IADC Committee Newsletter

BUSINESS LITIGATION

January 2012

IN THIS ISSUE

The authors report on the fundamentals of how to seek formal written discovery of various types of electronic communication in the ever changing forms of communicating on the web, and other internet-based and mobile communications. This is a useful summary and guide to discovery of electronic communications such as Facebook, Myspace, Google Chat and Twitter.

Behind the Privacy Veil, What E-Discovery Are You Entitled To and Developing Useful Strategies When Faced With Propounding Discovery for Essential Electronic Communications

ABOUT THE AUTHORS

Tim A. Agajanian is a Partner in the Los Angeles office of Murchison & Cumming, LLP. Mr. Agajanian serves as Co-Chair of the firm's Business Litigation practice group and Chair of the Toxic Tort & Environmental practice group. Mr. Agajanian is a Martindale-Hubbell AV-rated attorney. He can be reached at tagajanian@murchisonlaw.com.

Mhare O. Mouradian is a Senior Associate in the Los Angeles office of Murchison & Cumming, LLP, where he focuses his practice in the areas of complex civil litigation and business litigation. Mr. Mouradian is a Martindale-Hubbell AV-rated attorney and a recent graduate of the IADC's Trial Academy at Stanford Law School. He can be reached at MMouradian@murchisonlaw.com.

Friedrich W. Seitz serves as Chair of Murchison & Cumming, LLP's Wildland Fire Litigation practice group, and Co-Chair of the firm's Business Litigation, Product Liability/Utilities and International Law practice groups. A respected trial lawyer and member of the IADC, Mr. Seitz is also a member of the Los Angeles Chapter of the American Board of Trial Advocates, Advocate rank, and FDCC.

ABOUT THE COMMITTEE

The Business Litigation Committee consists of members involved in business and commercial litigation including business torts, contract and other commercial disputes, e-commerce, antitrust issues, trade secrets and intellectual property, unfair competition and business defamation and disparagement. The Business Litigation Committee helps connect members involved in these areas around the world through networking and referral opportunities; developing and keeping current in the substantive, strategic and procedural aspects of business litigation; and affords members an international forum for sharing current developments and strategies with colleagues. In addition, the Business Litigation committee has formed an IP subcommittee to intently focus on issues important to IP litigators. Among the committee's and subcommittee's planned activities are newsletters, publications, sponsorship of internal CLEs, and Webinars. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Jennifer P. Henry
Vice Chair of Publications
Thompson & Knight LLP
(817) 347-1733
jennifer.henry@tklaw.com

This article serves as an overview of the Stored Communications Act, 18 U.S.C.S. § 2701 et seq. ("SCA") and illustrates the fundamentals of developing strategies on how to successfully pursue discovery of electronic communications via internet service providers and/or social media companies. With the increased popularity of communication via email and social media websites like Facebook, the courts are being forced to apply the SCA to current technology more than ever. The SCA was enacted by Congress in 1986 before the advent of the World Wide Web in 1990, before the introduction of the web browser in 1994, and many years before companies like Yahoo!, Google, Facebook, and MySpace were founded. The SCA is celebrating its twenty-five year anniversary, but has not been amended to keep up with current technologies. "Despite the rapid evolution of computer and networking technology since the SCA's adoption, its language has remained surprisingly static. The resulting task of adapting the Act's language to modern technology has fallen largely upon the courts." *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 972 (C.D. Cal. 2010) (citing William Jeremy Robison, Note, Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act, 98 GEO. L.J. 1195, 1196 (2010)).

I. Overview of the Stored Communications Act

Congress passed the Stored Communications Act (SCA), 18 U.S.C.S. § 2701 et seq., in 1986 as part of the Electronic Communications Privacy Act. The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address. The SCA prevents "providers" of communication services from divulging private communications to certain entities and individuals. It creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information. First, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers. 18 U.S.C.S. § 2703. Although the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute confers greater privacy protection. Second, the statute limits the right of an Internet Service Provider to disclose information about customers and subscribers to the government voluntarily. 18 U.S.C.S. § 2702. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 971-972 (C.D. Cal. 2010).

