Legal Backgrounder

WLF Washington Legal Foundation

Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Vol. 21 No. 28 September 1, 2006

# COURT REFUSES TO ENFORCE DISCOVERY SUBPOENA AGAINST E-MAIL SERVICE PROVIDER

By

Jeffrey D. Neuburger and Maureen E. Garde

Are electronic records maintained by an electronic communications service provider fair game for discovery in civil litigation? In *O'Grady v. The Superior Court (Apple Computer, Inc.)*[1], a California state appeals court quashed a civil subpoena seeking e-mail records from an e-mail service provider, citing provisions of the federal Stored Communications Act that prohibit service providers from disclosing the contents of stored electronic communications.[2] The ruling is controversial because it appears to be the first time, in the twenty years since the enactment of the SCA in 1986, that a court has held that the Act prohibits civil litigants from obtaining discovery of electronic communications from providers of e-mail and other electronic communications services, even when a court has reviewed and approved the subpoena.

The issue was raised during Apple Computer's highly publicized effort to learn the identity of the anonymous individuals who were responsible for leaking the company's confidential new product information to Web site operators who ultimately posted it publicly on the Internet. Apple filed a "John Doe" suit against the anonymous leakers and then proceeded to seek discovery that might reveal their identities.[3] Apple obtained an order giving it the authority to subpoena documents, both from the Web sites that posted the confidential information and from their hosting and e-mail providers. The operators of the Web sites, who were not named parties in the underlying litigation, then moved for a protective order claiming, among other things, that the subpoenas to their e-mail service providers violated the

[1] *O'Grady v. The Superior Court of Santa Clara County (Apple Computer, Inc.)*, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 (Ct. App, 6th Dist. 2006).

[2] 18 U.S.C. §§ 2701-2712. These provisions are commonly referred to as the "Stored Communications Act," or the "SCA," and will be referred to as such in this article. The longer and more formal title in the United States Code is the "Stored Wire and Electronic Communications and Transactional Records Access" statute, and less formally the provisions are sometimes referred to as the "stored communications provisions of the Electronic Communications Privacy Act."

[3] Presumably, at least one of the leakers (or the only leaker) was an Apple employee. Apple asserted that its own internal investigation had failed to reveal the source of the leak.

**Jeffrey D. Neuburger** is a partner in the New York office of Brown Raysman Millstein Felder & Steiner LLP and is the Chair of the firm's Technology, Media and Communications Practice Group. **Maureen E. Garde** is an associate at the firm and member of that practice group.

Stored Communications Act. Although Apple prevailed in the trial court, the appellate court held in a sweeping ruling that the SCA prohibits the use of third-party civil subpoenas to obtain discovery of electronic communications from e-mail service providers.

The court's ruling on the SCA, coupled with its contemporaneous (and much more widely reported) ruling that the Web sites themselves are protected from civil discovery order by the California reporter's privilege, effectively insulated the anonymous leakers from Apple's efforts to obtain their identity through civil process.[4]

Despite the court's ruling, it is not obvious from either the language or the legislative history of the SCA that it was specifically intended to prohibit private parties from using civil subpoenas to obtain discovery of electronic communications from providers of electronic communications services.

The SCA was enacted in 1986, as part of the Electronic Communications Privacy Act.[5] As a general proposition, the ECPA was enacted to deal with concerns about how the technical aspects of electronic communications affect their status under the search and seizure provisions of the Fourth Amendment.[6] Thus, the SCA, as enacted and as amended several times, places express and extensive, "Fourth Amendment-like" limitations on the ability of government entities to access electronic communications stored by electronic communications service providers. [7]

But does the SCA limit only *government* access to such electronic communications? In ruling that the Act also prohibits private parties from obtaining access to electronic communications as part of court-supervised civil discovery, the court in *O'Grady* looked to the literal language of 18 U.S.C. §§ 2701 and 2702. Section 2701 provides in relevant part that "whoever" intentionally accesses an electronic communications facility and thereby obtains an electronic communication while it is in storage "shall be punished," unless the access falls within one of the enumerated exceptions in the Act. Section 2702 provides that an electronic communications provider "shall not knowingly divulge" the contents of electronic communications. The court concluded that in enacting the SCA, Congress not only sought to protect electronic communications from unwarranted government access, but also sought "to encourage 'innovative forms' of communication by granting them protection against unwanted disclosure *to anyone.*"[8]

None of the enumerated exceptions in the SCA unequivocally applies to a third-party civil subpoena, and neither the parties to the litigation nor any of the entities who filed "friend of the court"

---

[4]*See, e.g.*, Reporters Committee for Freedom of the Press, *Court applies reporter's privilege to Web site operator*, (May 30, 2006), http://www.rcfp.org/news/2006/0530-con-courta.html (last visited July 7, 2006).

[5]*See* Pub. L. 99- 508, 100 Stat.1848 (codified as amended in scattered sections of 18 U.S.C.).

[6]It had been speculated, for example, that because e-mail messages can be readily accessed as they pass through or are stored on the systems and networks of service providers, an individual has a lower expectation of privacy in those messages when they are in the hands of providers. That lower expectation of privacy might enable government entities to obtain access to such communications on a showing of less than Fourth Amendment probable cause. *See, e.g.*, Computer Crime & Intellectual Property Section, U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, III. The Electronic Communications Privacy Act, A. Introduction (2002), available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (last visited July 14, 2006).

[7]Orin S. Kerr, *A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It*, 72 GEORGE WASHINGTON L. REV., 1208, 1209-1219 (2004).

[8]139 Cal. App. 4th. at 1445 (emphasis in the original).

