United States Code Annotated
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes (Refs & Annos)
Chapter 121. Stored Wire and Electronic Communications and Transactional Records Access (Refs & Annos)

18 U.S.C.A. § 2701

§ 2701. Unlawful access to stored communications

Currentness

(a) Offense.--Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.--The punishment for an offense under subsection (a) of this section is--

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case--

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

CREDIT(S)

(Added Pub.L. 99-508, Title II, § 201[a], Oct. 21, 1986, 100 Stat. 1860; amended Pub.L. 103-322, Title XXXIII, § 330016(1)(K), (U), Sept. 13, 1994, 108 Stat. 2147, 2148; Pub.L. 104-294, Title VI, § 601(a)(3), Oct. 11, 1996, 110 Stat. 3498; Pub.L. 107-296, Title II, § 225(j)(2), Nov. 25, 2002, 116 Stat. 2158.)

Notes of Decisions (64)

18 U.S.C.A. § 2701, 18 USCA § 2701
Current through P.L. 114-61 (excluding P.L. 114-52, 114-54, 114-59, and 114-60) approved 10-7-2015

End of Document

KeyCite Yellow Flag - Negative Treatment
Proposed Legislation

United States Code Annotated
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes (Refs & Annos)
Chapter 121. Stored Wire and Electronic Communications and Transactional Records Access (Refs & Annos)

18 U.S.C.A. § 2702

§ 2702. Voluntary disclosure of customer communications or records

Effective: June 2, 2015
Currentness

(a) Prohibitions.--Except as provided in subsection (b) or (c)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[**(B)** Repealed. Pub.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) Reporting of emergency disclosures.--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8);

(2) a summary of the basis for disclosure in those instances where--

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges; and

(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).

CREDIT(S)

(Added Pub.L. 99-508, Title II, § 201[a], Oct. 21, 1986, 100 Stat. 1860; amended Pub.L. 100-690, Title VII, § 7037, Nov. 18, 1988, 102 Stat. 4399; Pub.L. 105-314, Title VI, § 604(b), Oct. 30, 1998, 112 Stat. 2984; Pub.L. 107-56, Title II, § 212(a)(1), Oct. 26, 2001, 115 Stat. 284; Pub.L. 107-296, Title II, § 225(d)(1), Nov. 25, 2002, 116 Stat. 2157; Pub.L. 108-21, Title V, § 508(b), Apr. 30, 2003, 117 Stat. 684; Pub.L. 109-177, Title I, § 107(a), (b)(1), (c), Mar. 9, 2006, 120 Stat. 202, 203; Pub.L. 110-401, Title V, § 501(b)(2), Oct. 13, 2008, 122 Stat. 4251; Pub.L. 114-23, Title VI, § 602(d), June 2, 2015, 129 Stat. 295.)

Notes of Decisions (19)

18 U.S.C.A. § 2702, 18 USCA § 2702
Current through P.L. 114-61 (excluding P.L. 114-52, 114-54, 114-59, and 114-60) approved 10-7-2015

End of Document

United States Code Annotated
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes (Refs & Annos)
Chapter 121. Stored Wire and Electronic Communications and Transactional Records Access (Refs & Annos)

18 U.S.C.A. § 2707

§ 2707. Civil action

Effective: November 2, 2002
Currentness

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) Defense.--A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper disclosure.--Any willful disclosure of a "record", as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

CREDIT(S)

(Added Pub.L. 99-508, Title II, § 201[a], Oct. 21, 1986, 100 Stat. 1866; amended Pub.L. 104-293, Title VI, § 601(c), Oct. 11, 1996, 110 Stat. 3469; Pub.L. 107-56, Title II, § 223(b), Title VIII, § 815, Oct. 26, 2001, 115 Stat. 293, 384; Pub.L. 107-273, Div. B, Title IV, § 4005(f)(2), Nov. 2, 2002, 116 Stat. 1813.)

Notes of Decisions (16)

18 U.S.C.A. § 2707, 18 USCA § 2707
Current through P.L. 114-61 (excluding P.L. 114-52, 114-54, 114-59, and 114-60) approved 10-7-2015

End of Document

18 U.S.C.A. § 2510

§ 2510. Definitions

Effective: November 2, 2002
Currentness

As used in this chapter--

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. [1]

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means--

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given that term in section 3 of the Communications Act of 1934;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who--

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means 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;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means--

(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) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

CREDIT(S)

(Added Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 212; amended Pub.L. 99-508, Title I, § 101(a), (c)(1)(A), (4), Oct. 21, 1986, 100 Stat. 1848, 1851; Pub.L. 103-414, Title II, §§ 202(a), 203, Oct. 25, 1994, 108 Stat. 4290, 4291; Pub.L. 104-132, Title VII, § 731, Apr. 24, 1996, 110 Stat. 1303; Pub.L. 107-56, Title II, §§ 203(b)(2), 209(1), 217(1), Oct. 26, 2001, 115 Stat. 280, 283, 290; Pub.L. 107-108, Title III, § 314(b), Dec. 28, 2001, 115 Stat. 1402; Pub.L. 107-273, Div. B, Title IV, § 4002(e)(10), Nov. 2, 2002, 116 Stat. 1810.)

Notes of Decisions (213)

Footnotes

1 So in original. The period probably should be a semicolon.

18 U.S.C.A. § 2510, 18 USCA § 2510

Current through P.L. 114-61 (excluding P.L. 114-52, 114-54, 114-59, and 114-60) approved 10-7-2015

End of Document

West's Annotated California Codes
Code of Civil Procedure (Refs & Annos)
Part 4. Miscellaneous Provisions (Refs & Annos)
Title 4. Civil Discovery Act (Refs & Annos)
Chapter 12. Discovery in Action Pending Outside California (Refs & Annos)
Article 1. Interstate and International Depositions and Discovery Act (Refs & Annos)

West's Ann.Cal.C.C.P. § 2029.300

§ 2029.300. Issuance of subpoena

Effective: January 1, 2010
Currentness

(a) To request issuance of a subpoena under this section, a party shall submit the original or a true and correct copy of a foreign subpoena to the clerk of the superior court in the county in which discovery is sought to be conducted in this state. A request for the issuance of a subpoena under this section does not constitute making an appearance in the courts of this state.

(b) In addition to submitting a foreign subpoena under subdivision (a), a party seeking discovery shall do both of the following:

(1) Submit an application requesting that the superior court issue a subpoena with the same terms as the foreign subpoena. The application shall be on a form prescribed by the Judicial Council pursuant to Section 2029.390. No civil case cover sheet is required.

(2) Pay the fee specified in Section 70626 of the Government Code.

(c) When a party submits a foreign subpoena to the clerk of the superior court in accordance with subdivision (a), and satisfies the requirements of subdivision (b), the clerk shall promptly issue a subpoena for service upon the person to which the foreign subpoena is directed.

(d) A subpoena issued under this section shall satisfy all of the following conditions:

(1) It shall incorporate the terms used in the foreign subpoena.

(2) It shall contain or be accompanied by the names, addresses, and telephone numbers of all counsel of record in the proceeding to which the subpoena relates and of any party not represented by counsel.

(3) It shall bear the caption and case number of the out-of-state case to which it relates.

(4) It shall state the name of the court that issues it.

(5) It shall be on a form prescribed by the Judicial Council pursuant to Section 2029.390.

Credits

(Added by Stats.2008, c. 231 (A.B.2193), § 3, operative Jan. 1, 2010.)

Editors' Notes

OPERATIVE EFFECT

<For operative effect of this Article, see Code of Civil Procedure § 2029.900.>

LAW REVISION COMMISSION COMMENTS

2008 Addition

Section 2029.300 is added to clarify the procedure for obtaining a California subpoena to obtain discovery from a witness in this state for use in a proceeding pending in another jurisdiction. For the benefit of the party seeking the subpoena and the court issuing it, the procedure is designed to be simple and expeditious.

Subdivisions (a), (c), and (d)(1)-(2) are similar to Section 3 of the Uniform Interstate Depositions and Discovery Act (2007). Subdivisions (b) and (d)(3)-(5) address additional procedural details.

To obtain a subpoena under this section, a party must submit the original or a true and correct copy of a "foreign subpoena." For definitions of "foreign subpoena" and "subpoena," see Section 2029.200 (definitions). The definition of "subpoena" is broad, encompassing not only a document denominated a "subpoena," but also a mandate, writ, letters rogatory, letter of request, commission, or other court document that requires a person to testify at a deposition, produce documents or other items, or permit inspection of property.

Subdivision (a) makes clear that requesting and obtaining a subpoena under this section does not constitute making an appearance in the California courts. For further guidance on avoiding unauthorized practice of law, see Bus. & Prof. Code § 6125; Cal.R.Ct. 9.40, 9.47; Report of the California Supreme Court Multijurisdictional Practice Implementation Committee: Final Report and Proposed Rules (March 10, 2004); California Supreme Court Advisory Task Force on Multijurisdictional Practice, Final Report and Recommendations (Jan. 7, 2002). In general, a party to out-of-state litigation may take a deposition in California without retaining local counsel if the party is self-represented or represented by an attorney duly admitted to practice in another jurisdiction of the United States. Birbrower v. Superior Court, 17 Cal.4th 119, 127, 949 P.2d 1, 70 Cal.Rptr.2d 304 (1998) ("[P]ersons may represent themselves and their own interests regardless of State Bar membership..."); Cal.R.Ct. 9.47; Final Report and Recommendations, *supra*, at 24. Different considerations may apply, however, if a discovery dispute arises in connection with such a deposition and a party to out-of-state litigation wants to appear in a California court with respect to the dispute.

