The Password Protection Act of 2012

Recent news reports have highlighted a disturbing increase in the number of employers asking prospective employees to hand over usernames and passwords to their personal, private accounts on websites like Facebook. Some job applicants are even being asked to provide passwords on job applications, allowing employers to view an applicant's private information at any time.

Requiring access to prospective or current employees' password-protected accounts as a condition for employment is an unreasonable violation of employees' privacy. Employees are not required to hand over the keys to their houses as a condition of employment, and should not be required to hand over access to their most private and personal digital email or social network accounts either. An employer has several reasonable and comprehensive ways to find out more information about an applicant, including the application or resume, the interview, references, or an internet search of the applicant.

Requiring prospective or current employees to provide login credentials to employers compromises the security of the employees' personal data. An employee who takes care to keep personal data secure through the use of encrypted networks and websites, secure logins, and other data security measures loses control over that data when forced to hand over usernames and passwords to an employer. Because the employee does not know whether the employer uses secure, responsible data practices, that employee's personal or financial information may face an increased risk of online breach and theft.

Employees who provide employers access to their email or social networking sites may face illegal or unfair discrimination based on information found on those sites. Social networking sites often contain information about an employee's race, religion, sexual orientation, marriage status, pregnancy status, and other personal information which may be used by the employer to discriminate against the employee. Employers who view such information, even if the information does not factor into an employment decision, also expose themselves to claims of discrimination.

The Password Protection Act of 2012 addresses this problem by enhancing current law to ensure that compelling or coercing employees into providing access to their own private systems and data—including social networking sites, online email accounts, or personal data storage systems—is prohibited:

- **No Compelled or Coerced Disclosure.** The Password Protection Act prohibits an employer from forcing prospective or current employees to provide access to their own private systems as a condition of employment. Examples of prohibited actions include forcing employees to—
    - Hand over their private passwords to personal Facebook or Gmail accounts.
    - Log into a password-protected account so that the employer may browse the account's contents.
- **No Retaliation.** The Password Protection Act prohibits employers from discriminating or retaliating against a prospective or current employee because of a refusal to provide access to a password-protected account.
- **Narrow Remedy.** The Password Protection Act only prohibits adverse employment-related actions as a consequence of an employee's failure to provide access to their own private accounts. It preserves the rights of employers to—
    - Permit social networking within the office on a voluntary basis.
    - Set their own policies for employer-operated computer systems and accounts.
    - Hold employees accountable for stealing data from their employers.
- **Enforcement.** Employers that violate the Password Protection Act may face financial penalties only.