II. How Does the Stored Communications Act Apply?

The SCA distinguishes between an electronic communication service (ECS)[1] provider and a remote computing service (RCS)[2] provider, establishing different standards of care for each. With certain enumerated exceptions, it prohibits an ECS provider from knowingly divulging to any person or entity the contents of a communication while in electronic

[1] The SCA defines an ECS provider as any service which provides to its users the ability to send or receive wire or electronic communications. 18 U.S.C.S. § 2510(15).

[2] The SCA defines RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system," 18 U.S.C.S. § 2711(2), and in turn defines an electronic communications system (as opposed to an electronic communication service) as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.*, § 2510(14).

storage by that service. 18 U.S.C.S. § 2702(a)(1), (b); *Crispin*, 717 F. Supp. 2d_at 972-973. With certain enumerated exceptions, it prohibits an ECS provider from knowingly divulging to any person or entity the contents of a communication while in electronic storage by that service. 18 U.S.C.S. § 2702(a)(1), (b). "Electronic storage" is "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C.S. § 2510(17). *Crispin*, 717 F. Supp. 2d. at 973. Email services such as Microsoft's Hotmail, Google's Gmail and social media services which provide one-to-one private messaging or with a large group of friends through wall postings and comments such as Facebook and MySpace have been held to constitute ECS. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 982 (C.D. Cal. 2010).

The SCA prohibits an RCS provider from "knowingly divulging to any person or entity the contents of any communication which is carried or maintained on that service." 18 U.S.C.S. § 2702(a)(2). "[A] person who does not provide an electronic communication service [or a remote communication service] can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage." *Wesley College v. Pitts*, 974 F.Supp. 375, 389 (D. Del. 1997) (citing 18 U.S.C. § 2702(a)). An archive of a text messaging pager service falls into this category. An airline's online reservations system was held that it would not fall under this category. *In re Jetblue Airways Corp. Prvacy Litigation*, 379 F.Supp.2d 299, 310 (E.D.N.Y. 2005). Also, an ECS provide becomes an RCS provider after a communication has been read and stored. *United States v. Weaver*, 636 F.Supp.2d 769, 770 (C.D. Ill. 2009) concluding that Microsoft, which provided email service through the Hotmail website, was both an ECS provider and an RCS provider).

In contrast to an ECS provider, an RCS provider may not divulge the content of any communication received by electronic transmission that is carried or maintained on its service for a customer or subscriber solely for the purpose of providing storage or computer processing services if the provider is not authorized to access the contents of the communications for purposes of providing services other than storage or computer processing. 18 U.S.C.S. § 2702(a)(2).

III. How Does the Stored Communications Act Affect Civil Discovery?

Ordinarily a party has no standing to seek to quash a subpoena issued to someone who is not a party to the action, unless the objecting party claims some personal right or privilege with regard to the documents sought. As a general matter, a party lacks standing under Fed. R. Civ. P. 45(c)(3) to challenge a subpoena issued to a non-party unless the party claims a personal right or privilege with respect to the documents requested in the subpoena. *Id.* At least two district courts have concluded that individuals have standing to move to quash a subpoena seeking personal information protected by the SCA. In *J.T. Shannon Lumber Co., Inc. v. Gilco Lumber, Inc.*, 2008 U.S. Dist. LEXIS 104966, 3-4 (N.D. Miss. Aug. 14, 2008), the court found that because the documents sought by the plaintiff were the personal documents and details of the email accounts of the defendant employees, the defendants had standing to seek to quash the subpoena as they had a

personal interest in the documents sought from the internet service provider. The U.S. District Court for the Central District of California, in *Crispin*, finds *J.T. Shannon Lumber* persuasive. Specifically, a Central District of California court concluded that an individual has a personal right in information in his or her profile and inbox on a social networking site, and in his or her webmail inbox, in the same way that an individual has a personal right in employment and bank records. As with bank and employment records, this personal right is sufficient to confer standing to move to quash a subpoena seeking such information. *Id.*

The SCA establishes a complex scheme pursuant to which a governmental entity can, after fulfilling certain procedural and notice requirements, obtain information from a remote computing service via administrative subpoena, or a grand jury or trial subpoena. 18 U.S.C.S. § 2703(b). It permits a governmental entity to obtain information from an ECS provider only pursuant to criminal warrant if the communication has been held by the provider for fewer than 180 days. In all other cases, the governmental entity can obtain information from an ECS provider using the subpoena procedures set forth in § 2703(b). 18 U.S.C.S. § 2703(a). The statute does not mention service of a civil subpoena duces tecum. *Crispin*, 717 F. Supp. 2d at 974-975.