See also Sections 2029.350 (issuance of subpoena by local counsel), 2029.640 (discovery on notice or agreement).

Background from Uniform Act

The term "Submitted" to a clerk of court includes delivering to or filing. Presenting a subpoena to the clerk of court in the discovery state, so that a subpoena is then issued in the name of the discovery state, is the necessary act that invokes the

jurisdiction of the discovery state, which in turn makes the newly issued subpoena both enforceable and challengeable in the discovery state.

The committee envisions the standard procedure under this section will become as follows, using as an example a case filed in Kansas (the trial state) where the witness to be deposed lives in California (the discovery state): A lawyer of record for a party in the action pending in Kansas will issue a subpoena in Kansas (the same way lawyers in Kansas routinely issue subpoenas in pending actions). That lawyer will then check with the clerk's office, in the California county in which the witness to be deposed lives, to obtain a copy of its subpoena form (the clerk's office will usually have a Web page explaining its forms and procedures). The lawyer will then prepare a California subpoena so that it has the same terms as the Kansas subpoena. The lawyer will then hire a process server (or local counsel) in California, who will take the completed and executed Kansas subpoena and the completed but not yet executed California subpoena to the clerk's office in California. The clerk of court, upon being given the Kansas subpoena, will then issue the identical California subpoena. The process server (or other agent of the party) will pay any necessary filing fees, and then serve the California subpoena on the deponent in accordance with California law (which includes any applicable local rules).

The advantages of this process are readily apparent. The act of the clerk of court is ministerial, yet is sufficient to invoke the jurisdiction of the discovery state over the deponent. The only documents that need to be presented to the clerk of court in the discovery state are the subpoena issued in the trial state and the draft subpoena of the discovery state. [Note: In California, an application form would also be required.] There is no need to hire local counsel to have the subpoena issued in the discovery state, and there is no need to present the matter to a judge in the discovery state before the subpoena can be issued. In effect, the clerk of court in the discovery state simply reissues the subpoena of the trial state, and the new subpoena is then served on the deponent in accordance with the laws of the discovery state. The process is simple and efficient, costs are kept to a minimum, and local counsel and judicial participation are unnecessary to have the subpoena issued and served in the discovery state.

The Act will not change or repeal the law in those states that still require a commission or letters rogatory to take a deposition in a foreign jurisdiction. The Act does, however, repeal the law in those discovery states that still require a commission or letter rogatory from a trial state before a deposition can be taken in those states. It is the hope of the Conference that this Act will encourage states that still require the use of commissions or letters rogatory to repeal those laws.

The Act requires that, when the subpoena is served, it contain or be accompanied by the names, addresses, and telephone numbers of all counsel of record and of any party not represented by counsel. The committee believes that this requirement imposes no significant burden on the lawyer issuing the subpoena, given that the lawyer already has the obligation to send a notice of deposition to every counsel of record and any unrepresented parties. The benefits in the discovery state, by contrast, are significant. This requirement makes it easy for the deponent (or, as will frequently be the case, the deponent's lawyer) to learn the names of and contact the other lawyers in the case. This requirement can easily be met, since the subpoena will contain or be accompanied by the names, addresses, and telephone numbers of all counsel of record and of any party not represented by counsel (which is the same information that will ordinarily be contained on a notice of deposition and proof of service).

[Adapted from UIDDA § 3 comment.] [37 Cal.L.Rev.Comm. Reports 99 (2007)].

OFFICIAL FORMS

2015 Electronic Update

<Mandatory and optional Forms adopted and approved by the Judicial Council are set out in West's California Judicial Council Forms Pamphlet.>

West's Ann. Cal. C.C.P. § 2029.300, CA CIV PRO § 2029.300

Current with urgency legislation through Ch. 807 of 2015 Reg.Sess. and Ch. 1 of 2015-2016 2nd Ex.Sess.

End of Document

West's Annotated California Codes
Code of Civil Procedure (Refs & Annos)
Part 4. Miscellaneous Provisions (Refs & Annos)
Title 4. Civil Discovery Act (Refs & Annos)
Chapter 12. Discovery in Action Pending Outside California (Refs & Annos)
Article 1. Interstate and International Depositions and Discovery Act (Refs & Annos)

West's Ann.Cal.C.C.P. § 2029.350

§ 2029.350. Foreign subpoenas; issuance of subpoena under this article

Effective: January 1, 2010
Currentness

(a) Notwithstanding Sections 1986 and 2029.300, if a party to a proceeding pending in a foreign jurisdiction retains an attorney licensed to practice in this state, who is an active member of the State Bar, and that attorney receives the original or a true and correct copy of a foreign subpoena, the attorney may issue a subpoena under this article.

(b) A subpoena issued under this section shall satisfy all of the following conditions:

(1) It shall incorporate the terms used in the foreign subpoena.

(2) It shall contain or be accompanied by the names, addresses, and telephone numbers of all counsel of record in the proceeding to which the subpoena relates and of any party not represented by counsel.

(3) It shall bear the caption and case number of the out-of-state case to which it relates.

(4) It shall state the name of the superior court of the county in which the discovery is to be conducted.

(5) It shall be on a form prescribed by the Judicial Council pursuant to Section 2029.390.

Credits
(Added by Stats.2008, c. 231 (A.B.2193), § 3, operative Jan. 1, 2010.)

Editors' Notes

OPERATIVE EFFECT

<For operative effect of this Article, see Code of Civil Procedure § 2029.900.>

LAW REVISION COMMISSION COMMENTS

2008 Addition

Section 2029.350 is added to make clear that if certain conditions are satisfied, local counsel may issue process compelling a California witness to appear at a deposition for an action pending in another jurisdiction.

To issue a subpoena under this section, a California attorney acting as local counsel must receive the original or a true and correct copy of a "foreign subpoena." For definitions of "foreign subpoena" and "subpoena," see Section 2029.200 (definitions). The definition of 'subpoena' is broad, encompassing not only a document denominated a "subpoena," but also a mandate, writ, letters rogatory, letter of request, commission, or other court document that requires a person to testify at a deposition, produce documents or other items, or permit inspection of property.

This section does not make retention of local counsel mandatory. For guidance on that point, see Section 2029.300(a); Bus. & Prof. Code § 6125; Cal.R.Ct. 9.40, 9.47; Report of the California Supreme Court Multijurisdictional Practice Implementation Committee: Final Report and Proposed Rules (March 10, 2004); California Supreme Court Advisory Task Force on Multijurisdictional Practice, Final Report and Recommendations (Jan. 7, 2002). In general, a party to out-of-state litigation may take a deposition in California without retaining local counsel if the party is self-represented or represented by an attorney duly admitted to practice in another jurisdiction of the United States. Birbrower v. Superior Court, 17 Cal.4th 119, 127, 949 P.2d 1, 70 Cal.Rptr.2d 304 (1998) ("[P]ersons may represent themselves and their own interests regardless of State Bar membership..."); Cal.R.Ct. 9.47; Final Report and Recommendations, *supra*, at 24. Different considerations may apply, however, if a discovery dispute arises in connection with such a deposition and a party to out-of-state litigation wants to appear in a California court with respect to the dispute.

See also Sections 2029.300 (issuance of subpoena by clerk of court), 2029.640 (discovery on notice or agreement). [37 Cal.L.Rev.Comm. Reports 99 (2007)].

OFFICIAL FORMS

2015 Electronic Update

<Mandatory and optional Forms adopted and approved by the Judicial Council are set out in West's California Judicial Council Forms Pamphlet.>

West's Ann. Cal. C.C.P. § 2029.350, CA CIV PRO § 2029.350
Current with urgency legislation through Ch. 807 of 2015 Reg.Sess. and Ch. 1 of 2015-2016 2nd Ex.Sess.

End of Document

West's Annotated California Codes
Code of Civil Procedure (Refs & Annos)
Part 4. Miscellaneous Provisions (Refs & Annos)
Title 4. Civil Discovery Act (Refs & Annos)
Chapter 12. Discovery in Action Pending Outside California (Refs & Annos)
Article 1. Interstate and International Depositions and Discovery Act (Refs & Annos)

West's Ann.Cal.C.C.P. § 2029.400

§ 2029.400. Service of subpoena

Effective: January 1, 2010
Currentness

A subpoena issued under this article shall be personally served in compliance with the law of this state, including, without limitation, Section 1985.

Credits
(Added by Stats.2008, c. 231 (A.B.2193), § 3, operative Jan. 1, 2010.)

Editors' Notes

OPERATIVE EFFECT

<For operative effect of this Article, see Code of Civil Procedure § 2029.900.>

LAW REVISION COMMISSION COMMENTS

2008 Addition

Section 2029.400 is similar to Section 4 of the Uniform Interstate Depositions and Discovery Act (2007). Section 2029.400 applies not only to a subpoena issued by a clerk of court under Section 2029.300, but also to a subpoena issued by local counsel under Section 2029.350. [37 Cal.L.Rev.Comm. Reports 99 (2007)].

OFFICIAL FORMS

2015 Electronic Update

<Mandatory and optional Forms adopted and approved by the Judicial Council are set out in West's California Judicial Council Forms Pamphlet.>

West's Ann. Cal. C.C.P. § 2029.400, CA CIV PRO § 2029.400
Current with urgency legislation through Ch. 807 of 2015 Reg.Sess. and Ch. 1 of 2015-2016 2nd Ex.Sess.

