

Written Testimony

On Behalf of the

Pennsylvania Chamber of Business and Industry

Prepared by

Stephanie Catarino Wissman

Director, Government Affairs

On

House Bill 1298

Submitted to the Pennsylvania House Judiciary Committee

Honorable Thomas Caltagirone, Chairman

Honorable Ron Marsico, Minority Chairman

July 1, 2009

Chairman Caltagirone, Chairman Marsico and other distinguished members of the House Judiciary Committee and guests, the Pennsylvania Chamber of Business and Industry appreciates the opportunity to provide written testimony to discuss a very important issue to our membership.....employee email monitoring. We applaud Representative Cohen's ongoing efforts to balance employee workplace privacy with the need for employers to manage and protect company resources from non-productive, non-work related activities. However, as currently drafted, we believe HB1298 is extremely prescriptive and is not necessary in light of federal and case law and repetitive of existing employee monitoring disclosure policy utilized by Pennsylvania businesses today.

The Pennsylvania Chamber of Business and Industry is the state's largest broad-based business advocacy association, serving more than 24,000 members and customers. PA Chamber membership comprises nearly 50 percent of the private workforce, ranging from Fortune 100 companies to sole proprietors, and crosses all industry sectors. Many of these employers monitor their employees' use of their computer systems. House Bill 1298 proposes a specific standard for notifying employees about such monitoring. This bill is not necessary because the norms for notifying employees are already well established, in Pennsylvania and throughout the country. Moreover, the bill poses substantial burdens for many Pennsylvania businesses that have employees in multiple states and would have to comply with this unique proposed Pennsylvania standard in addition to the norm in other states.

The caselaw regarding an employers' practices for monitoring employees' use of the employers' computers in Pennsylvania and elsewhere is uniform: an employer that notifies its employees or obtains their consent may monitor their communications through the employers' computer and computer system. The employer may do so to properly administer its system, to prevent unauthorized access, to ensure the system is being used for legitimate corporate business and to investigate improper access or use. In Pennsylvania case of *Commonwealth v. Sodomsky*, 939 A.2d 363, 369 (Pa. Super 2007), the court explained that "if a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those

contents.” This requirement to inform employees before monitoring is rooted in the federal and state wiretap acts, including Pennsylvania’s Act.

An earlier federal case, decided under Pennsylvania law, evidenced the employer’s strong interest in monitoring its employees use of its computer system. In that case the court held that “an employee did not have a reasonable expectation of privacy in email communications voluntarily made by an employee” and that “the company’s interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.” *Smyth v. Pillsbury Company*, 914 F. Supp. 97, 101 (E.D. Pa. 1996).

Pennsylvania cases show that there is no magic formula for notifying employees of an employer’s practice of monitoring. *Sodomsy* cited to three cases from three different parts of the country where employers were permitted to monitor their employees’ computer use because the employers informed their employees of such monitoring. Similarly, in another recent case, *Ober v. Miller, et al*, 2007 U.S. Dist. Lexis 93236, *59 (M.D. Pa. Dec. 18, 2007), the court addressed “the prevalence of workplace monitoring on computers” and cited to a half-dozen cases also evidencing that an employer can monitor its employees upon notice to them.

Many Pennsylvania employers actually obtain the consent of their employees before monitoring their computer use. Indeed, many of these employers actually obtain the consent of their employees each day as their employees sign on to their computers; that is, the employee cannot even access their computer unless they consent to such monitoring. Some of the cases referenced above specifically addressed and approved of such frequency. Other Pennsylvania employers provide notice to employees in a Code of Conduct or Employee Manual near the start of their employment. Again, some of the cases referred to above approved of such practices.

Against this background of settled law and practice, and in light of the various manners by which an employer may permissibly inform its employees of a practice of monitoring, we do not believe it makes sense for Pennsylvania to direct that a specific approach be observed. The facts and circumstances regarding each monitoring program and each employer are different: an

established body of caselaw, rather than the short notice proposed in House Bill No. 1298, is most appropriate for guiding Pennsylvania employers.

The Chamber also believes that House Bill 1298, as currently drafted, dictates a disclosure process that creates the risk of the adoption of different standards in different states. Separate disclosure requirements in each state present costly and logistically complex hurdles for Pennsylvania employers that have employees in other states. We believe that informing employees before monitoring their computer use satisfies the standard in caselaw and that such an approach should be sufficient.

We appreciate the House's concern that there be some specific requirement that ensures that Pennsylvania employers provide some form of information to their employees about their monitoring processes. We respectfully submit that in light of the caselaw referenced above, and the Pennsylvania wiretap statute, that additional legislation is not required. Nevertheless, if the House believes that some additional requirement is needed, we have proposed amendments to the Bill (attached) to allow for monitoring after written general notice of the employers' intent to monitor.

Today more than ever, Pennsylvania businesses are being forced to improve their efficiency and security while competing and in ever-changing technologically driven global environment. Monitoring employee email and Internet activity over corporate networks is necessary to discourage the use of employer-owned computers and Internet services to facilitate harm to the employers' network or protect the company's intellectual property or its customers' information. Employers also want to make sure their employees are using company time productively and not creating a legal liability for their business as a result of harassing or offensive communications or by accessing pornography. In addition, employers have security concerns relating to the intentional or accidental sending of sensitive data via email attachments as well as the ongoing concern of viruses entering the business from outside communications. As a result, both public and private sector employers are monitoring employee's computer and Internet access to a greater degree than in the past and are using the surveillance of corporate networks to moderate

the temptations to use employer resources for personal use and encourage employees to adhere to company policies.

Again, thank you for allowing the Pennsylvania Chamber of Business and Industry the opportunity to testify on behalf of its members.