Among the most significant, although unstated, privacy protections of the SCA is the ability to prevent a third party from using a subpoena in a civil case to get a user's stored communications or data directly from an electronic communication service provider or a remote computing service provider. Courts interpret the absence of a provision in the SCA for compelled third-party disclosure to be an intentional omission reflecting Congress's desire to protect users' data in the possession of a third-party provider from the reach of private litigants. Without this blanket immunity from subpoena in civil cases, a user's entire portfolio of stored communications and data might be fair game for an adversary. *Id at 975.*

The Ninth Circuit has noted that "storage" for purposes of the SCA, was equivalent to a virtual filing cabinet. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 902 (9th Cir. 2008). The Ninth Circuit has also concluded that providers of e-mail services are undisputedly an ECS provider under the SCA. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004). Computer bulletin boards generally offer both private electronic mail services and newsgroups. The latter is essentially email directed to the community at large, rather than a private recipient. The term "computer bulletin board" evokes the traditional cork-and-pin bulletin board on which people post messages, advertisements, or community news. Court precedent and legislative history establish that the definition of an ECS provider under the SCA was intended to reach a private electronic bulletin board service (BBS). Unquestionably, BBS is to be restricted in some fashion; a completely public BBS does not merit protection under the SCA. Only electronic bulletin boards which are not readily accessible to the public are protected under the SCA. *Crispin*, 717 F. Supp. 2d *at 981.*

A. Is a Person's Social Media Account Such as Facebook Discoverable in Civil Cases?

A Central District of California U.S. District Court was faced with the issue of whether a party could subpoena someone's Facebook page. In *Crispin*, plaintiff Buckley Crispin filed an action against famous fashion

designer Christian Audigier, Christian Audigier, Inc. and their various sublicensees for breach of contract, direct, contributory and vicarious copyright infringement, breach of implied covenant of good faith and fair dealing, and declaration of rights as to artwork and constructive trust. Crispin alleged that he licensed fifteen works to defendants to use in a limited manner in connection with the manufacture of certain types of garments. The agreement required the defendants to include the Crispin logo in exchange for compensation. Crispin alleged that defendants failed to not only include his logo, but at times attributed the artwork to another artist or to Audigier himself. The defendants served subpoenas duces tecum on social networking websites including Facebook and MySpace that sought plaintiff's basic subscriber information as well as communications between plaintiff and a tattoo artist and all communications that referred or related to defendants Christian Audigier, Christian Audigier, Inc., the Ed Hardy brand, or any of the sublicensee defendants. *Crispin*,717 F. Supp. 2d at 968-969. Christian Audigier and Christian Audigier, Inc. contended that the information they sought in the subpoenas were relevant in determining the nature and terms of their agreement with Crispin.

Plaintiff filed a motion to quash defendants' subpoenas. A magistrate judge denied plaintiff's motion and held that plaintiff was not entitled to quash the subpoenas served by defendants. Plaintiff filed a motion for reconsideration of the magistrate judge's decision. The parties submitted a Joint Stipulation stating that Facebook and MySpace, Inc. are companies that provide social networking websites which allow users to send and receive messages through user-created profile pages or through private messaging services. The *Crispin* court's analysis included a determination of whether the information sought by the subpoenas – private messages and postings – constituted electronic storage within the meaning of the SCA.

The SCA provides two definitions of electronic storage. One definition includes any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof. 18 U.S.C.S. § 2510(17)(A). A second definition of "electronic storage" includes any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C.S. § 2510(17)(B).

The *Crispin* court concluded that Facebook and MySpace were both ECS and RCS providers in relation to wall postings and comments which were also found to constitute electronic storage within the meaning of the SCA. The Court granted plaintiff's motion for reconsideration, reversed the magistrate's order, and quashed the defendants' subpoenas with respect to the portions seeking private messages from Facebook and MySpace. The Court remanded for reconsideration the portions of the subpoenas that sought wall postings and comments because it did not have enough information regarding the privacy settings of plaintiff's Facebook and MySpace accounts.