End of Document

West's Annotated California Codes
Code of Civil Procedure (Refs & Annos)
Part 4. Miscellaneous Provisions (Refs & Annos)
Title 3. Of the Production of Evidence (Refs & Annos)
Chapter 2. Means of Production (Refs & Annos)

West's Ann.Cal.C.C.P. § 1985

§ 1985. "Subpoena" defined; affidavit for subpoena duces tecum; issuance of subpoena in blank

Effective: January 1, 2013
Currentness

(a) The process by which the attendance of a witness is required is the subpoena. It is a writ or order directed to a person and requiring the person's attendance at a particular time and place to testify as a witness. It may also require a witness to bring any books, documents, electronically stored information, or other things under the witness's control which the witness is bound by law to produce in evidence. When a county recorder is using the microfilm system for recording, and a witness is subpoenaed to present a record, the witness shall be deemed to have complied with the subpoena if the witness produces a certified copy thereof.

(b) A copy of an affidavit shall be served with a subpoena duces tecum issued before trial, showing good cause for the production of the matters and things described in the subpoena, specifying the exact matters or things desired to be produced, setting forth in full detail the materiality thereof to the issues involved in the case, and stating that the witness has the desired matters or things in his or her possession or under his or her control.

(c) The clerk, or a judge, shall issue a subpoena or subpoena duces tecum signed and sealed but otherwise in blank to a party requesting it, who shall fill it in before service. An attorney at law who is the attorney of record in an action or proceeding, may sign and issue a subpoena to require attendance before the court in which the action or proceeding is pending or at the trial of an issue therein, or upon the taking of a deposition in an action or proceeding pending therein; the subpoena in such a case need not be sealed. An attorney at law who is the attorney of record in an action or proceeding, may sign and issue a subpoena duces tecum to require production of the matters or things described in the subpoena.

Credits

(Enacted in 1872. Amended by Stats.1933, c. 567, p. 1479, § 1; Stats.1961, c. 496, p. 1590, § 1; Stats.1967, c. 431, p. 1645, § 1; Stats.1968, c. 95, p. 305, § 1; Stats.1979, c. 458, p. 1607, § 1; Stats.1982, c. 452, § 1; Stats.1986, c. 603, § 3; Stats.1990, c. 511 (S.B.163), § 1, eff. Aug. 13, 1990; Stats.2012, c. 72 (S.B.1574), § 1.)

Editors' Notes

OFFICIAL FORMS

2007 Main Volume

<Mandatory and optional Forms adopted and approved by the Judicial Council are set out in West's California Judicial Council Forms Pamphlet.>

West's Annotated California Codes
Code of Civil Procedure (Refs & Annos)
Part 4. Miscellaneous Provisions (Refs & Annos)
Title 4. Civil Discovery Act (Refs & Annos)
Chapter 12. Discovery in Action Pending Outside California (Refs & Annos)
Article 1. Interstate and International Depositions and Discovery Act (Refs & Annos)

West's Ann.Cal.C.C.P. § 2029.500

§ 2029.500. Deposition, production, and inspection; applicable laws and rules

Effective: January 1, 2010
Currentness

Titles 3 (commencing with Section 1985) and 4 (commencing with Section 2016.010) of Part 4, and any other law or court rule of this state governing a deposition, a production of documents or other tangible items, or an inspection of premises, including any law or court rule governing payment of court costs or sanctions, apply to discovery under this article.

Credits

(Added by Stats.2008, c. 231 (A.B.2193), § 3, operative Jan. 1, 2010.)

Editors' Notes

OPERATIVE EFFECT

<For operative effect of this Article, see Code of Civil Procedure § 2029.900.>

LAW REVISION COMMISSION COMMENTS

2008 Addition

Section 2029.500 is similar to Section 5 of the Uniform Interstate Depositions and Discovery Act (2007). Section 2029.500 applies not only to a subpoena issued by a clerk of court under Section 2029.300, but also to a subpoena issued by local counsel under Section 2029.350 and to discovery taken in this state pursuant to properly issued notice or by agreement.

Background from Uniform Act

The Act requires that the discovery permitted by this section must comply with the laws of the discovery state. The discovery state has a significant interest in these cases in protecting its residents who become non-party witnesses in an action pending in a foreign jurisdiction from any unreasonable or unduly burdensome discovery request. Therefore, the committee believes that the discovery procedure must be the same as it would be if the case had originally been filed in the discovery state.

[Adapted from UIDDA § 5 comment.] [37 Cal.L.Rev.Comm. Reports 99 (2008)].

OFFICIAL FORMS

2015 Electronic Update

<Mandatory and optional Forms adopted and approved by the Judicial Council are set out in West's California Judicial Council Forms Pamphlet.>

Notes of Decisions (2)

West's Ann. Cal. C.C.P. § 2029.500, CA CIV PRO § 2029.500
Current with urgency legislation through Ch. 807 of 2015 Reg.Sess. and Ch. 1 of 2015-2016 2nd Ex.Sess.

End of Document

West's Annotated California Codes
Code of Civil Procedure (Refs & Annos)
Part 4. Miscellaneous Provisions (Refs & Annos)
Title 4. Civil Discovery Act (Refs & Annos)
Chapter 12. Discovery in Action Pending Outside California (Refs & Annos)
Article 1. Interstate and International Depositions and Discovery Act (Refs & Annos)

West's Ann.Cal.C.C.P. § 2029.600

§ 2029.600. Application to court

Effective: January 1, 2010
Currentness

(a) If a dispute arises relating to discovery under this article, any request for a protective order or to enforce, quash, or modify a subpoena, or for other relief may be filed in the superior court in the county in which discovery is to be conducted and, if so filed, shall comply with the applicable rules or statutes of this state.

(b) A request for relief pursuant to this section shall be referred to as a petition notwithstanding any statute under which a request for the same relief would be referred to as a motion or by another term if it was brought in a proceeding pending in this state.

(c) A petition for relief pursuant to this section shall be accompanied by a civil case cover sheet.

Credits
(Added by Stats.2008, c. 231 (A.B.2193), § 3, operative Jan. 1, 2010.)

Editors' Notes

OPERATIVE EFFECT

<For operative effect of this Article, see Code of Civil Procedure § 2029.900.>

LAW REVISION COMMISSION COMMENTS

2008 Addition

Section 2029.600 is similar to Section 6 of the Uniform Interstate Depositions and Discovery Act (2007). It serves to clarify the procedure for using a California court to resolve a dispute relating to discovery conducted in this state for purposes of a proceeding pending in another jurisdiction.

The objective of subdivision (a) is to ensure that if a dispute arises relating to discovery under this article, California is able to protect its policy interests and the interests of persons located in the state. In particular, the state must be able to protect its residents from unreasonable or unduly burdensome discovery requests. A court should interpret the provision with this objective in mind.

Subdivision (b) makes clear that a request for relief pursuant to this section is properly denominated a "petition," not a "motion." For example, suppose a party to an out-of-state proceeding subpoenas personal records of a nonparty consumer under Section 1985.3 and the nonparty consumer serves a written objection to production as authorized by the statute. To obtain production, the subpoenaing party would have to file a "petition" to enforce the subpoena, not a "motion" as Section 1985.3(g) prescribes for a case pending in California.

See also Sections 2029.610 (fees and format of papers relating to discovery dispute), 2029.620 (subsequent discovery dispute in same case and county), 2029.630 (hearing date and briefing schedule), 2029.640 (discovery on notice or agreement), 2029.650 (writ petition). [37 Cal.L.Rev.Comm. Reports 99 (2007)].

OFFICIAL FORMS

2015 Electronic Update

<Mandatory and optional Forms adopted and approved by the Judicial Council are set out in West's California Judicial Council Forms Pamphlet.>

West's Ann. Cal. C.C.P. § 2029.600, CA CIV PRO § 2029.600
Current with urgency legislation through Ch. 807 of 2015 Reg.Sess. and Ch. 1 of 2015-2016 2nd Ex.Sess.

End of Document

550 F.Supp.2d 606
United States District Court,
E.D. Virginia,
Alexandria Division.

In re SUBPOENA DUCES TECUM TO AOL, LLC.

No. 1:07mc34 (GBL). | April 18, 2008.

Synopsis

Background: Non-party witnesses in an action pending in another district moved to quash a subpoena duces tecum issued to their Internet service provider, seeking production of the witnesses' emails.

Holdings: Affirming an order of Poretz, United States Magistrate Judge, the District Court, Gerald Bruce Lee, J., held that:

[1] Electronic Communications Privacy Act prohibited the provider from producing the emails;

[2] subpoena was overbroad, and thus imposed an undue burden on the witnesses; and

[3] court presiding over the action in the other district was better posed to evaluate the witnesses' privilege claim.

Ordered accordingly.

West Headnotes (9)

[1] **Telecommunications**
Computer communications

Electronic Communications Privacy Act prohibited Internet service provider from producing the emails of non-party witnesses in an action pending in another district, which were sought pursuant to a subpoena duces tecum; issuance of the civil discovery subpoena was not an exception to the provisions of the Act so as to allow the provider to disclose the communications. 18 U.S.C.A. §§ 2701, 2702(a–c), 2703.

20 Cases that cite this headnote

[2] **Statutes**
Plain language; plain, ordinary, common, or literal meaning

In cases involving statutory construction, the court must presume that Congress expressed its intent or legislative purpose through the ordinary meaning of the words used.

Cases that cite this headnote

[3] **Statutes**
Statute as a Whole; Relation of Parts to Whole and to One Another

To ascertain legislative intent, the court must look at the statute as a whole, rather than analyzing a single sentence or a single word within a sentence.

Cases that cite this headnote

[4] **Statutes**
Absence of Ambiguity; Application of Clear or Unambiguous Statute or Language

When the words of a statute are clear and unambiguous, the court's inquiry ends and the statutory language must be regarded as conclusive.

