Employment Issues Related to Electronic Communications

IACP Annual Conference
Legal Officers Section
October 2009 - Denver

I. Recent Cases

Cowles Publishing Company v. Kootenai County Board of County Commissioners, 159 P.3d 896 (Idaho 2007) – Employee who had signed county's email policy stating that employees had no right to personal privacy when using the county's email system, lacked any reasonable expectation of privacy in person emails between herself and her supervisor, regardless of the subject matter of the emails.

Quon v. Arch Wireless Operating Company, 529 F.3d 892 (9th Cir. 2008), reh. den., 554 F.3d 769 (2009), petitions for cert. pending – Police Department investigating excessive text message usage obtained transcript from their contracted provider and discovered sexually explicit text messages. In ensuing litigation, the Court held that Arch Wireless is an "electronic communication service" (ECS) for purposes of the federal Stored Communications Act of 1986 and hence was liable for the release of transcripts to anyone other than the addressee or intended recipient of those communications (as opposed to an RCS, remote computing service, which can release transcripts to the subscriber).

The Court also held that despite a department policy entitled "Computer Usage, Internet and E-mail Policy" which stated that users "should have no expectation of privacy or confidentiality when using these resources," and which was considered applicable to text messages, and despite the fact that these messages were public records under California law, because the operating practice of the Plaintiffs' supervisor was not to review the records if any charges related to overuse were paid by the user, Plaintiffs had a reasonable expectation of privacy in their text messages and the ensuing search by the department was held to be unreasonable in violation of the Fourth Amendment.

Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. MI 2008) – In ruling on a discovery challenge by the principals in the much-reported situation that led to the removal of the Detroit Mayor, the District Court ruled that the SCA does not override Defendants' obligation to produce relevant, non-privileged electronic communications within their possession, custody, or control.

Stengart v. Loving Care Agency, 973 A.2d 390 (N.J. App. Div. 2009) – Plaintiff communicated with her attorney via personal emails using a personal email account accessed from her company's computer system. The company's policies stated that all communication on company computers would be considered to be part of the company's business records (although also permitting "occasional personal use"). The Court held, not surprisingly, that the attorney-client privilege trumped the corporate policies and ordered all copies of such emails returned to plaintiff and deleted from any hard drives. The Court noted that a "policy imposed by a employer, purporting to transform all private communications into company property—merely because the company owned the computer used to make private communications or used to access such private information during work hours—furthers no legitimate business interest."

Van Alstyne v. Electronic Scriptorium, 560 F.3d 199 (4th Cir. 2009) – In subsequent litigation with a former employee, the President of Defendant's company produced documents obtained by his accessing, without permission, the Plaintiff's personal aol email account (which she had occasionally used for company business). Following a jury trial, a verdict was returned in Plaintiff's favor for $175,000 in compensatory damages against the company and its president and $100,000 in punitive damages against the two for violations of the federal Stored Communications Act. The Court of Appeals upheld the punitive damages (and attorney's fees), but found that compensatory damages would not lie under the Stored Communications Act absent prove of actual damages.

Steinbach v. Village of Forest Park, 2009 WL 2605283 (N.D. Ill. August 25, 2009) - Plaintiff, a Commissioner and City employee, sued the City and the Mayor over the Mayor's unauthorized accessing of her city email account, citing violations of the federal wiretap law and the Stored Communications Act and alleging a state tort claim of "intrusion upon seclusion." The Court allowed Plaintiff to proceed on the tort claim and the SCA claim, but found that municipalities are not liable under the wiretap law (contrary to the position of the 6th Cir.)

Pietrylo v.Hillstone Restaurant Group, 2008 WL 6085437 (D.N.J. July 25, 2008) – Plaintiffs in this case were two former employees of a Houston's Restaurant who started an invitation only MySpace page, inviting co-workers to join to blog about negative experiences at Houston's. One invitee showed the site to a manager and then allowed the manager to use her password to access the site. Upper management was not impressed with the initiative shown by the Plaintiffs, who were subsequently fired and filed suit.