In a recent personal injury case, a Pennsylvania court ordered a plaintiff to turn over her Facebook password to defendant. *Largent v. Reed*, 2009-1823 (Pa. Ct. of Common Please; Nov. 8, 2011). Defendant contended that certain posts to plaintiff's Facebook account contradicted her claims of "serious and severe injury," including pictures posted of her enjoying life with her family and status updates regarding going to the

gym. The *Largent* court distinguished the *Crispin* case on the basis that in *Crispin* the information was sought directly from Facebook, and in *Largent* the information was sought directly from plaintiff who was the account holder. Defendant had 21 days to inspect plaintiff's Facebook account, and then plaintiff could change her password. There are several other cases where the Court ordered a party to turn over their Facebook passwords. *See Zimmerman v. Weis Markets, Inc.*, CV-09-1535 (Pa. Ct. Common Pleas; May 19, 2011); *See also McMillen v. Hummingbird Speedway, Inc., et al.*, Case No. 113-200 CD (Pa. Ct. of Common Please) (Sept. 9, 2010). Therefore it appears that a party's best chance in obtaining social media postings are directly from the opposing party rather than subpoenaing the third party Social Media entity such as Facebook or MySpace. Of course a completely public Bulletin Board Service such as Facebook or MySpace does not merit protection under the SCA. *(See Kaufman v. Nest Seekers, LLC*, 2006 U.S. Dist. LEXIS 71104 (S.D.N.Y. Sept. 26, 2006).

B. Are a Person's Emails from Internet Service Providers Discoverable in Civil Cases?

In May 2006, the Court of Appeal of California considered the issue of whether a subpoena to an email service provider could not be enforced because of the SCA in *O'Grady v. Superior Court*, 130 Cal. App. 4th 1423 (2006). Apple Computer, Inc. (Apple), brought an action alleging that unknown persons caused the wrongful publication of Apple's secret plans to release a device that would facilitate the creation of digital live sound recordings on Apple computers on the internet. In an effort to identify the source of the disclosures, Apple sought and obtained authority to issue civil subpoenas to the publishers of the websites where the information appeared and to the e-mail service provider for one of the publishers. The publishers moved for a protective order to prevent any such discovery. The trial court denied the motion on the ground that the publishers had involved themselves in the unlawful misappropriation of a trade secret. The court held that this was an error because (1) the subpoena to the e-mail service provider cannot be enforced consistent with the plain terms of the federal Stored Communications Act (18 U.S.C. §§ 2701–2712); (2) any subpoenas seeking unpublished information from petitioners would be unenforceable through contempt proceedings in light of the California reporter's shield (Cal. Const., art. I, § 2, subd. (b); Evid. Code, § 1070); and (3) discovery of petitioners' sources is also barred on this record by the conditional constitutional privilege against compulsory disclosure of confidential sources (*see Mitchell v. Superior Court* (1984) 37 Cal.3d 268 [208 Cal. Rptr. 152, 690 P.2d 625] (Mitchell)). The court issued a writ of mandate directing the trial court to grant the motion for a protective order. *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1431-1432 (Cal. App. 6th Dist. 2006).

The *O'Grady* court specified that the SCA does not authorize the disclosure of the identity of the author of a stored message; it authorizes the disclosure of a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications). 18 U.S.C. § 2703(c)(1). A party seeking to identify the sender of communications to the subscriber, or the addressee of communications from the subscriber, steps well outside the statutory authorization. *O'Grady*,139 Cal. App. 4th at 1434. Therefore, pursuant to *O'Grady*, records or information pertaining to a