1 Cases that cite this headnote

[5] **Telecommunications**
Computer communications

Unauthorized private parties and governmental entities are prohibited from using civil discovery subpoenas to circumvent the Electronic Communications Privacy Act's protections. 18 U.S.C.A. §§ 2701, 2702(a–c), 2703; Fed.Rules Civ.Proc.Rule 45, 28 U.S.C.A.

18 Cases that cite this headnote

[6] **Witnesses**
Subpoena duces tecum

Subpoena duces tecum seeking emails of non-party witnesses in an action was overbroad, and thus imposed an undue burden on the witnesses, to the extent that it did not limit the documents requested to subject matter relevant to the claims or defenses in the action; the subpoena requested "all" of a witness' emails for a six-week period, which would likely include privileged and personal information unrelated to the action. Fed.Rules Civ.Proc.Rule 45(c)(3)(A)(iv), 28 U.S.C.A.

6 Cases that cite this headnote

[7] **Witnesses**
Subpoena duces tecum

When a non-party claims that a subpoena is burdensome and oppressive, the non-party must support its claim by showing how production would be burdensome. Fed.Rules Civ.Proc.Rule 45(c)(3)(A)(iv), 28 U.S.C.A.

2 Cases that cite this headnote

[8] **Witnesses**
Subpoena duces tecum

Subpoena imposes an undue burden on a party when a subpoena is overbroad. Fed.Rules Civ.Proc.Rule 45(c)(3)(A)(iv), 28 U.S.C.A.

7 Cases that cite this headnote

[9] **Telecommunications**
Privacy in general

Court presiding over an action in another district was better posed to evaluate a privilege claim asserted by non-party witnesses in that action in support of their motion to quash a subpoena duces tecum seeking to compel an Internet service provider to produce their emails, and thus, the instant court would not rule on the merits of the issue; the subpoena sought information relevant to the claims or defenses available to the parties in the other action. Fed.Rules Civ.Proc.Rule 26(b)(5)(A), 28 U.S.C.A.; Fed.Rules Civ.Proc.Rule 26(b)(1), 28 U.S.C.App.(2000 Ed.)

3 Cases that cite this headnote

Attorneys and Law Firms

***607** Ellen D. Marcus, Zuckerman Spader LLP, Washington, DC, for Movant.

Theodore Ira Brenner, Alexander Spotswood de Witt, Brenner Evans & Millman PC, Richmond, VA, for Defense.

MEMORANDUM ORDER

GERALD BRUCE LEE, District Judge.

THIS MATTER is before the Court on State Farm Fire and Casualty Co.'s Objections to Magistrate Judge Poretz's Order, entered on November 30, 2007, quashing State Farm's subpoena to AOL, LLC. This case concerns Cori and Kerri Rigsby's claims that State Farm's subpoena issued to AOL violated the Electronic Communications Privacy Act ("Privacy Act"), codified as 18 U.S.C. §§ 2701–03 (2000), imposed an undue burden on the Rigsbys, and requested e-mails from the Rigsbys that were protected by the attorney-client privilege. The issue before the Court is whether Magistrate Judge Poretz clearly erred by granting the Rigsbys' Motion to Quash, where State Farm's civil discovery subpoena requested: (1) production of the Rigsbys' e-mails from AOL; (2) all of Cori Rigsby's e-mails from a six-week period; and (3) information relevant to *McIntosh v. State Farm Fire & Casualty Co.*, subject to the Rigsbys' attorney-client privilege claims. The Court upholds Magistrate Judge Poretz's decision quashing State Farm's subpoena, and holds that it was not clearly erroneous for the following reasons: (1) the Privacy Act prohibits ***608** AOL from producing the Rigsbys' e-mails in response to State Farm's subpoena because a civil discovery subpoena is not a disclosure exception under the Act; (2) State Farm's subpoena imposes an undue burden on the Rigsbys because the subpoena is overbroad and the documents requested are not limited to subject matter relevant to the claims or defenses in *McIntosh*; and (3) the Southern District of Mississippi is better suited to decide whether the information relevant to *McIntosh* is privileged because no action is pending in this Court. Thus, Magistrate Judge Poretz's Order is affirmed.

I. BACKGROUND

Cori and Kerri Rigsby are non-party witnesses in *McIntosh v. State Farm Fire & Casualty Co.*, an action pending in the Southern District of Mississippi. No. 1:06cv1080 (S.D. Miss. filed Oct. 23, 2006). The Rigsbys were employed as insurance adjusters by E.A. Renfroe and Co. ("E.A. Renfroe") and discovered what they believed to be fraud with respect to State Farm's treatment of Thomas and Pamela McIntosh's Hurricane Katrina damage claim. [1] The Rigsbys provided supporting documents to state and federal law enforcement authorities and filed a *qui tam* action, *United States ex rel. Rigsby v. State Farm Insurance Co.*, in the Southern District of Mississippi, alleging that State Farm defrauded the United States Government by improperly shifting costs from State Farm's wind damage coverage to the federal flood insurance program. No. 1:06cv433 (S.D. Miss. filed Apr. 26, 2006).

In the course of discovery litigation related to *McIntosh*, State Farm issued a subpoena through this Court to AOL, requesting production of documents from the Rigsbys' e-mail accounts pertaining to Thomas or Pamela McIntosh, State Farm Fire & Casualty Co.'s claims handling practices for Hurricane Katrina, Forensic Analysis & Engineering Corporation's documents for Hurricane Katrina, and E.A. Renfroe & Co.'s claims handling practices for Hurricane Katrina over a ten-month period. [2] State Farm's subpoena also requested any and all documents, including electronically stored information, related to Cori Rigsby's e-mail account or address from September 1, 2007, to October 12, 2007, a six-week period where Cori Rigsby and her attorneys allegedly concealed from State Farm that her computer had crashed. [3] In a letter dated November 1, 2007, the Rigsbys requested that State Farm withdraw the subpoena directed to AOL (Pet'r Mem. in Supp. Ex. C), and State Farm declined. (Pet'r Mem. in Supp. 1.) The Rigsbys then moved to quash State Farm's subpoena, claiming ***609** that the subpoena violated the Privacy Act, was overbroad and unduly burdensome, and requested production of e-mails that included privileged communications. (Pet'r Mem. in Supp. 1–2.)

On November 30, 2007, in a hearing conducted by Magistrate Judge Poretz, the court held that: (1) the Rigsbys have standing to object to the disclosure of their personal records; and (2) the information sought by State Farm through its subpoena to AOL was relevant to the claims or defenses asserted in the underlying action and within the permissible scope of discovery, subject to any claim of privilege by the Rigsbys. Magistrate Judge Poretz declined to decide whether any of the information sought was privileged, or whether any exceptions or waiver applied to the privilege claims, finding that the presiding judge in the Southern District of Mississippi was in a better position to make a ruling on the asserted privilege. Magistrate Judge Poretz granted the Rigsbys' Motion to Quash "for the reasons set forth in the ... [Rigsbys'] Memorandum in Support." (Order, Nov. 30, 2007.) State Farm subsequently filed Objections to Magistrate Judge Poretz's Order. [4]

II. DISCUSSION

A. Standard of Review

When a magistrate judge issues a written order deciding a pretrial matter that is not dispositive of a party's claim or defense, the parties may file timely objections to the order. FED.R.CIV.P. 72(a). The district judge must consider timely objections and modify or set aside any part of the order that is clearly erroneous or contrary to law. 28 U.S.C. § 636(b)(1)(a) (2000); FED.R.CIV.P. 72(a).

B. Analysis

1. *The Privacy Act*

[1] [2] [3] [4] The Court upholds Magistrate Judge Poretz's Order, quashing State Farm's subpoena, because the plain language of the Privacy Act prohibits AOL from producing the Rigsbys' e-mails, and the issuance of a civil discovery subpoena is not an exception to the provisions of the Privacy Act that would allow an internet service provider to disclose the communications at issue here. In cases involving statutory construction, the court must presume that Congress expressed its intent or legislative purpose through the ordinary meaning of the words used. *Am. Tobacco Co. v. Patterson*, 456 U.S. 63, 68, 102 S.Ct. 1534, 71 L.Ed.2d 748 (1982). To ascertain legislative intent, the court must look at the statute as a whole, rather than analyzing a single sentence or a single word within a sentence. *Elm Grove Coal Co. v. Dir., Office of Workers' Comp. Programs*, 480 F.3d 278, 293 (4th Cir.2007). When the words of a statute are clear and unambiguous, the court's inquiry ends and the statutory language must be regarded as conclusive. *Am. Tobacco Co.*, 456 U.S. at 68, 102 S.Ct. 1534.

