GESMER UPDEGROVE LLP
Attorneys At Law

Technology Law Bulletin

Providing comprehensive legal services to high technology companies

Vol. XII, No. 3 **Fall 2004**

First Circuit Ruling Curtails Wiretap Act Protections

Joseph J. Laferrera
joe.laferrera@gesmer.com

"Civilization is the progress toward a society of privacy."
– Ayn Rand, *The Fountainhead*

"[T]he advance of civilization is nothing but an exercise in the limiting of privacy."
– Isaac Asimov, *Foundation's Edge*

Privacy. Highly valued by patriots and scoundrels alike, we sometimes seem torn about whether our society needs more privacy or less. Although "privacy" is not even mentioned in the Constitution or Bill of Rights, the Supreme Court has long recognized it to be among the rights guaranteed to every citizen by those documents. Like all civil rights, however, privacy has its limits, and it must sometimes bow to the demands of public safety and national security. Congress tried to strike a balance in 1968 with the passage of the so-called "Wiretap Act," which strictly limited the conditions under which certain communications could be intercepted. In recent years, terrorist threats and advances in technology have altered that balance, forcing lawmakers and others to reexamine the issue.

"Wiretap Act protections may now be…all but unenforceable, a quaint reminder of a pre-digital world."

The scales tipped in June, perhaps dramatically, when the First Circuit Court of Appeals in Boston issued its decision in *United States v. Councilman*. In that case, the Court concluded that the federal Wiretap Act did not prohibit an Internet service provider (ISP) from surreptitiously diverting and reading its customers' emails. While that fact alone should give pause to all email users, the logic driving the decision may portend even broader application. The Court's reading of the Act may extend to more traditional modes of communications, and greatly ease the government's ability to tap telephone calls.

The defendant in the case, Bradford Councilman, was the vice-president of a company involved in the online sale of rare and out-of-print books. His company, Interloc, had provided email service to its book dealer customers. Councilman and others at the company devised a scheme to secretly divert emails sent by rival Amazon.com to those customers' Interloc email accounts, so Interloc employees could examine them for competitive advantage. In July 2001, the government indicted Councilman and others for intercepting those emails in violation of the Wiretap Act. Councilman challenged the indictment, contending the Act did not apply.

The fundamental question for the Court was whether emails qualify as electronic communications whose interception is forbidden by the Act. On its face, the Act's definition of "electronic communications" seems broad enough to cover email. But Councilman argued that it did not apply if the email was obtained from storage – either from the memory or the hard drive of a physical device. Comparing different provisions of the Act, he noted that the definition pertaining to telephone calls expressly included stored communications (such as voicemails), but the definition pertaining to emails was silent on the issue. So, Councilman reasoned, Congress must have intended to *exclude* stored communications from "electronic communications" protected under the Act.

In the context of emails, the storage limitation is a severe one. Like all information transmitted over the Internet, emails are split into small packets of data, which skip from machine to machine until they reach their target. At each intermediate stop, each packet is temporarily stored and read before it is forwarded along. Because of this "store and forward" method of transmission, virtually any interception of an email will involve obtaining it from "storage."

The government argued that the Wiretap Act covered any email interception contemporaneous with its transmission, whether it was obtained from "storage" or not. Because Councilman intercepted customers' emails during the transmission of the messages, the government had no difficulty concluding that he violated the Wiretap Act. Essentially, the government argued that only final storage of a completed transmission was beyond the Act's scope, while Councilman argued that communications stored at any point in the process were off limits.

First Circuit Ruling Curtails Wiretap Act Protections

(cont'd from page 1)

Earlier cases examining the question of stored and transiting communications did not provide the *Councilman* court with clear guidance. Some courts had already concluded that stored electronic communications were not covered under the Act, but none of the communications they considered were in transit at the time of interception. Conversely, the First Circuit issued an opinion in 2003 explaining the importance of contemporaneous interception under the Wiretap Act, but it never spoke plainly to the storage issue. In the end, the *Councilman* Court was the first to squarely confront the modern paradox of communications that are simultaneously stored **and** in transit. Finding itself relatively unconstrained by precedent, the Court focused on the Act's definitional language and sided with Councilman.

