



## PRIVACY, DATA SECURITY & INFORMATION LAW UPDATE

### The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers. Sidley provides services in the following areas: Privacy and Internet Litigation and Regulatory Advice; Data Breach, Incident Response, and Cybercrime Advice; Global Data Protection and Information Security; International Data Transfer Solutions; Outsourcing and Cross-Border Issues; Gramm-Leach-Bliley and Financial Privacy; HIPAA and Healthcare Privacy; Workplace Privacy and Employee Monitoring; Cyberlaw, E-Commerce, and Internet Issues; Unfair Competition and Consumer Protection; Trademark and Copyright Litigation and Counseling; Website Policies and Domain Name Protection; Records Retention and Electronic Discovery.

To receive future copies of this and other Sidley Updates via email, please sign up at [www.sidley.com/subscribe](http://www.sidley.com/subscribe)

This **Sidley Update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000. Prior results do not guarantee a similar outcome.

### Supreme Court Unanimously Upholds Employer Ability to Access and Search Employee Messages Under Reasonable Circumstances

In one of the most closely watched information privacy decisions of recent years, the Supreme Court unanimously upheld an employer's ability to access and review employee text messages on employer-provided service and equipment under certain circumstances. The Court made clear that the right of the employer to access and review employee communications in the workplace is not unbounded. Rather, employers must consider whether the purpose and scope of such searches are legitimate and reasonable in light of the employer's privacy policy regarding workplace monitoring and surveillance.

The Court chose not to decide any issue categorically in this "sexting" case involving salacious text messages apparently sent by a member of the Ontario, California SWAT team, *City of Ontario v. Quon*, Nos. 09-497, 09-448. The Court took a restrained approach, declining to clarify privacy expectations for specific technologies or to provide certainty regarding whether an employer's privacy policies can definitively extinguish any employee expectation of privacy in the workplace. The decision avoided articulating any new general rules, although it did decide that the particular government-employer search conducted in the case was reasonable, and that the type of limited employer search in *Quon* - which ultimately resulted in the employee being disciplined - would be "regarded as reasonable and normal in the private-employer context" as well. A key point, however, is that the propriety of employer searches - at least in the context of government-employer searches subject to the Fourth Amendment - will be determined on a case-by-case basis.

The implications of the decision for private companies are generally favorable. Specifically, the Court appeared to acknowledge that employer searches are normal and reasonable in the private sector. The Court did not in any way undercut the ability of private employers to shape their employees' privacy expectations through privacy policies and disclosures regarding monitoring practices. It should be noted, of course, that the private sector is not generally subject to the Fourth Amendment's guarantee of freedom from unreasonable searches and seizures. The Court, however, left open the possibility that under certain circumstances, some employee communications on

some technologies might be deemed beyond an employer's ability to monitor legally. Lower courts had already been moving in this direction, for example, with employee communications with their personal attorneys over an employer network. Thus, companies would be well advised to revisit and clarify their privacy policies and practices with regard to employee monitoring and surveillance. In addition, companies should consider developing investigative protocols for vetting, conducting and limiting searches, documenting the purpose for such searches, and establishing minimization procedures in order to enhance the likelihood that such searches will be deemed compliant by any future reviewing courts and not offensive to evolving notions of privacy.

### Background

The principal issue in *Quon* was whether a government employee had a reasonable expectation of privacy in text messages sent through government-issued communications equipment despite a written policy that such messages were subject to monitoring without notice. A supervisor had orally assured the employees that their messages would not be reviewed, but nevertheless, the employer conducted a limited review of two months of messages to determine whether the text allowance under the plans was adequate to cover business use before employees had to pay for their own messages. During the review, Quon's supervisor discovered that Quon was sending a disproportionately large amount of personal and even sexually explicit texts during his shifts, and referred the matter to internal affairs to determine if Quon was violating Ontario Police Department rules. Ultimately, Quon was disciplined for his texting habits.

The District Court ruled in favor of the City of Ontario, but the Ninth Circuit reversed in relevant part, holding that the examination of the respondents' text messages was "unreasonable as a matter of law" in violation of the Fourth Amendment. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (2008). The decision of the Ninth Circuit had raised some fears that employers' written policies would not be respected as

conclusively precluding employees from having an expectation of privacy in their employer-provided electronic devices, particularly in the context of governmental employers as presented by the case. The briefing in the case had urged the Court to move beyond the government employer context presented and address whether employees have an expectation of privacy - or not - in personal communications sent using their workplace pagers and other information technology. For instance, the Solicitor General, as *amicus curiae*, urged that the Court broadly establish that employers' written policies conclusively establish the relevant expectation of privacy. Specifically, the United States contended that a non-policy-making official such as the supervisor should be unable to modify the policies established by the City of Ontario and that any lax or contradictory enforcement by Quon's supervisor did not undermine the City's written policies.

### Decision

Writing for eight members of the Court, Justice Kennedy declined to embrace a broad view of the issue presented or to attempt to announce new rules for emerging technologies. "A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds." *City of Ontario v. Quon*, Nos. 09-497, 09-448, *Slip op.* at 11-12.

