Law & Forensics

E-Discovery, Forensics, Cyber Security, and Cyber Warfare ™

APPROACHING PRIVACY IN WIRELESS COMMUNICATION

Tips for counsel on the most pertinent issues to resolve in privacy cases involving mobile device messaging, seen through the lense of the landmark case City of Ontario, California, et al v. Quon

By Daniel Garrie

INTRODUCTION: AFFORDABLE DEVIES RESULT IN AN INCREASE IN WIRELESS COMMUNICATIONS

According to Gartner Inc., an information technology research and advisory company, "[w]orldwide mobile phone sales to end users totalled 1.211 billion units in 2009, a 0.9 per cent decline from 2008. In the fourth quarter of 2009, the market registered a single-digit growth as mobile phone sales to end users surpassed 340 million units, an 8.3 per cent increase from the fourth quarter of 2008." As demand for handheld wireless communications increases, so does competition in the mobile market. As devices become more affordable to consumers, data usage grows lock step - exponentially.

BlackBerry's Research In Motion Inc. (RIM) reported this year that more than 250,000 organizations worldwide use Blackberry Enterprise Server and in fiscal 2010 RIM sold 36,707,000 mobile devices in the fiscal year ending February 2010, which is a 41.1 percent from 26,009,000 in fiscal year 2009. iPhone's Apple Inc. reported opening 273 stores as of Sept. 26, 2009 and that "[n]et sales of iPhone and related products and services were $6.7 billion for 2008, with iPhone handset unit sales totaling 11.6 million. This compared to the $630 million in net sales of iPhone and related products and services in 2007 captures the tremendous growth."

CITY OF ONTARIO, CALIFORNIA, ET AL. V. QUON: REDEFINING PRIVACY IN THE MOBILE AGE

The ease of use provided by text messaging (SMS) and multimedia messaging (MMS) (e.g., transmittals of pictures, audio and video files) has created the ultimate supplementation to traditional landline networks, in the business environment. *City of Ontario, California, et al. v. Quon*, 130 S.Ct. 2619 (2010) is a recent - and now seminal - example of how the ease of use provided by mobile technology is transforming the legal construct of "private" communications and what is truly a "private communication."

Privacy of communications are typically protected pursuant to statute (e.g., Wire Tap Statute); or pursuant to common law (e.g., attorney-client privilege, patient-physician privilege, etc.). Therefore, the *user* of SMS messaging and mobile e-mail is what places the privacy of one's communications at risk - not some esoteric aspect of mobile technology. Understanding how SMS and e-mail work technologically will assist in knowing how not to compromise one's individual right to privacy. Unwary mobile communications users are more vulnerable to undermining their own privacy.

In *Quon*, a SWAT team member of the Ontario Police Department had been issued a department-issued two-way pager. The messaging carrier was Arch Wireless Inc. which was subsequently acquired by USA Mobility Inc. The Ontario Police Department had a "no-privacy" policy, reserving the right to audit the SMS conversation chains. A lieutenant without policy-making authority permitted SWAT team members to use the SMS messaging service for personal use if the officers themselves paid the police department for any coverage charges. The city of Ontario eventually conducted an audit of Sgt. Jeff Quon's messaging account revealing Quon had been sending personal messages (at times containing sexual content) to his wife as well as a police dispatcher/co-worker with whom Quon was alleged to be having an affair. In addition to his wife and dispatcher, Quon sent various messages to another SWAT team officer, Sgt. Steve Trujillo, which were of a personal nature.

Quon, his wife, and Trujillo filed suit against the city of Ontario and the SMS carrier, Arch Wireless. The complaint was filed in federal court, claiming certain privacy violations under the Fourth Amendment and the corollary contained in California's constitution. The complaint also alleged Arch Wireless violated the federal Stored Communications Act for being the SMS carrier that divulged the paging content of the text messages without prior consent from Quon.

PRIVACY EXPECTATIONS IN THE PUBLIC EMPLOYEE WORKSPACE

Quon was extensively litigated before the U.S. District Court, resulting in a jury verdict that led to absolving the police department of any privacy violation. The 9th U.S. Circuit Court of Appeals vacated the jury verdict and ruled the city of Ontario's

review of the SMS content violated Quon's Fourth Amendment right to privacy. The 9th Circuit relied upon the fact that Quon has been informed by the department that the content of his messages would not be audited if he paid overages on the department's paging account attributed to his personal use.

The U.S. Supreme Court overruled the 9th Circuit, reversing and remanding the case to the District Court. The Court held, inter alia, that "[b]ecause the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable under the approach of the O'Connor plurality." Therefore, Quon appears to suggest that so long as the intention of the search into employee communications is legitimate, there is not necessarily a violation of privacy.

An open question seems to remain whether it truly matters if technology issued by the employer lowers one's expectation of privacy. Quon involved a public sector employer presenting a different and heightened level of privacy. However, the Supreme Court does not appear to differentiate between a public employee and private citizen when it comes to a subjective expectation of privacy in electronic communications that are not work-related - despite being transmitted using a mobile communications device issued by an employer. Notably, the Supreme Court explicitly stated that it "...must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer, and the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." Importantly, Quon does not establish that the Fourth Amendment requires that an employer be circumspect in how it reviews use of its technology.

TIPS FOR COUNSEL

All attorneys, regardless of their practice areas, can learn a great deal from the privacy implications raised in Quon. Counsel must not rest simply knowing a client uses mobile messaging device, but must resolve the following issues, which are not all inclusive and will be case specific:

- Determine the setting in which the client used mobile communications (e.g., public or private employment setting).

- Investigate the usage and privacy policies for mobile communications issued by the employer or agency to the client. When private actors are at issue, there is no legally founded right to privacy in a verbal representation.
- Evaluate the contractual relationship between the mobile communications carrier and the user - what are the "terms and conditions" applicable to the carrier's service? Personal e-mail accounts for a client may be accessible and subject to discovery if the information technology schematics and policies for the entity provides for it. Therefore, all counsel must ensure that clients use personal computers and mobile communications devices.
- Determine the messaging gateway system used by the employer or agency to which may betray the privacy of the content by the nature of the system (e.g., copying all messages sent and received to a third-party server). Confirm the client understands the type of technology used by the employer or agency and the industry in which it is being employed. For example, a pager issued to law enforcement who are first responders are likely less private than a mobile handheld issued to a physician at a medical facility or attorney at a law firm.

CONCLUSION

Whether one works for a small, closely-held business or a large, multinational corporation, the purpose of the mobile device and who issued it to the client will likely impact one's ability to claim a reasonable expectation of privacy

6506 3rd Ave. NW, Suite C
Seattle, WA 98117

T: 425.395.4092

F: 866.893.4785

E: info@lawandforensics.com

W: http://lawandforensics.com