The import of the *Councilman* decision extends well beyond the facts of the case presented to the Court. Changes made to the Wiretap Act after Councilman's indictment may effectively remove most telephone calls from its protection as well. That is because, in the wake of the September 11 terrorist attacks, the President signed the USA PATRIOT Act, which amended the Wiretap Act in a seemingly innocuous but important way. Among other things, it made the section of the Wiretap Act pertaining to telephone calls more closely mirror the language dealing with email. Consequently, using the logic of *Councilman*, telephone calls that are stored during their transmission are as legally vulnerable to interception as email messages.

One might think that the risk for telephone calls is more theoretical than real, since the Wiretap Act loophole exists only when communications are "stored" during transmission. It is the Internet's "store and forward" protocol that makes email messages vulnerable, and telephone conversations are not generally conducted over the Internet. So why would the USA PATRIOT Act changes have any practical impact? The answer is that telephone companies have undergone a transition from analog to digital technology, and modern telephone networks bear more than a passing resemblance to the Internet. Most telephone calls are conveyed using the same "store and forward" process as email messages, and are consequently stored in telephone company routers along their journey. The dissenting Judge in *Councilman* understood that very well. Complaining about the new approach adopted by the majority, he worried that the government would be essentially free to dispense with wiretap orders, and simply "install taps at telephone company switching stations to monitor phone conversations that are temporarily 'stored' in electronic routers during transmission." The majority conceded this possibility, stating that "It may well be that the protections of the Wiretap Act have been eviscerated as technology advances." At least in First Circuit states, core Wiretap Act protections may now be rendered all but unenforceable, a quaint reminder of a pre-digital world.

Stored communications are not ignored entirely by the federal statutory framework, however. Their privacy is addressed by the aptly-named Stored Communications Act. But its protections are not nearly as robust as those offered by the Wiretap Act. For example, law enforcement authorities seeking information covered by the Stored Communications Act need only obtain a search warrant, while authorities obtaining an order under the Wiretap Act must satisfy much more extensive procedural requirements and submit to ongoing judicial oversight. The Stored Communications Act also has exceptions not found in the Wiretap Act. In the circumstances of the *Councilman* case, the defendant was not charged under the Stored Communications Act because Interloc was entitled to an exception that permits ISPs to examine stored communications on their own systems. Consequently, the shifting of communications from the Wiretap Act to the Stored Communications Act can be truly significant.

TLB Comment: *In April of this year, Google.com was excoriated in the press for introducing an email service in which users knowingly consent to having incoming emails scanned by machine to permit the display of targeted ads.* Councilman*, which received far less press than Google's "Gmail" service, arguably lets email providers scan their users' emails for almost any purpose, without permission. While it remains to be seen whether the logic of* Councilman *will be widely adopted by the other Circuits, and whether the Supreme Court or Congress will ultimately weigh in, there is little doubt that the decision marks a significant point in the jurisprudence of communications privacy. Technology allowed us to think of telephone calls as a substitute for face-to-face conversations, and email as a substitute for traditional letters. The USA PATRIOT Act and decisions such as* Councilman *may soon make the postcard a more apt comparison. As Judge Kermit Lipez wrote in his dissent, "Councilman's approach…would essentially render the Act irrelevant to the protection of wire and electronic privacy. I find it inconceivable that Congress could have intended such a result…." It is a message Judge Lipez clearly hopes is read widely. Maybe he should put it in an email.*

Granting Employees Stock under Federal and State Securities Law

Peter Moldave
peter.moldave@gesmer.com

Recently, Google offered to buy back shares of employee-held stock because the shares may have been issued in violation of federal and state securities rules.

Private companies sometimes consider securities law compliance issues only when they are seeking investor funds. However, every issuance or promise to issue securities involves federal or state securities laws. Many times, compliance is either automatic (requiring no filing or other act) or relatively simple, so long as the issuances remain within certain limits. Private companies should ensure that they monitor employee stock and option issuances for compliance with securities laws, under both federal and state law.

