NATIONAL WORKRIGHTS INSTITUTE
Bringing Human Rights to the Workplace

July 26, 2014

Senator Chris Rothfuss, Chairman
Task Force on Digital Information Privacy
Wyoming Legislative Service Office
213 State Capitol
Cheyenne, W Y 82002

Dear Chairman Rothfuss:

Thank you for inviting me to share the National Workrights Institute's views on employment privacy with the task force.

The task force can make a vital contribution to privacy law in America. The core statute in this area, the Electronic Communications Privacy Act (ECPA) (18 U.S.C. 2510) was enacted in 1986. At that time, the primary method of communication was the telephone. Personal computers, E-mail, the Internet, and text messaging did not exist.

Communications technology has changed dramatically since 1986. But privacy law has not changed. There have been several attempts to update ECPA, but none of them has succeeded. We are trying to regulate 21st century communications technology with a law that was written before any of it was invented. The few state laws that have been enacted are reflexive responses to a specific incident.

It is high time to systematically examine modern methods of communications technology and create rules that are fair to both employers and employees. In creating the task force, Wyoming has initiated this critical and long overdue process.

Need for Employment Rules

Many people are legitimately concerned with the NSA's monitoring of personal communications. But monitoring by employers is far more common. While only limited information about the extent of federal government monitoring is available, the number of citizens affected is limited. The average person has little chance of having their personal communication monitored by the government.

Employment is entirely different. The Bentley Center for Business Ethics surveyed employers and found that 94% conduct electronic monitoring of employee communications. Other studies, including those conducted by the American Management Association, reach similar findings.

128 Stone Cliff Road
Princeton, NJ 08540
Tel. 609-683-0313
Fax. 609-683-1787
www.workrights.org

This does not mean that legislators should ignore government monitoring. But the first priority should be employer monitoring.

Employment Rules

The vital first step in this analysis is recognizing the need for different rules for employers and the government. The government generally monitors communications for the purpose of law enforcement. Employers are concerned with productivity, quality control, and compliance with company policies. Because the government and employers have different needs, they need different rules.

For example, the government generally needs a warrant to monitor a person's telephone or computer. To require employers to go to court every time they want to see an e-mail message sent by an employee on a company computer would be unfair and unworkable.

Current Paradigm

In the absence of statutory guidance, courts have been forced to develop common law to decide privacy disputes. The official standard that has emerged is whether an employee has a "reasonable expectation of privacy" in light of all the facts of her situation. Courts are to balance employees' need for privacy against the business needs of the employer.

In practice, the test is who owns the equipment involved in transmitting the communication. Courts have consistently held that employees have no reasonable expectation of privacy on company owned computers under any circumstances. In Smyth v. Pillsbury Baking (914 F.Supp 97) the court held that an employee had no reasonable expectation in e-mail sent from a company computer even when the employer told employees it would not monitor. I have been following the caselaw in this area for 25 years and have never seen a single case holding that employees have any right to privacy on company owned equipment.

Harm to Employees

This paradigm is often unfair to employees. Initially, employers took the position that workplace computers were for business purposes only. Courts held that an employee who used her employer's computer for personal business in violation of company police could not complain if her employer read the message. Employers quickly realized, however, that such a policy is unreasonable and unenforceable. In today's world, the once sharp line between work and personal life has been erased. People routinely log on to their company computer from home after they put their children to bed and return business calls from their cell phones on weekends. They also send personal e-mail from the workplace. The vast majority of employers (over 90%) have adopted policies that allow for reasonable personal use of employer communications technology.

But the legal rule has not changed. Even though employers now allow employees to send personal messages on company equipment, employees who do so are treated like trespassers who have no right to privacy. An employer can allow employees to use company equipment for personal matters, tell employees it will not monitor personal messages, and then deliberately read messages it knows are personal for no reason (or to learn about the employee's private life) without breaking the law. How is this reasonable or fair?

The loss of privacy is constant and serious. An employee's e-mail to her spouse, doctor, bank, and many others frequently contains extremely sensitive personal information. Monitoring the web sites an employee visits is possibly even more revealing. People visit the Internet for information and help about the most sensitive subjects imaginable People seeking help with substance abuse, marital problems, unplanned pregnancy, psychiatric problems, or financial difficulties will often turn to the Internet. If you were trying to pry into someone's personal secrets, you couldn't find a better way than monitoring her Internet activity.

We now live in a world where people routinely communicate about personal matters while they are working with absolutely no privacy protection.

Harm to Employers

Employers are now beginning to experience difficulties with the ownership paradigm in privacy law. Increasingly, workplace communication takes place on equipment that the employer does not own. Many people download workplace information onto their personal computers so they can work at home. Sometimes this information includes important intellectual property. An employer could legitimately be concerned about how an employee uses this information.

But it is very difficult for employers to find out what employees do with downloaded business information. Because the computer involved belongs to the employee, courts are very reluctant to give employers access, even when employers have legitimate concerns. For example, in *Sabin v. Miller* (423 F. Supp. 2d 943), the court refused to give the employer access to an employee's personal computer, even though the employee had downloaded company documents and there was evidence of misconduct. In *Wyatt Technology v. Smithson* (2006 WL 5668246, C.D. Cal.), the court found the employer liable for violating the Computer Fraud and Abuse Act (18 U.S. C. 1030) when it accessed the computer of a former employee even though he was working for a competitor and the company had evidence that he was misusing its trade secrets.

Employers have the same problem regarding wireless communications. The Stored Communications Act (18 U.S.C. 121) provides that Internet Service Providers can reveal the contents of messages only to the parties. Employers are not considered parties to the message, even if they pay for the service. In *Quon v. Arch Wireless* (529 F.3d 892), the 9th circuit court of appeals held that the ISP violated SCA by disclosing the content of an employee's text messages to his employer. The court also held that the employer violated the act. The employer appealed other issues in this case to the Supreme Court, but

did not appeal this ruling. This problem will grow more serious as more the use of wireless communication grows.

New Paradigm

Both employers and employees would be better off if employer access to electronic information were determined by whether the employer has a legitimate interest in the information rather than whether it owns the equipment used to transmit/store the information.

This is the original paradigm for federal privacy law. The Electronic Communications Privacy Act (supra) allows employers to listen to employees' telephone conversations if they are work related, but not if they are personal. Both employers and employees receive fair treatment with this rule and courts had no difficulty implementing it.

The key to creating employment privacy legislation for the 21st century is returning to this paradigm for other forms of electronic communication.

Enforcement

Creating effective enforcement mechanisms for privacy laws has always been a challenge. Criminal penalties are not effective because law enforcement agencies are reluctant to divert resources from crimes against people or property to prosecuting violations of privacy law. Private civil actions are difficult to bring because violation of privacy laws seldom creates demonstrable economic harm.

These challenges can be met by providing successful plaintiffs with reasonable attorney's fees and the alternative of an administrative remedy.

Enforcement of employment laws is difficult because at will employees have little choice but to agree to waive their rights when their employers requests it. This problem can be addressed by providing that rights created by a statute are not subject to waiver.

I look forward to speaking with you and the rest of the task force on July 30.

Sincerely yours,

Lewis L. Maltby
President
National Workrights Institute