The statutory language of the Privacy Act must be regarded as conclusive because it contains plain and unambiguous language and a coherent and consistent statutory scheme. Section 2701 clearly establishes a punishable offense for intentionally accessing without or exceeding authorization and obtaining electronic communications stored at an electronic communication service facility. 18 U.S.C. § 2701 (2000). Section 2702 plainly prohibits an electronic communication or remote computing service to the public from knowingly divulging to any person or entity ***610** the contents of customers' electronic communications or records pertaining to subscribing customers. *Id.* § 2702(a). Additionally, § 2702 lists unambiguous exceptions that allow an electronic communication or remote computing service to disclose the contents of an electronic communication or subscriber information. *Id.* § 2702(b-c). Section 2703 provides instances related to ongoing criminal investigations where a governmental entity may require an electronic communication or remote computing service to disclose the contents of customers' electronic communications or subscriber information. *Id.* § 2703. Protecting privacy interests in personal information stored in computerized systems, while also protecting the Government's legitimate law enforcement needs, the Privacy Act creates a zone of privacy to protect internet subscribers from having their personal information wrongfully used and publicly disclosed by "unauthorized private parties," S.REP. NO. 99–541, at 3 (1986), as *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

In *Theofel v. Farey–Jones,* the court reversed the district court's dismissal of the plaintiffs' claim that the defendants intentionally accessed without authorization the plaintiffs' e-mails in violation of the Privacy Act, where the defendants issued a subpoena to the plaintiffs' internet service provider to obtain the plaintiffs' stored e-mails during the course of civil discovery. 359 F.3d 1066, 1071–72, 1077 (9th Cir.2004). After the internet service provider complied with the subpoena, the defendants read the plaintiffs' e-mails, including many that were privileged, personal, and unrelated to the commercial litigation between the parties. *Id.* at 1071. In the course of evaluating the claim, the court emphasized that the Privacy Act protects users whose electronic communications are stored with an internet service provider and reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications stored at such a facility. *Id.* at 1072–73. The court found that the subpoena was invalid because it "transformed ... a bona fide state-sanctioned inspection into private snooping." *Id.* at 1073. Because the invalid "subpoena caused disclosure of documents that otherwise would have remained private," the court held that the invalid subpoena invaded " 'the specific interests that the [Privacy Act] seeks to protect.' " *Id.* at 1073–74 (quoting *J.H. Desnick, M.D., Eye Serv., Ltd. v. ABC,* 44 F.3d 1345, 1352 (7th Cir.1995)).

Similarly, in *Federal Trade Commission v. Netscape Communications Corp.*, the court denied the Federal Trade Commission's ("FTC") motion to compel, where an internet service provider, a non-party in the underlying action, refused to turn over documents containing subscriber identity information to the FTC. 196 F.R.D. 559, 559, 561 (N.D.Cal.2000). The FTC filed a civil lawsuit against the subscribers for violating the FTC unfair competition statute. *Id.* at 559. During pre-trial discovery, the FTC issued a subpoena to the internet service provider pursuant to Federal Rule of Civil Procedure 45. *Id.* at 559. The court distinguished discovery subpoenas from trial subpoenas based on differences in scope and operation and concluded that Congress would have specifically included discovery subpoenas in the Privacy Act if Congress meant to include this as an exception requiring an internet service provider to disclose subscriber information to a governmental entity. *Id.* at 560–61. The court held that the statutory phrase "trial subpoena" does not apply to discovery subpoenas in civil cases and declined to allow the FTC to use Rule 45 to circumvent the protections built into the Privacy Act that protect subscriber privacy from governmental entities. *Id.* at 561.

***611** In *O'Grady v. Superior Court,* the Court of Appeal of the State of California, Sixth Appellate District, held that enforcement of a civil subpoena issued to an e-mail service provider is inconsistent with the plain terms of the Privacy Act. 139 Cal.App.4th 1423, 44 Cal.Rptr.3d 72, 76–77 (2006). Apple brought a civil action against several unknown defendants for wrongfully publishing on the World Wide Web Apple's secret plans to release a new product. *Id.* at 76. To identify the unknown defendants, Apple issued civil discovery subpoenas to non-party internet service providers, requesting copies of any e-mails that contained certain keywords from the published secret plans. *Id.* at 81. When considering whether the trial court should have quashed the subpoenas, the appellate court analyzed the language of the Privacy Act and found it to be clear and unambiguous. *Id.* at 84, 86–87. The court also found that any disclosure by an internet service provider of stored e-mail violates the Privacy Act unless it falls within an enumerated exception to the general prohibition. *Id.* at 86. Emphasizing the substantial

burden and expense that would be imposed on internet service providers if they were required to respond to every civil discovery subpoena issued in a civil lawsuit and how such a policy may discourage users from using new media, the court refused to create an exception for civil discovery and found the subpoenas unenforceable under the Privacy Act. *Id.* at 88–89.

[5] Applying the clear and unambiguous language of § 2702 to this case, AOL, a corporation that provides electronic communication services to the public, may not divulge the contents of the Rigsbys' electronic communications to State Farm because the statutory language of the Privacy Act does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas. Like the FTC in Netscape, State Farm insists that a facially valid subpoena *duces tecum* issued under Federal Rule of Civil Procedure 45 fits within the Privacy Act's recognized exceptions under § 2703. However, unlike the FTC in *Netscape*, State Farm argues that all Rule 45 subpoenas fit within the exception for disclosures pursuant to a court order. The Court finds State Farm's argument unpersuasive because § 2703 pertains exclusively to *criminal* investigations, not civil discovery matters such as this. Because State Farm is a private party and this is a civil lawsuit, none of the exceptions for governmental entities under § 2703 apply. Furthermore, agreeing with the reasoning in *Netscape*, the Court holds that "unauthorized private parties" and governmental entities are prohibited from using Rule 45 civil discovery subpoenas to circumvent the Privacy Act's protections.

State Farm has issued a subpoena to the Rigsbys' internet service provider that resembles the subpoena at issue in *Theofel* because it seeks to obtain copies of the Rigsbys' e-mails in the course of discovery for a civil lawsuit. Similar to the plaintiffs in *Theofel,* the Rigsbys seek to protect the privacy of their e-mails, asserting that they are privileged, personal, and unrelated to the civil lawsuit. In line with the court's reasoning in *Theofel,* the Court finds that the Privacy Act protects the Rigsbys' stored e-mails because the Rigsbys have a legitimate interest in the confidentiality of their personal e-mails being stored electronically by AOL. Agreeing with the reasoning in *O'Grady,* this Court holds that State Farm's subpoena may not be enforced consistent with the plain language of the Privacy Act because the exceptions enumerated in § 2702(b) do not include civil discovery subpoenas. Furthermore, § 2702(b) does not make any references to civil litigation or the civil discovery process. For the foregoing reasons, Magistrate Judge Poretz did not ***612** clearly err when he found that the Privacy Act prohibits AOL from producing the Rigsbys' e-mails in response to State Farm's subpoena because the Privacy Act's enumerated exceptions do not authorize disclosure pursuant to a civil discovery subpoena.

2. *Undue Burden*

[6] **[7]** **[8]** The Court upholds Magistrate Judge Poretz's Order, quashing State Farm's subpoena, because the subpoena is overbroad to the extent that it does not limit the documents requested to subject matter relevant to the claims or defenses in *McIntosh* and imposes an undue burden on the Rigsbys. "A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena." FED.R.CIV.P. 45(c)(1). A court must quash or modify a subpoena that subjects a person to an undue burden. FED. R. CIV. P. 45(c)(3)(A)(iv). When a non-party claims that a subpoena is burdensome and oppressive, the non-party must support its claim by showing how production would be burdensome. *Vaughan Furniture Co. v. Featureline Mfg., Inc.,* 156 F.R.D. 123, 125 (M.D.N.C.1994). A subpoena imposes an undue burden on a party when a subpoena is overbroad. *Theofel,* 359 F.3d at 1071–72.

In *Theofel,* the defendant sought access to the plaintiffs' e-mails by issuing a subpoena to the plaintiff's internet service provider in the course of discovery related to commercial litigation between the parties. 359 F.3d at 1071. The defendant's subpoena "ordered production of 'all copies of e-mails sent or received by anyone' ... with no limitation as to time or scope." *Id.* After the internet service provider produced 339 messages, many of which were unrelated to the litigation, privileged or personal, the plaintiffs asked the court to quash the subpoena. *Id.* Finding that the subpoena was "massively overbroad," "patently unlawful," and violated the Federal Rules, the magistrate judge quashed the subpoena and awarded sanctions. *Id.* at 1071–72. The plaintiffs subsequently sued the defendant and the defendant's attorney for violating the Privacy Act based on the internet service provider's disclosure of the plaintiffs' e-mails. *Id.* at 1072. On appeal, the court reversed the dismissal of the plaintiffs' Privacy Act claim, emphasizing that the defendant's attorney was supposed to avoid imposing an undue burden on the internet service provider and that the subpoena should have requested only e-mail related to the subject matter of the litigation, messages sent during some relevant time period or messages sent to or from employees in some way connected to the litigation. 359 F.3d at 1071, 1079. The court also

emphasized that the subpoena was properly quashed because it imposed an undue burden on the internet service provider by being overbroad and requesting all of the parties e-mails. *Id.*

Similar to the subpoena in *Theofel,* State Farm's subpoena must be quashed because it imposes an undue burden on the Rigsbys by being overbroad and requesting "all" of Cori Rigsby's e-mails for a six-week period. Like the subpoena in *Theofel,* State Farm's subpoena is overbroad because it does not limit the e-mails requested to those containing subject matter relevant to the underlying action or sent to or from employees connected to the litigation, other than Cori Rigsby. Although State Farm limited the e-mails requested to an allegedly relevant six-week period, in contrast to the subpoena in *Theofel* that requested e-mails without any time period limitation, State Farm's subpoena remains overbroad because the e-mails produced over a six-week period would likely include privileged and personal information unrelated to the *McIntosh* litigation, imposing an undue burden on Cori Rigsby. Thus, ***613** Magistrate Judge Poretz did not clearly err when he found that State Farm's subpoena was overbroad and imposed an undue burden on Cori Rigsby because State Farm's subpoena did not limit the documents requested to subject matter relevant to *McIntosh.*