The Supreme Court decision thus does not provide a broad, categorical rule - "Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices." *Slip op.* at 10. The court assumed, *arguendo*, that Quon had an expectation of privacy in his text messages, but held that the City's search was nevertheless reasonable under the Fourth Amendment because it fell within a government employer special needs exception. *Id.*, at 13. Further, the Court expounded that the *Quon* search would be

“regarded as reasonable and normal in the private–employer context.” *Id.*, at 8.

Although the audit and search of text messages were deemed normal and reasonable in this case, that judgment depended upon the Court’s *post hoc* assessment that the employer’s purpose was just and the methods used during the search were not unduly intrusive or excessive. The Supreme Court’s recognition of the nuances in employer searches, however, has not substantially undermined the general ability of employers to establish workplace expectations through applicable privacy policies and practices and conduct reasonable searches. Indeed, much of the law on the reasonableness of searches in the employment context will continue to evolve in the context of state statutory protections and state employment tort cases.

Under the Supreme Court’s approach, employers will continue to face the uncertain consideration of “how employees’ privacy expectations will be shaped by... changes [in technology] or the degree to which society will be prepared to recognize those expectations as reasonable.” *Slip op.*, at 11. Under the decision, it would seem that devices deemed “essential means or necessary instruments for self-expression, even self-identification” will be accorded some degree of privacy, but it is also necessary to consider the cost of these devices and “employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.” *Id.* In his concurring opinion, Justice Scalia criticized this approach, however, writing that “[a]ny rule that requires evaluating whether a given gadget is a ‘necessary instrumen[t] for self-expression, even self-identification,’ on top of assessing the degree to which ‘the law’s treatment of [workplace norms has] evolve[d],’... is (to put it mildly) unlikely to yield objective answers.” Concurring op. of Scalia, J., at 3. Employers may well bemoan that their policies seem to be but one factor that will apparently be considered in deciding whether an expectation of privacy exists. Likewise, employees have no reasonable

assurance that the court would find any expectation of privacy in any of their workplace communications.

### **Implications of *Quon***

The Supreme Court’s opinion does make clear that it will restrain itself for some time from deciding whether expectations of privacy will be recognized for each new electronic device. The benefit of this approach is that it provides room for another branch of government to weigh the interests at hand and establish privacy norms for the evolving generations of information technology. In taking this tactic, the Court likely implicitly intended to refer the issue to legislatures – both federal and state – to decide the extent of privacy interest that workers have in their employer provided information technologies, if any.

On a practical level, employers should no doubt continue to follow best practices for a reasonable and proportionate investigation for employment purposes. Clear policies should be established and implemented to ensure that monitoring and searches are reasonable in the given circumstances. Anyone conducting an investigation in an employment context should be particularly careful to document the justified initial purpose of the search, the parameters of the search, and efforts to minimize the acquisition of collateral personal data. Investigators should also pay special attention to the impact of the search on third parties who have communicated with the employees, particularly in states with all-party consent electronic communications wiretapping statutes.

### **Similar Cases To Note**

The Supreme Court’s *Quon* decision may be usefully contrasted with the recent decision of the New Jersey Supreme Court, which adopted a less deferential view of employer monitoring rights than those advanced by the Solicitor General in *Quon*. The New Jersey Justices ruled that communications with an employee’s attorney – even if accessed or transmitted over the employer’s network and saved on the employee’s work computer – could not be reviewed by the employer. *Stengart v.*

*Loving Care Agency, Inc.*, Case No. A-16-09 (decided March 31, 2010). The employer's monitoring policy did not allow the employer to review privileged communications, and thus an employee retained a reasonable expectation of privacy in e-mail communications with her lawyer over a personal, password protected, web-based email account, despite using the company's computer and network. Under New Jersey law, using a company laptop to send and receive the message did not eliminate the attorney-client privilege. The New Jersey court thus made clear that while companies can adopt and enforce policies protecting the technological assets of the company, employers should proportionally limit review of employee communications for legitimate business purposes.

The Supreme Court will soon be hearing another employee privacy right case in *NASA v. Nelson*, No. 09-530 (U.S. cert.

granted March 8, 2010). The case involves a challenge to background checks for NASA non-sensitive contract employees. The employees challenged broad questionnaires soliciting "adverse" information from third parties on a range of topics including employee's drug treatment, mental or emotional stability, financial information and "other matters." Employees who did not submit to the background check would be deemed to have resigned. The District Court denied the employee's motion for a preliminary injunction, but the ninth Circuit found that the background check had the potential to violate Constitutional privacy rights. While the long term significance of *Quon* is uncertain, it is thus clear that these issues of evolving technology and privacy in the workplace will be back before the Supreme Court in the future.

**If you have questions about any of these items, please contact your regular Sidley Austin LLP contact.**

Alan C. Raul, Partner

Washington, D.C.

araul@sidley.com

+1.202.736.8477

Edward R. McNicholas, Partner

Washington, D.C.

emcnicholas@sidley.com

+1.202.736.8010

Colleen T. Brown, Associate

Washington, D.C.

ctbrown@sidley.com

+1.202.736.8465

**www.sidley.com**

*Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley, or the firm.*