Federal Law. Does the issuance have to be registered with the Securities and Exchange Commission? Under federal securities law, compensatory issuances of securities to employees and consultants are permitted without registration under Rule 701 so long as:

- The issuances are to qualifying individuals – generally, employees and qualifying consultants who are natural persons. Rule 701 does not exempt issuing shares to companies, or to non-employees who help in fund raising.

- The amount of securities issued is less than one of several limits, during any 12-month period. Relevant limits for early-stage companies are usually: (1) the aggregate sale price of shares granted cannot exceed $1,000,000; or (2) the number of shares granted cannot exceed 15% of the outstanding common stock (including any preferred stock on an as-converted basis).

The Rule 701 limits cover both the issuance of stock and stock options – and verifying compliance with both is somewhat complicated. This is part of the reason why a formal compliance program is important.

In the event the Rule 701 limits are reached, other exemptions under federal securities law may be available, but their use is often not optimal for other reasons. Ultimately, if no other exemptions are available, issuances to employees and others may need to be registered with the SEC.

State Law. The laws in each state in which a recipient of stock or stock options resides must be considered (in addition to the laws of the state where the company is located and where it is incorporated, if different). Many states exempt issuances if they are exempt under federal law. Some, notably New York, require pre-issuance filings with state regulators. Others, notably California, have substantive rules on the terms of options and grants to employees and consultants, such as required minimum vesting schedules and pricing terms. In general, before any issuance to residents of a new state, the state's laws need to be reviewed.

Reporting and Other Requirements. Under both federal and some state laws, stock and option holders have the right to periodically receive basic financial information. In addition, stockholders have certain basic rights (regardless of how they obtained their shares) under state law.

Consequences of Non-Compliance. One result of non-compliance is the right of a holder to rescission. In general, this would involved repayment by the company of any amounts paid for acquisition of the shares. Although in many cases these amounts may be nominal, this is not always the case (examples include grants to senior executives, which could be substantial). The rescission demand could also come at a time (unlike the Google public offering) in which the company's prospects are much less clear, and cash demands could then be material.

In addition, although not yet an issue for Google at the time of this article, there is always the possibility of state or federal enforcement actions against the company or those individuals responsible for the failure to comply.

Finally, the process involved in securities law compliance also serves as an opportunity to confirm the accuracy and availability of stock records, which are important to maintain for other purposes.

GESMER UPDEGROVE LLP
Attorneys At Law

Gesmer Updegrove LLP
40 Broad Street
Boston, MA 02109

Return Service Requested

GU Events & Announcements

EVENTS

September 29, 2004. Ken Appleby will be a presenter at a seminar entitled "Advanced Partnerships, LLCs and LLPs: Organization and Operation in Massachusetts" sponsored by Lorman Education Services in Boston, MA. His presentation will focus on advanced issues in the area of partnership taxation.

October 18, 2004. Andrew Updegrove will be a speaker at the Annual Meeting of the Licensing Executives Society (USA and Canada). Andy's topic will be "From Life Sciences to Telecom: What you Need to Know About Standard Setting Organizations and Consortia."

October 26, 2004. Ken Appleby will be the guest speaker at a seminar entitled "Three Challenges Facing Non-Profit Organizations: Fundraising, Investment Policy Development & Asset Management" sponsored by Smith Barney in Newton, MA.

ANNOUNCEMENTS

August 17, 2004. Andrew Updegrove was a speaker in Ottawa, Ontario, at the Annual Meeting of the Standards Engineering Society. Andy's topic was called "Standards Trends of the Future."

September 1, 2004. Lee Gesmer has been named as the co-chair of the Boston Bar Association Computer & Internet Law Committee.

September 1, 2004. Patrick R. Jones was elected to the Board of Directors of the WPI Venture Forum.

September 14, 2004. Andrew Updegrove was the wrap-up speaker at the "Open Source – Open Standards" conference in Scottsdale, Arizona. The conference was organized and sponsored by leading open source organizations and vendors.

September 16, 2004. Andrew Updegrove was a speaker in Washington, D.C. at a conference organized by the U.S. Chamber of Commerce. The conference is entitled "The Future of Standards Setting – Legal, Marketplace, and Consumer Implications." Andy's topic was: "Will Clearer Rules in Standards Setting Solve all Problems?"