Privacy law developments

How to understand and comply with recent changes in privacy law

Interviewed by Troy Sympson

Last year, the landscape of privacy law changed on several different fronts, and if companies aren't aware of those changes, they could find themselves at severe risk.

First, in terms of workplace privacy, the Supreme Court ruled in *City of Ontario v. Quon* that the Ontario, California Police Department did not violate the Fourth Amendment rights of a SWAT team member by reviewing personal text messages he sent and received on a department-issued pager. Significantly, the court declined to rule on the broader issue of whether employees have a reasonable expectation of privacy when using employer-provided equipment for personal communications. The court did provide a bit of guidance for employers by noting that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."

Also, the FTC had a significant up-tick in its focus on privacy issues, including a very significant settlement with the social networking site Twitter and release of a proposed framework that would provide considerable clarification and guidance on issues of consumer data privacy.

"The third notable thing that occurred with privacy law in 2010 was the increased presence of plaintiff lawyers in the fray," says Kit Winter, a member with Dykema Gossett PLLC. "We're seeing more and more businesses being sued for violating consumer privacy rights."

Smart Business spoke with Winter about these changes to privacy law and what companies can do to ensure they're covered.

Kit Winter
Member
Dykema Gossett PLLC

What are the primary areas of privacy law that businesses should be most concerned with?

The first is employee privacy in the workplace. Although the trend seems to favor employers, the Supreme Court's decision in *Quon* leaves many questions open, making it especially critical to obtain appropriate legal advice when dealing with employees' personal communications and information. For example, the New Jersey Supreme Court ruled in April 2010 that an employee had a reasonable expectation of privacy in personal e-mails sent via her employer-issued computer, even though the employer had a policy stating that the company could monitor such communications and that all e-mails were not to be considered private. The court found that because the employer's privacy policy permitted 'occasional' personal use and did not specifically inform employees that the company stored copies of employees' private Web-based e-mails, the policy was ambiguous and did not override the employee's subjective expectation that her communications would be private. To avoid this sort of result, businesses should adopt and disclose detailed privacy policies, comply with those policies, and know the specific laws applicable to the locations in which they operate.

Protection of consumer data is another area of potential risk. There have been laws in effect at the state level for more than a decade that say businesses need to use reasonable measures to keep consumer electronic data private. In 2010 the FTC raised the bar on the understanding of 'reasonable measures' by bringing an action against Twitter alleging that it permitted users to select easily guessed passwords. Twitter settled the FTC action by, among other things, agreeing to permit the FTC to audit its privacy protection practices for the next 20 years. The FTC's action against Twitter is a clear message that robust privacy measures are required to pass FTC muster.

How can companies protect themselves against privacy litigation?

The FTC's proposed privacy framework provides some welcome guidance. In order to reduce the burden on consumers resulting from long, legalistic privacy policies and ensure basic privacy protections, the FTC recommends that 'companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices.' Companies can protect themselves by providing reasonable security for consumer data, limiting and monitoring collection and retention of such data, and implementing reasonable procedures to promote data accuracy. In order to accomplish these goals, companies should consider assigning personnel to oversee privacy issues and training employees in privacy practices, among other things. The FTC is also encouraging companies to broadly disclose their privacy policies and to honor consumer requests to opt out of information gathering procedures like click tracking.

The big picture is that it is increasingly imperative that companies accurately describe what information they collect and what they do with that information in a manner that can be easily understood by consumers. Companies cannot store consumer data in an unencrypted manner and they must implement vigorous security protection for all consumer data and information that they collect and store.

Going forward, what should businesses in particular be aware of?

The trend in the future is for increased regulation of privacy and businesses' use of consumer data. For example, the FTC is proposing a universal opt-out provision akin to the Do Not Call Registry that would allow Internet users to opt out of being tracked by companies and advertisers. The FTC has also made clear that when a company makes representations about how it treats consumers' personal information, it has to live up to those promises or face FTC action.

The landscape of privacy regulation is rapidly changing and companies need to carefully examine what consumer data they collect and how they use it in order to avoid potential liability. <<

KIT WINTER is a member with Dykema Gossett PLLC. Reach him at (213) 457-1736 or kwinter@dykema.com.

Insights Legal Affairs is brought to you by Dykema Gossett PLLC