The District Court dismissed some of the claims (notably their Free Speech, protected by "public policy" claims), but allowed the case to proceed to trial on allegations that the employer's actions violated federal and state Stored Communications Acts and interfered with the Plaintiffs right to privacy. The jury found in favor of the Defendant on the privacy claims (finding no reasonable expectation of privacy in MySpace postings), but found that the Defendant violated the statutory communications law provisions, awarding $3,400 in back pay and $13,600 in punitive damages.

II. Policy and Practice Tips for employers

Banning employee use of social networking sites is shortsighted and probably unenforceable, particularly if the employer uses social networking. Most police agencies take a proactive approach, with a policy in place to encourage positive interaction in social media.

- Proxy sites abound to permit employees to access blocked sites; those proxy sites probably pose a greater risk to your online security than the social networking sites
- Morale likely to be negatively affected by total ban
- The employer should encourage its employees to interact positively with the employer's social networking site, with policies in place to ensure that the agency's brand and reputation is enhanced
- Sites serve an important recruiting tool

There are many model policies, but an agency should tailor its policy to its specific needs. Lauri Stevens, principal consultant and founder of LAwS Communications, at www.ConnectedCops.net, says law enforcement-specific policies should address:

1. Integrity. Perhaps the most important part of everything a law enforcement agency does, online or elsewhere, is integrity. Agency participants in social media should be reminded that integrity is the essential ingredient to using social media ethically. Agency employees should, therefore, be honest in their use of social media and maintain high regard for the public interest. All information disseminated should be absolutely accurate.

2. Disclaimers. Because you may be giving your personnel the authority to comment on issues relating to the department, it's imperative to emphasize the importance that officers, especially, state that what they write is their own opinion and not that of the department.

3. Identity. Some bloggers work anonymously, using pseudonyms or false screen names. Law enforcement agencies should absolutely insist that in blogs, wikis or other forms of online participation that relate to the department or the city, or activities or issues with which the department is engaged, department employees use their accurate identity.

4. Department-sanctioned tools. While it should be stated that the agency's social media policy covers activity by agency employees on tools they may create on their own or those of others that they might contribute to, department-sanctioned tools—the ones the agency initiates and sponsors—should be governed more closely. The guidelines for these can be as strict as the agency deems necessary, but should also include encouragement of participation along with the

requirements for an officer to use his agency email and photo and in his online profiles.

5. Competence. Department employees, whether staff or sworn, should not use any social media tool unless they really understand how it works. It hearkens back to that higher moral standard for police. Officers have often stated, with Facebook for example, "I don't friend anyone I don't know." Good idea.

   However, they don't know everyone that their friends know. Consider the case of the friend of the wife of an officer who posted some party pictures which included lots of cops drinking beer at a local watering hole. In and of itself, that's not the problem. But the friend of the wife tags a few of the guys by name, others comment on the content of the photos with statements like "how drunk were you guys?", and it goes on from there.

   None of it was created by any "friend" an officer knew, but rather friends of friends of friends. To be absolutely safe, the best recommendation is that officers keep separate profiles for work and play. On non-department related profiles however, officers should still exercise command sense and a great deal of caution.

6. Command staff responsibility. Standard disclaimers do not, by themselves, exempt command staff from any special responsibility. By virtue of their position, they must consider whether personal thoughts they publish may be misunderstood as expressing opinions of the agency. Additionally, a command staff member should assume that department employees will read what is written. A public blog is not the place to communicate department policies to department employees.

7. Training. Provide social media training for your officers and staff. Once your policy is written, be sure to distribute it with conversations about departmental support for social media. That would be a good time to roll out training in the various tools. Social media tools scare some people. They shouldn't. However, scary things can happen if they're not understood; a little knowledge goes a long way.

III. Liability risk exposure for employers

- Stored Communications Act penalties for accessing employees' private email or restricted social networking site content
- Fourth Amendment claims against governmental employers for unreasonable search or seizure of electronic information where there is a reasonable expectation of privacy
- State privacy laws and other statutory protections
- Regulating off-duty conduct
- Title VII or state antidiscrimination laws (accessing publicly available information regarding prospective employees)

- Trade secret laws (posting confidential or proprietary information may waive statutory protection for such information)
- FLSA (wage and hour employees' use of the company social networking site during non-work hours)
- Use of publicly-available social networking content to impeach or otherwise discredit agency employees in criminal and civil cases