subscriber to or customer of such a service (not including contents of communications) is discoverable. Although not specified by the *O'Grady* court, this may include information such as email headers and subscriber information. The *O'Grady* court also concluded that the SCA enumerates several exceptions to the rule that service providers may not disclose the contents of stored messages. Among the disclosures authorized are those that are incidental to the provision of the intended service (see 18 U.S.C. § 2702(b)(1), (4), (5)); incidental to the protection of the rights or property of the service provider (18 U.S.C. § 2702(b)(5)); made with the consent of a party to the communication or, in some cases, the consent of the subscriber (see 18 U.S.C. § 2702(b)(3)); related to child abuse (18 U.S.C. § 2702(b)(6)); made to public agents or entities under certain conditions (18 U.S.C. § 2702(b)(7), (8)); related to authorized wiretaps (18 U.S.C §§ 2702(b)(2), 2517, 2511(2)(a)(ii)); or made in compliance with certain criminal or administrative subpoenas issued in compliance with federal procedures (18 U.S.C. §§ 2702(b)(2), 2703)) *O'Grady*, 139 Cal. App. 4th at 1441. Further, the SCA does not authorize the disclosure of the identity of the author of a stored message; it authorizes the disclosure of "a record or other information pertaining to *a subscriber to or customer of such service* (not including the contents of communications) … ." (18 U.S.C. § 2703(c)(1), italics added.) The Court of Appeal reasoned that Apple already knew the identities of the subscribers and that by seeking to identify the sender of communications to the subscriber, or the addressee of communications from the subscriber, Apple stepped well outside the statutory authorization.

In April 2008, the Eastern District of Virginia, U.S. District Court considered the issue whether a magistrate clearly erred by granting State Farm Fire & Casualty Company's Motion to Quash. *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606 (E.D. Va. 2008). State Farm Fire & Casualty Company's civil subpoena requested: (1) production of their e-mails from the communications company, (2) all of one of the adjuster's e-mails from a six-week period, and (3) information relevant to McIntosh, subject to the their attorney-client privilege claims. The court upheld the magistrate's decision quashing the subpoena, and held that it was not clearly erroneous for the following reasons: (1) the SCA prohibited the communications company from producing the e-mails in response to the subpoena because a civil discovery subpoena was not a disclosure exception under the SCA, (2) the subpoena imposed an undue burden because it was overbroad and the documents requested were not limited to subject matter relevant to the claims or defenses in McIntosh, and (3) the Southern District of Mississippi was better suited to decide whether the information relevant to McIntosh was privileged because no action was pending in the instant court. *Id*.

IV. Conclusion

In conclusion, lawyers should be very careful when conducting civil discovery to obtain electronic communications. Based on the breadth of case law on the SCA, it appears the best way to obtain electronic communications is directly from the opposing party. When lawyers are forced to subpoenaing electronic communications from third parties such as internet service providers and social media, the scope of the subpoena needs to comply with the SCA and all that you may be entitled to are records or information pertaining to a subscriber to or customer of such a service (not including contents of communications).

PAST COMMITTEE NEWSLETTERS

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

NOVEMBER 2011
Insider Trading Regulations in Taiwan: A Remark on Recent Developments
Edgar Y. Chen and Ya-Wen Yang

SEPTEMBER 2011
Federal Arbitration Act Overcomes State Law Obstacle
John T. Lay

JUNE 2010
Shady Grove and CAFA: Opening the Federal Door for Class Actions Barred by States
John T. Lay and Shaun C. Blake

MAY 2010
Spoliation of Evidence – Contemporary Status and Trends
Stephen L. Cotter and Pamela N. Lee

DECEMBER 2009 (Business Litigation and Alternative Dispute Resolution Joint Newsletter)
5 Things You Always Wanted to Know about Arbitration: Five Issues Recently Decided by the Courts
Scott D. Marrs and Sean P. Milligan

NOVEMBER 2009
Are You Able to Disregard "Manifest Disregard" After *Hall Street*: A Continuing and Twisted Tale
Keith A. Dotseth and Hilary J. Loynes

OCTOBER 2009
Standard of Review and Discovery after *Glenn*: The Effect of the *Glenn* Standard of Review on the Role of Discovery in Cases Involving Conflicts of Interest
Elizabeth J. Bondurant

MARCH 2009
Plausibility Pleadings: How the United Supreme Court with *Bell Atlantic Corporation v. Twombly* and *Erickson v. Pardus*, Energized Rule 12(b)(6) and Changed the Playbook in all Civil Cases
Pat Long Weaver