  ISBN 1056 3059

briefs discussing the issue were able to point to any legislative history that discussed the applicability of the SCA to civil discovery.[9] Thus, Apple was forced to argue a series of alternative theories, none of which was accepted by the court. Among other things, the court rejected the argument that an exception for civil discovery could be implied from 18 U.S.C. § 2707, which affords a service provider a complete defense to a violation of the statute where the provider allows a third party to have access to electronic communications in good faith reliance on a "court warrant or order." The court concluded that the existence of this "safe harbor" was intended to protect service providers who might be forced to choose between complying with "seemingly valid coercive process" and potential liability under the Act; the court commented that this exception "does not make compliance with such process lawful."[10] More generally, the court held that the broad language prohibiting access to electronic communications is not limited to government officials, and thus rejected the argument that there is an "implied exception" to the SCA for civil discovery.[11]

Prior to the decision in *O'Grady*, no court had held that the SCA completely prohibits this kind of civil discovery of e-mail or other stored communications. On the contrary, although in several reported cases, courts quashed civil discovery subpoenas directed to e-mail service providers – none appear to have been quashed on the broad, general principle that such subpoenas are prohibited completely by the SCA. For example, in *Theofel v. Farey-Jones*, the U.S. Court of Appeals for the Ninth Circuit quashed a civil subpoena issued to an e-mail service provider because the subpoena was overbroad.[12] Apple proffered the case as implicitly supporting the proposition that a narrowly drawn third-party civil subpoena is permissible under the SCA, but the California court summarily dismissed *Theofel v. Farey-Jones* with the comment that the federal court had simply disposed of the case on "a less difficult ground of decision."[13] In *Doe v. 2TheMart.com, Inc.*[14], an analogous case involving anonymous Internet communications via a Web site bulletin board, the federal District Court in Washington quashed a civil subpoena directed to a service provider because the party seeking the identity of the anonymous posters on the bulletin board had failed to meet the high standard required to overcome the posters' First Amendment right to anonymity. There was no suggestion in *Doe v. 2TheMart.com, Inc.*, that the subpoena (which sought access to stored electronic communications)[15] was facially invalid under the SCA.

For now, the ruling in *O'Grady* will stand as precedent, at least in California state courts, as

---

[9]The case attracted the attention of trade groups such as the Information Technology Industry Council and the Business Software Alliance, who filed briefs in support of Apple, and the U.S. Internet Industry Association and the Netcoalition, who supported the Web site operators.

[10]139 Cal. App. 4th at 1442.

[11]139 Cal. App. 4th at 1442-48.

[12]*Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004). *See also Quinby v. WestLB AG*, 2006 U.S.Dist. LEXIS 1178 (S.D. N.Y. Jan. 11, 2006) (quashing a civil discovery subpoena directed to a party's e-mail service provider on the grounds of overbreadth).

[13]139 Cal. App. 4th at 1443 n.11.

[14]*Doe v. 2TheMart.com, Inc.*, 140 F. Supp. 2d (W.D. Wash. 2001).

[15]That material stored on an Internet Web site may constitute "electronic communications" within the meaning of the Stored Communications Act is supported by the Ninth Circuit opinion in *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003) (a Web site constitutes an "electronic communications service" and the contents of the Web site are in "electronic storage" within the meaning of the SCA).

Apple has indicated that it will not pursue an appeal.[16] Whether the *O'Grady* opinion will be followed by other courts in similar cases is uncertain. Despite the court's suggestion that the language of the SCA is clear, the Act and its related statutes, the federal Wiretap Act and the Electronic Communications Privacy Act are generally recognized to be notoriously complex and difficult statutes to understand and construe, and frequently generate conflicting court opinions.[17]

The potential impact of the decision is also uncertain. In the case of a civil subpoena directed to the electronic communications provider of a known party litigant or even a known non-party, a court might look to the consent exception to the statute[18] and order a party to consent to the disclosure of electronic communications by a service provider, if the court determined that the applicable rules governing the scope and manner of civil discovery were otherwise met.[19] Thus, the application of the decision may be relatively limited, for example, to cases such as the Apple litigation involving as-yet unidentified "John Doe" parties. While this may be a small set of cases relative to all civil litigation, it is an important set of cases to the trade secret owners and other plaintiffs, such as parties trying to track down phishers and other scammers,[20] who are seeking redress from the online activities of anonymous wrongdoers.

[16] *See* Declan McCullagh, *Apple abandons effort to unmask leaker* (CNET News.com July 12, 2006).

[17] *See, e.g., United States v. Councilman*, 418 F.3d 67, 80 (1st Cir. 2005) (en banc) & *id.* at 89-90 (dissenting opinion) (both opinions referring to the difficulty of interpretation of these statutes).

[18] 18 U.S.C. § 2702 permits disclosure of electronic communications with the consent of the originator, an addressee or an intended recipient of the communication.

[19] *See, e.g., Federal Trade Commission v. Ameridebt*, No. 3:05-mc-80253 (N.D. Cal. Dec. 14, 2005) (unpublished) (court ordered non-party to execute consent document requested by e-mail provider in response to subpoena, where relevance requirements of FED. R. CIV. P. 26 were met, and non-party was provided procedure for raising privilege objections to production of specific e-mails); stay pending appeal denied 2006 U.S. Dist. LEXIS 13687 (Mar. 13, 2006).

[20] *See, e.g., First National Bank of Nebraska v. John Does 1-5*, 8:06-cv-00504, 2006 U.S. Dist. LEXIS 53881 (D. Neb. July 26, 2006) (granting ex parte motion for expedited third-party discovery addressed to providers of e-mail, Web hosting and other services, to obtain information identifying parties responsible for bank phishing scam).

  ISBN 1056 3059