3. *Privilege*

[9] The Court upholds Magistrate Judge Poretz's decision to decline making a determination with respect to the assertion of privilege by the Rigsbys because the Court agrees that the presiding judge in the Southern District of Mississippi is in a better position to make a ruling on the asserted privilege. "Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party." FED.R.CIV.P. 26(b)(1). When a party withholds information by claiming that it is privileged or subject to protection as trial preparation material, the party must expressly make the claim and describe the nature of the documents or communications not produced in a manner that does not reveal the privileged or protected information, but enables other parties to assess the applicability of the privilege or protection. FED.R.CIV.P. 26(b)(5)(A). Upon motion by a party or a non-party from whom discovery is sought, the court *in which the action is pending* may make an order protecting a party from "annoyance, embarrassment, oppression, undue burden or expense" by prohibiting or limiting discovery. FED.R.CIV.P. 26(c) (emphasis added). If the motion for a protective order is denied, the court may order a party or non-party to provide or permit discovery. *Id.*

The Rigsbys contend that their personal e-mail accounts likely contain communications with their attorneys related to pending litigation where the Rigsbys are parties or witnesses, including the *McIntosh* litigation in the Southern District of Mississippi. Because State Farm's subpoena requests information relevant to the claims or defenses available to the parties in *McIntosh,* the district court in Mississippi is better posed to evaluate the Rigsbys' privilege claim. Whereas State Farm's subpoena at issue here is the only pending litigation involving the parties in the Eastern District of Virginia. While acknowledging State Farm's argument that the Rigsbys did not allege sufficient facts or provide a privilege log to support an assertion of privilege, this Court declines to reach the merits of the privilege claim because the Mississippi district court in which the action is pending is better suited to decide whether the information relevant to *McIntosh* is privileged based on their familiarity with the underlying litigation.[5] Thus, Magistrate Judge Poretz did not clearly err when he declined to evaluate ***614** the Rigsbys' privilege claim on the merits because the Southern District of Mississippi is better posed to determine whether the Rigsbys' information requested by State Farm's subpoena is privileged as it pertains to claims and defenses associated with pending litigation in that jurisdiction.

III. CONCLUSION

The Court affirms Magistrate Judge Poretz's Order and finds that it was not clearly erroneous for three reasons: (1) the plain language of the Privacy Act prohibits AOL from producing the Rigsbys' e-mails in response to State Farm's subpoena because a civil discovery subpoena is not a disclosure exception under the Privacy Act; (2) State Farm's subpoena imposes an undue burden on the Rigsbys because the subpoena is overbroad and does not limit the documents requested to subject matter relevant to the claims or defenses in *McIntosh*; and (3) the Southern District of Mississippi is better posed to decide whether the Rigsbys' information relevant to the claims and defenses in *McIntosh* is privileged because the action is pending in their court, and no action is pending in this Court. For the foregoing reasons, it is hereby

ORDERED that Magistrate Judge Poretz's Order quashing State Farm's subpoena to AOL is AFFIRMED.

The Clerk is directed to forward a copy of this Order to counsel of record.

All Citations

550 F.Supp.2d 606

Footnotes

1 E.A. Renfroe is a state Farm contractor.

2 State Farm alleges that the Rigsbys admitted to: (1) stealing approximately 15,000 confidential documents from a State Farm laptop computer provided to the Rigsbys when they worked for E.A. Renfroe; (2) forwarding the stolen information via e-mail to the Rigsbys' personal AOL accounts; and (3) providing the stolen information to attorney Dickie Scruggs, who used the stolen information to file hundreds of lawsuits against State Farm, including McIntosh. In *McIntosh*, Magistrate Judge Walker ruled that "State Farm is entitled to Know the basis for the Rigsbys' charges of wrongdoing," and ordered the Rigsbys "to produce the requested documents within their actual or constructive possession" to State Farm. (Order on Mot. to Compel 5, Oct. 1, 2007).

3 In this Court, State Farm asserts that the Rigsbys can not comply with the Southern District of Mississippi's court order because the Rigsbys' home computer crashed. However, in *McIntosh*, Magistrate Judge Walker granted State Farm permission to have Cori Rigsby's computer examined by a court-selected expert to retrieve documents from the computer's hard drive. (Order on Mot. to Clarify, Nov. 19, 2007).

4 State Farm did not object to Magistrate Judge Poretz's finding regarding the Rigsbys' standing to object to disclosure of their personal records. (Resp't Objections.)

5 The district court in Mississippi could require the Rigsbys to create a privilege log and disclose this log to State Farm for further negotiations. *See Med. Components, Inc. v. Classic Med., Inc.*, 210 F.R.D. 175, 179–80 (M.D.N.C.2002) (discussing creation and disclosure of a privilege log to further negotiations between the parties, where the subpoena appeared overbroad on its face and likely asked for privileged materials). In the alternative, the district court in Mississippi could order the Rigsbys to consent to AOL's disclosing the contents of their e-mails under the pain of sanctions. FED.R.CIV.P. 37; *O'Grady*, 44 Cal.Rptr.3d at 88. Furthermore, the district court in Mississippi could conduct an in camera review of the documents that State Farm requested from AOL. *See Hohenwater v. Roberts Pharm. Corp.*, 152 F.R.D. 513, 515 (D.S.C.1994) (conducting an in camera review and finding that both the attorney-client privilege and the work product privilege apply to the documents at issue). But *see Vaughan*, 156 F.R.D. at 125 (declining in camera review of the parties' documents where the parties' failed to provide in their privilege log a *Vaughan* index or specific points regarding why each document was or was not privileged).

End of Document

KeyCite Yellow Flag - Negative Treatment
Declined to Extend by Apple Inc. v. Superior Court, Cal., February 4, 2013

139 Cal.App.4th 1423
Court of Appeal, Sixth District, California.

Jason O'GRADY et al., Petitioners,
v.
The SUPERIOR COURT of Santa Clara County, Respondent;
Apple Computer, Inc., Real Party in Interest.

No. H028579. | May 26, 2006.
| As Modified June 23, 2006.

Synopsis
Background: Computer manufacturer filed action against Web site publishers alleging they published confidential company information about an impending product, and seeking to identify the source of the disclosures. The Santa Clara County Superior Court, No. CV032178, James Kleinberg, J., granted manufacturer authority to issue civil subpoenas to publishers, and denied publishers motion for a protective order, Publishers petitioned for writ of mandate.

Holdings: The Court of Appeal, Rushing, P.J., held that:

[1] Stored Communications Act (SCA) prohibited disclosure;

[2] Web sites were periodicals under reporter's shield law; and

[3] manufacturer failed to exhaust other means of obtaining information.

Writ issued.

West Headnotes (22)

[1] **Mandamus**
Existence and Adequacy of Other Remedy in General
Mandamus
Proceedings in civil actions in general

Although review of discovery rulings by extraordinary writ is disfavored, extraordinary review will be granted when a discovery ruling plainly threatens immediate harm, such as loss of a privilege against disclosure, for which there is no other adequate remedy, or where the case presents an opportunity to resolve unsettled issues of law and furnish guidance applicable to other pending or anticipated cases.

6 Cases that cite this headnote

[2] **Mandamus**
Proceedings in civil actions in general

Review by extraordinary writ was proper and warranted in case raising several novel and important issues affecting the rights of web publishers to resist discovery of unpublished material, and the showing required of an employer who seeks to compel a newsgatherer to identify employees alleged by the employer to have wrongfully disclosed its trade secrets, and also raising issues of First Amendment rights and privileges. U.S.C.A. Const.Amend. 1.

5 Cases that cite this headnote

[3] **Telecommunications**
Computer communications

Under the Stored Communications Act (SCA), which provides that a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service, the exception for disclosures that "may be necessarily incident to the protection of the rights or property of the provider of that service," did not apply to web publisher resisting discovery by subpoena of unpublished material sought by employer to compel publisher to identify employees alleged by the employer to have wrongfully disclosed its confidential information. 18 U.S.C.A. § 2702(b)(5).

10 Cases that cite this headnote

[4] **Telecommunications**

Computer communications

Under the Stored Communications Act (SCA), which provides that a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service, safe harbor provision is intended to protect service providers who would otherwise be faced with a seemingly valid coercive process to disclose protected information or face liability under the SCA; it does not make compliance with such process lawful, but excuses the provider from the consequences of an unlawful act taken in good faith. 18 U.S.C.A. § 2707.

3 Cases that cite this headnote

[5] **Statutes**

Plain Language; Plain, Ordinary, or Common Meaning

Statutes

Unintended or unreasonable results; absurdity

Statutes

Relation to plain, literal, or clear meaning; ambiguity

The starting point in discerning congressional intent is the existing statutory text, and when the statute's language is plain, the sole function of the courts, at least where the disposition required by the text is not absurd, is to enforce it according to its terms.

Cases that cite this headnote

[6] **Statutes**

Relation to plain, literal, or clear meaning; ambiguity

If giving statutory terms their natural significance produces an unreasonable result plainly at variance with the policy of the legislation as a whole, then courts will examine the reason of the enactment and inquire into its antecedent history and give it effect in accordance with its design and purpose, sacrificing, if necessary, the literal meaning in order that the purpose may not fail.

Cases that cite this headnote

[7] **Telecommunications**

Computer communications

Since the Stored Communications Act (SCA), which prohibits any disclosure of stored e-mail other than as authorized by enumerated exceptions, makes no exception for civil discovery and no repugnancy has been shown between a denial of such discovery and congressional intent or purpose, the SCA must be applied, in accordance with its plain terms, to render unenforceable subpoenas in civil suit seeking to compel disclosure of the contents of e-mails containing company's confidential information stored on providers' facilities. 18 U.S.C.A. § 2701 et seq.

See 4 Witkin & Epstein, Cal. Criminal Law (3d ed. 2000) Illegally Obtained Evidence, § 87.

