CENTER FOR
DEMOCRACY
& TECHNOLOGY

March 28, 2016

To Whom It May Concern:

The Center for Democracy & Technology (CDT) is pleased that policymakers are addressing the issue of employee privacy. Technological advancements have increased efficiency in the modern workplace but also blurred the lines between personal and work life. The availability of fine-grained information about individuals, such as their location, their activity levels, or their online habits, have made it tempting for employers to monitor their employees in a way that erodes an individual's ability to control the collection, use, and sharing of her personal information. Economic fair play, as well as the dignity of the individual, is at stake when her privacy is infringed upon in the workplace. We agree that codifying protections for employees is necessary and write to share our perspective and recommendations for how model legislation can be responsive to current, and near-future, workplace technology trends.

CDT is a nonpartisan, nonprofit advocacy organization dedicated to protecting and promoting civil liberties and human rights online and within digital technologies. We are known for advocating for pragmatic privacy solutions based on principled judgement and technologically sound insight.

The following policy recommendations offer two likely scenarios that might prompt an employer to ask their employee for access to content of an online account associated with the personal identity of their employees.

1) Situational: An employer requests access to content of a personal online account in response to a specific concern or complaint, most often to conduct an internal investigation. For example, one employee might accuse another of harassment conducted through a social network, and the employer could request to see the relevant content to determine whether to intervene.
2) Ongoing: An employer monitors activity on a personal account or device that is directly affiliated with the employer or business activities (described in the 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.

When the employer's request is situational, legislation should establish narrow and specific exceptions for employers to investigate bullying, harassment, fraud, misuse of company technology and information, or similar scenarios where an employee's action could or does incur employer-liability. Furthermore, we recommend that legislative language prevent using a discrete problem as an excuse to demand blanket access to an employee's personal account. If an employer discovers circumstances that might result in employer liability, they should conduct a targeted investigation including requests for access to specific content relevant to the concerns at hand. This

minimizes privacy risks, provided that the request is specific to to one situation, narrowly tailored in terms of the scope of data gathering and who can access the information, and directly issued to the individuals involved. Additionally, legislation should require that employers have a written policy that details the parameters of this type of investigation and provides information about employee rights. We agree with the ACLU that narrow requests for content should reference to a particular piece of content, rather than accessing an entire account. This is an important distinction in a world where very few people entirely separate personal and business correspondence, either on accounts or devices.

An ongoing scenario presents different circumstances for employers, and these cannot always be regulated by expecting requests for defined pieces of content. We believe employee privacy would be best served by legislation that requires employers to detail, in a written policy agreed to by both the employer and the employee, the terms of employer access to employer supported accounts and devices. The policy should delineate the amount and nature of ongoing employee surveillance and employee redressability under the legislation. Regulation should demand that policies cover, at a minimum, online accounts and bring-your-own-device (BYOD) environments. The increasing popularity of conscripting employee's accounts and devices for business use makes this a substantial demand, but CDT believes it is worthwhile in the service of both employee privacy and business liability.

Please be advised that, while our framework describes individuals as employees, job applicants should be afforded these benefits, including notice of the organization's workplace digital privacy policy, before accepting a position, especially in workplaces where technology is a core part of the job.

Many current state laws focus primarily on preventing employers from requesting or demanding authentication credentials to log into personal accounts. While we support mitigating this particular privacy harm, we also recognize that the ecosystem of technological interactions between employer and applicants and employees is much more complicated. While we cannot address all of the privacy issues raised in a digital workplace in this letter, we hope that sharing a framework for considering a broader perspective will allow drafters to think more comprehensively about workplace privacy. Current drafts already address the most extreme scenarios, but we believe this legislation provides an opportunity to redefine workplace norms and protect individuals' digital dignity in the workplace for years to come.

Please feel free to contact us with questions and thank you for your consideration.

Sincerely,

Ali Lange, Policy Analyst
Katie McInnis, Privacy & Technology Fellow