ (last accessed May 4, 2016).

interactions among employees[28] and sensors sewn into clothing that measure and track motions.[29] Some new technologies use traditional data to power new software that makes predictions about employees, such as which employees are about to leave a job.[30] The metrics revealed from these methods of tracking and prediction have no analog comparison, and it is not clear exactly what new privacy concerns they may introduce to the workplace.

Monitoring the physical behavior of employees creates similar privacy risks to wearable health devices (for example, potentially revealing a disability), but some of the technologies could also alter the course of business by chilling interactions among employees. For example, Humanyze Workplace Solutions tracks employee movement and interaction through small chips in their ID cards. The idea is to analyze social interactions with an eye toward understanding, "if your top performers act differently."[31] The attempt to create an objective measure of leadership has the potential to benefit traditionally under-promoted populations. Perhaps this data could unseat stereotypes of male and female leadership styles and result in more women being promoted.[32] This would be a good outcome, but there are other ways to achieve this end that pose fewer privacy risks. This type of monitoring will cause employees to attempt to game the system, most likely further marginalizing any employee not already in the mainstream of the organization's culture. Knowing that the boss can observe your interactions alters, and likely chills, workplace interactions. Individuals will carefully consider with whom to interact, for how long, and even where in the office they should schedule their meetings to optimize their scores.

---

[28] Sociometic Bages, MIT Media Library (June 2011), http://hd.media.mit.edu/badges/. ID badges that include RFID chips, allowing employers to track interactions between employees.

[29] "Other early adopters of this type of physiolytics have been in health care, the military and the industrial sector. They use tracking not just to increase productivity but also for health and personal safety, and they have gotten a better reception among workers." H. James Wilson, *Wearables in the workplace*, The Hindu (Oct. 2, 2013), http://www.thehindu.com/todays-paper/tp-features/tp-opportunities/wearables-in-the-workplace/article5191022.ece.

[30] "VoloMetrix Inc., which examines HR data as well as anonymized employee email and calendar data, found that it could predict flight risk up to a year in advance for employees who were spending less time interacting with certain colleagues or attending events beyond required meetings." Rachel Emma Silverman and Nikki Waller, *The Algorithm That Tells the Boss Who Might Quit*, Wall Street Journal (Mar. 13, 2015), http://www.wsj.com/articles/the-algorithm-that-tells-the-boss-who-might-quit-1426287935.

[31] Humanyze, http://www.humanyze.com/index.html (last accessed April 11, 2016). "Visualize your team's engagement and cohesion communication network diagrams. Understand if your top performers act differently or if you have knowledge experts controlling communication flow in your organization."

[32] A study by Catalyst confirms that, "despite the numerous business contributions of women leaders, men are still largely seen as the leaders by default...As 'atypical leaders,' women are often perceived as going against the norms of leadership or those of femininity."
Catalyst, *The Double-Bind Dilemma for Women in Leadership: Damned if You Do, Doomed if You Don't* (2007).

Businesses using this technology must take care not to further amplify and entrench existing biases that have caused inequality in the workplace.

Replicating success is a popular motivation for using predictive analytics, raising serious diversity and discrimination concerns. Monitoring allows companies to observe the qualities that make one individual successful so that when you are hiring you can screen for these same qualities. It is essentially creating a formula for a successful employee based on past performance that can be replicated in the hiring process. While this idea has superficial appeal, it can also create major problems. It is a bad business practice to essentially freeze your definition of 'talent' based on the historic traits that have helped employees succeed in a particular venture. Not only does it forestall innovation, it may also hinder the larger objective of creating a diverse workplace and unintentionally encourage discrimination in hiring by disfavoring diverse employees who may not have the same qualities on paper as the group of currently successful employees, but who could individually succeed at a particular business setting.

Finally, the collection and use of this data moves past traditional measures of employee performance, like output, toward less empirical data analytics and inferences, like state of mind. These technologies can also be used to protect important business assets by predicting who will steal proprietary information. This kind of monitoring may take an emotional toll on employees and potentially exposes them to an opaque system of interpretation by their employers. Additionally, some have argued that, "continuous or unpredictable surveillance tends to lead to 'more negative attitudes on the job and towards the organization'...research also suggests that close monitoring leads employees to report more stress and feel they have no control organising their workloads."[33] This calls into question the value of these technologies, and whether the insights they reveal are worth the costs to overall job satisfaction.

CDT Policy Recommendation

Legislation should require that employers disclose any type of passive monitoring in a policy that is affirmatively agreed to by both employer and employee, and that is disclosed to applicants. This protection allows individuals the dignity of having enough information to leave a workplace that does not meet their privacy needs. However, even this basic recommendation

[33] Nicole Kobie, *Big Brother Boss: The Psychological Weight of Workplace Monitoring*, ALPHR (Jan. 18, 2016), http://www.alphr.com/business/1002466/big-brother-boss-the-psychological-weight-of-workplace-monitoring/page/0/1.

is an imperfect solution as, of course, many people do not have the flexibility to turn down work or choices for workplace environments.

But more importantly, the companies designing and promoting this type of technology should be aware of the privacy and discrimination risks posed by their use. Rather than presenting and promoting one state of the world, there could be an option to see alternate futures based on various characteristics and values. This would reduce the risk of prediction becoming a self-fulfilling prophecy that is posed by creating new metrics, analyzing current performance rates, and replicating the existing model of success, as well as replicating existing problems. Additionally, employers should note that there are current anti-discrimination laws on the books that may apply even in a technologically mediated decision-making process.

Conclusion

United States law has limited guidance on how to negotiate the evolving modern workplace, particularly with regard to the boundaries of personal privacy, leaving state policymakers, employers, and employees to sort things out amongst themselves. Policies must default to strong protections against company access to personal information, with some exceptions. To determine these exceptions, it is helpful to use practical frameworks that can be adjusted over time, such as situational and ongoing employer access exceptions. In addition, passive monitoring is unacceptable in a workplace without meaningful affirmative consent from employees and employers, and employers must serve routine notice and reminders that this type of monitoring is occurring, along with details about the data collected and the rationale for collection. Health programs, like employee wellness programs, should not be proxies for passive monitoring of employees. Employers should require the highest standards for privacy and security when employee health data is collected and used for any reason.

When an employee uses technology in the workplace, even when it used for business-related activities, they are not relinquishing their right to privacy. A strong default is also necessary given the inherent power asymmetry in the employer-employee relationship. Many of the technology changes we discuss in this paper leave employees vulnerable to privacy violations and it is crucial that policymakers, companies, and employers remain aware of this reality and adopt policies that default to strong protections against company access to personal information.