12 Cases that cite this headnote

[8] **Telecommunications**

Computer communications

The Stored Communications Act (SCA), which prohibits any disclosure of stored e-mail other than as authorized by enumerated exceptions, 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.A. § 2703(c)(1).

3 Cases that cite this headnote

[9] **Telecommunications**

Computer communications

Business that stored e-mail was entitled to a protective order barring computer maker from obtaining discovery by subpoena of stored material in violation of the Stored Communications Act (SCA), which prohibits any disclosure of stored e-mail other than as authorized by enumerated exceptions; controversy was ripe for adjudication since

business had been made target of discovery by computer maker's securing orders authorizing it to conduct discovery by civil subpoena against it, thereby ending any speculation about its intention to seek discovery and creating a concrete dispute concerning its right to do so. 18 U.S.C.A. § 2701 et seq.

6 Cases that cite this headnote

[10] **Action**

Moot, hypothetical or abstract questions

A controversy is not deemed ripe for adjudication unless it arises from a genuine present clash of interests and the operative facts are sufficiently definite to permit a particularistic determination rather than a broad pronouncement rooted in abstractions.

4 Cases that cite this headnote

[11] **Privileged Communications and Confidentiality**

Journalists

Protections of reporter's shield law extended to compelled disclosure of e-mail storage company's sources or any other unpublished material in their possession relating to computer maker's confidential information about impending product obtained anonymously; even if company merely reprinted verbatim copies of internal information while exercising no editorial oversight, that furnished no basis for denying company the protection of the statute. West's Ann.Cal. Const. Art. 1, § 2(b); West's Ann.Cal.Evid.Code § 1070(a).

Cases that cite this headnote

[12] **Appeal and Error**

Cases Triable in Appellate Court

Controversy that turned on questions of statutory interpretation was subject to review entirely independent of the trial court's ruling, and because it implicated interests in freedom of expression, Court of Appeal would review all subsidiary issues, including factual ones, independently in light of the whole record; while this standard did not permit an original evaluation of controverted live testimony, it was the equivalent of de novo review where the trial court decided the case on a paper record fully duplicated before the reviewing court.

1 Cases that cite this headnote

[13] **Privileged Communications and Confidentiality**

Journalists

Under the reporter's shield law, which protects unpublished material from disclosure, the phrase "newspaper, magazine, or other periodical publication," was applicable to a news-oriented Web site that gathered news for that purpose by the site's operators; such sites differ from traditional periodicals only in their tendency, which flows directly from the advanced technology they employ, to continuously update their content. West's Ann.Cal. Const. Art. 1, § 2(b); West's Ann.Cal.Evid.Code § 1070(a).

4 Cases that cite this headnote

[14] **Statutes**

Contemporary and Historical Circumstances

In construing an ambiguous statute, courts will attempt to ascertain the Legislature's purpose by taking its words in the sense in which they were understood at the time the statute was enacted.

1 Cases that cite this headnote

[15] **Statutes**

General and specific terms and provisions; ejusdem generis

Under the canon of statutory interpretation known as ejusdem generis, where general words follow the enumeration of particular classes of persons or things, the general words will be construed as applicable only to persons or things of the same general nature or class as those enumerated.

7 Cases that cite this headnote

[16] **Constitutional Law**
Disclosure of sources
Privileged Communications and Confidentiality
Journalists

The gist of the confidential source privilege is that a newsgatherer cannot to be compelled to divulge the identities of confidential sources without a showing of need sufficient to overbalance the inhibitory effect of such disclosure upon the free flow of ideas and information which is the core object of the guarantees of free speech and press. U.S.C.A. Const.Amend. 1; West's Ann.Cal. Const. Art. 1, § 2(b).

Cases that cite this headnote

[17] **Appeal and Error**
Review of constitutional questions
Appeal and Error
Cases Triable in Appellate Court
Appeal and Error
Effect of findings below

Under constitutional fact review, when a Federal right has been denied as the result of a factual finding or where a conclusion of law as to a Federal right and a finding of fact are so intermingled as to make it necessary, in order to pass upon the Federal question, to analyze the facts, the reviewing court must independently review these findings, and facts that are germane to the First Amendment analysis must be sorted out and reviewed de novo, independently of any previous determinations by the trier of fact; the reviewing court must examine for itself the statements in issue and the circumstances under which they were made to see whether they are of a character which the principles of the First Amendment protect. U.S.C.A. Const.Amend. 1.

1 Cases that cite this headnote

[18] **Privileged Communications and Confidentiality**
Journalists

In a civil action a reporter, editor, or publisher has a qualified privilege to withhold disclosure of the identity of confidential sources and of unpublished information supplied by such sources; the scope of that privilege in each particular case will depend upon the consideration and weighing of a number of interrelated factors.

Cases that cite this headnote

[19] **Privileged Communications and Confidentiality**
Journalists

Under the confidential source privilege, a news-oriented Web site that gathers news for that purpose by the site's operators are reporters, editors, or publishers for purposes of the privilege. West's Ann.Cal. Const. Art. 1, § 2(b); West's Ann.Cal.Evid.Code § 1070(a).

2 Cases that cite this headnote

[20] **Privileged Communications and Confidentiality**
Journalists

The scope of the newsgatherer's privilege depends on several factors, including the nature of the litigation and whether the reporter is a party, the relevance of the information sought to plaintiff's cause of action, the extent to which the party seeking disclosure of confidential sources has exhausted all alternative sources of obtaining the needed information, the importance of protecting confidentiality in the case at hand, and in a libel case, whether plaintiff made a prima facie case that the challenged statements were false. West's Ann.Cal. Const. Art. 1, § 2(b); West's Ann.Cal.Evid.Code § 1070(a).

Cases that cite this headnote

[21] **Privileged Communications and Confidentiality**
Journalists

Compulsory disclosure of confidential sources is the last resort under the confidential source privilege, permissible only when the party

seeking disclosure has no other practical means of obtaining the information. West's Ann.Cal. Const. Art. 1, § 2(b); West's Ann.Cal.Evid.Code § 1070(a).

Cases that cite this headnote

[22] Privileged Communications and Confidentiality

Trade secrets; commercial information

In action by computer manufacturer against Web site publishers alleging they published confidential company information about an impending product, manufacturer was not entitled to a subpoena to compel publishers to identify the source of the disclosures, obtained anonymously, where manufacturer failed to demonstrate that it could not identify the sources of the challenged information by means other than compelling publishers to disclose unpublished information.

See Weil & Brown, Cal. Practice Guide: Civil Procedure Before Trial (The Rutter Group 2005) ¶ 8:342.2 (CACIVP Ch. 3-C.).

2 Cases that cite this headnote

Attorneys and Law Firms

****76** Law Offices of Richard R. Wiebe, Richard R. Wiebe, San Francisco, Tomlinson Zisko, Thomas E. Moore, III, Palo Alto, Electronic Frontier Foundation, Kurt B. Opsahl, Kevin S. Bankston, Los Angeles, for Petitioner Jason O'Grady et al.

O'Melveny & Myers, George A. Riley, David R. Eberhart, Dhaivat H. Shah, San Francisco, James A. Bowman, Los Angeles, Ian N. Ramage, San Francisco, for Real Party in Interest Apple Computer Inc.

Thomas W. Newton, San Francisco, James W. Ewert, for Amicus Curiae for Petitioner California Newspaper Publishers Assoc.

Lucy D. Dalglish, Gregg P. Leslie, Grant D. Penord, for Amicus Curiae for Petitioner Reporters Committee for Freedom of the Press.

Center for Internet & Society, Lauren Gelman, Stanford, for Amicus Curiae for Petitioner Center for Internet & Society.

Paumilia & Adamec, Justene Adamec, Pasadena, WLF The Williams Law Firm, J. Craig Williams, Newport Beach, Enterprise Counsel Group, Jeffrey Lewis, Benjamin P. Pugh, Irvine, for Amicus Curiae for Petitioner Bear Flag League.

Akin Gump Strauss Hart & Feld, Elizabeth H. Rader, San Francisco, for Amicus Curiae for Petitioner United States Internet Society et al.

Keker & Van Nest, Michael D. Celio, Steven A. Hirsch, Clement S. Roberts, San Francisco, for Amicus Curiae for Real Party in Interest Genetech, Inc.

Ann Brick, San Francisco, for Amicus Curiae for Real Party in Interest ACLU.

Perkins Coie Brown & Bain, Dan L. Bagatell, Joel W. Nomkin, Phoenix, AZ, Covington & Burling, Sonja D. Winner, San Francisco, for Amicus Curiae for Real Party in Interest Intel Corp., et al.

Quinn Emanuel Urquhart, etc., Robert W. Stone, Kathleen M. Sullivan, Redwood Shores, for Amicus Curiae for Real Party in Interest Information Technology Industry Council.

Opinion

RUSHING, P.J.

***1431** Apple Computer, Inc. (Apple), a manufacturer of computer hardware and software, brought this action alleging that persons unknown caused the wrongful publication on the World Wide Web of Apple's secret plans to release a device that would facilitate the creation of digital live sound recordings on Apple computers. In an effort to identify the source of the disclosures, Apple sought and obtained authority to issue civil subpoenas to the publishers of the Web sites where the information appeared and to the email 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 ****77** secret. We hold that this was error ***1432** because (1) the subpoena to the email 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*)). Accordingly, we will issue a writ of mandate directing the trial court to grant the motion for a protective order.

FACTUAL AND PROCEDURAL BACKGROUND

Petitioner Jason O'Grady declared below that he owns and operates "O'Grady's PowerPage" an "online news magazine" devoted to news and information about Apple Macintosh computers and compatible software and hardware. PowerPage has its principal place of business in Abington, Pennsylvania, and has been published daily since 1995. O'Grady acts as its publisher and one of nine editors and reporters. Since 2002 the site has occupied its present address on the World Wide Web, where it publishes 15 to 20 items per week. Over the two years preceding the execution of the declaration, the Web site received an average of 300,000 unique visits per month. [1]

Under the pseudonym "Kasper Jade," a person identifying himself as "primary publisher, editor and reporter" for Apple Insider declared that Apple Insider is an "online news magazine" devoted to Apple Macintosh computers and related products. [2] He identified petitioner Monish Bhatia as the publisher of "Mac News Network," which provides hosting services to a number of Web sites, including "Apple Insider." Apple Insider has published "daily or near-daily technology news" at the same web address since 1998 at an average rate of seven to 15 articles per week. In July 2004, it received 438,000 unique visitors.

Over a period of several days in November 2004, PowerPage and Apple Insider published several articles concerning a rumored new Apple product ***1433** known as Asteroid or Q97. The first article appeared on PowerPage on November 19, 2004, with O'Grady's byline. It stated that PowerPage had "got [ten] it's [*sic*] hands on this juicy little nugget about a new FireWire breakout box for GarageBand that Apple plans to announce at MacWorld Expo SF 2005 in January." [3] The article ****78** described a device that permitted the user of an Apple computer to record analog audio sources, such as microphones or guitars, using an existing Apple application known as GarageBand, the primary function of which is to facilitate the production of digital audio recordings. [4] The article included a drawing of a smallish box with a few input/output connectors. Next to the drawing was a list of further details: "FW [i.e., FireWire] based audio input device," "[t]wo inputs, two outputs," "powered from FireWire," "[s]oftware driven input gain control," and "[l]imiter circuit to automatically prevent 'clipping.' "

On the following Monday, November 22, 2004, PowerPage published an article entitled "Apple's Asteroid Breakout Box Part II: Product Details," also with O'Grady's byline. It gave additional product details plus a "[t]arget price," "[t]arget intro date," and "[t]arget intro q[uanti]ty." Also included was a "concept drawing," attributed to "Bob Borries," which diverged substantially from the simple box depicted in the first article, more nearly resembling a small audio mixing board.

On November 23, 2004, PowerPage ran another article by O'Grady addressing Asteroid's integration into GarageBand. The article said, "Today we have some juice on new GarageBand functionality for extremely easy setup, recording and playback through Asteroid." It listed a number of details concerning the anticipated integration.

Also on November 23, 2004, an article appeared on the Apple Insider site, authored by "Kasper Jade," entitled "Apple developing FireWire audio interface for GarageBand." It stated that the device would "allow users to directly record audio using any Mac and Apple's GarageBand music studio application," and that "[a]ccording to reputable sources, the company is on track to begin manufacturing the device overseas next month." Included was an "[a]rtist rendition" of the device "based on Apple prototype design and ... likely [to] change." The illustration was attributed to "Paul Scates," whose ***1434** email address was provided. The article recapitulated the technical details noted on the PowerPage site, adding that "a more advanced version" of the device had been "recently seen floating around the [*sic*] Apple's Cupertino campus" with an additional output port of a stated type. The article stated that it was "unclear which version the company will ultimately send to manufacturing." It noted that the device, "code-named 'Q97' or 'Asteroid,' " had been "under development" for "the better part of a year." It reported some details concerning the history of the product, identified a named Apple subsidiary as having participated in its design, and named a company with whom Apple had

already contracted for its manufacture. The article stated that a production run of a specified number of units was to occur in a matter of weeks and that the product would probably be announced at an upcoming trade show. It specified a price range for the product and stated that it would "aggressively target similar products," examples of which were provided. Even at the upper end of its anticipated price range, the article opined, the product would "represent one of the lowest priced FireWire breakout boxes on the market...." Allusion was also made to "internal company estimates" concerning expected quarterly earnings from the product.

****79** On November 26, 2004, PowerPage ran "Part IV" of its series on Asteroid, entitled "What's it all mean?" The article was bylined "Dr. Teeth and the Electric Mayhem." It alluded to an "article at createddigitalmusic," to which a hypertext link was provided, which had gone "further into the rumored Apple audio interface Asteroid, as reported here on PowerPage." Readers were advised not to "get too excited, as this hardware is similar to hardware already available, though you can probably expect a very cool box and some new software integration features ... that may ultimately benefit even competitive audio interfaces...." "Dr. Teeth" wrote that the device reflected in the "concept" drawing in the November 22, 2004 article was "probably more interesting than the product that's actually coming," as to which "[i]nside reports suggest ... a simple 2–in, 2–out box, NOT a control surface with knobs and faders...." The image shown in Apple Insider was said to be "probably dead-on" in making the product "Apple white," and "appears to be adapted from the same prototype image posted on the PowerPage," though it got one detail wrong, i.e., it showed one type of connector while "rumored specs" pointed to another, more adaptable connector type. "Dr. Teeth" observed that the product might "pave the way for future interfaces," but "only if Apple decides it wants to compete in an already-oversaturated pro market. At the entry level, Apple has one major advantage: there's nothing pretty or particularly friendly to new users, meaning this is in fact a ripe opportunity for the company's ongoing push to make Mac THE computer of ***1435** music-making." Finally, "Dr. Teeth" endorsed the suggestion by createddigitalmusic that "the codename here is credible, too: Asteroid is a play on the video game Breakout—as in audio breakout box."[5]

According to declarations later filed by Apple investigators, much of the published information appears to have originated in "an electronic presentation file—or 'slide stack,' " generated by Apple and "conspicuously marked as 'Apple Need–to–Know Confidential.' " The investigators note "striking similarities between the Confidential Slides and the articles posted on PowerPage and AppleInsider," as detailed in a portion of the declarations that remains sealed. Perhaps most telling of these similarities is an image from the presentation file that looks identical to the drawing published on PowerPage on November 19, 2004, except that the latter bears the superimposed legend "www.powerpage.org" and lacks the caption "Apple Need to Know Confidential," which appears under the image in the presentation file. Various other parts of the file are closely paraphrased, and in some cases echoed verbatim, in the articles, particularly the PowerPage articles. However, those articles also contained information not attributed by Apple to the presentation file, notably the alternative, more complex design drawing. Nor did the Apple Insider articles appear to contain comparably striking similarities to the presentation file. In particular, the drawing there was designated an "Artist rendition" and attributed ****80** to one Paul Scates, whose email address was given. It differed from the drawing in the presentation file in several particulars, i.e., it was a different color, viewed from a different angle, and appeared to have slightly different connectors.[6]

On or about December 8, 2004, O'Grady received an email from an attorney for Apple who referred to the appearance on PowerPage of "references to an unreleased Apple product, namely the ['']Asteroid.['']" Citing the four articles described above, he demanded that O'Grady remove "all references to this product." He asserted, "The information in these posts and accompanying comments constitutes trade secrets that you have published without Apple['']s authorization.... It appears that you may be engaged in a ***1436** practice of soliciting and disseminating such trade secrets. Apple also demands that you provide all information available to you regarding the sources for the posting and comments identified above...."

On December 13, 2004, Apple filed a complaint against "Doe 1, an unknown individual," and "Does 2–25," whom it described as unidentified persons or entities. The gist of the claim was that one or more unidentified persons, presumably the defendants, had "misappropriated and disseminated through web sites confidential information about an unreleased product...." Such information, Apple alleged, constitutes a trade secret: It possesses commercial and competitive value that would be impaired by disclosure in that, if it is revealed, "competitors can anticipate and counter Apple's business strategy, and Apple loses

control over the timing and publicity for its product launches." Therefore, Apple alleged, it "undertakes rigorous and extensive measures to safeguard information about its unreleased products." All Apple employees sign an agreement acknowledging that product plans are " 'Proprietary Information' " and that " 'employment by Apple requires [employees] to keep all Proprietary Information in confidence and trust for the tenure of [their] employment and thereafter, and that [they] will not use or disclose Proprietary Information without the written consent of Apple....' "

Apple alleged that Doe 1, acting alone or with others, misappropriated a trade secret by "post[ing] technical details and images of an undisclosed future Apple product on publicly accessible areas of the Internet." This information, alleged Apple, "could have been obtained only through a breach of an Apple confidentiality agreement." Apple alleged that the unauthorized use and distribution of the information constituted a violation of California's trade secret statute. It prayed for compensatory and exemplary damages, and other relief.

Along with the complaint Apple filed an ex parte application for commissions and orders empowering it to "serve Subpoenas on Powerpage.org, Appleinsider.com, Thinksecret.com and any Internet service providers or other persons or entities identified in the information and testimony produced by Powerpage.org, Appleinsider.com, and Thinksecret.com." The stated basis for the application was that "the true identities of the defendants in this action cannot be ascertained without these subpoenas." The application was accompanied by a request that it and the supporting declarations be filed under seal. The ****81** trial court entered an order sealing the documents. The court then granted the application for discovery, authorizing Apple "to serve subpoenas, whether through use of commissions or in-state process, on Powerpage.com, Appleinsider.com, and Thinksecret.com for documents that may lead to the identification of the proper defendant or defendants in this action."

***1437** On February 4, 2005, Apple filed a further ex parte application seeking authorization to direct discovery to Nfox.com and Karl Kraft. Counsel for Apple declared that Kraft had contacted one of Apple's attorneys as a result of news reports about this lawsuit. Kraft said that his company, Nfox.com, hosted the email account for PowerPage, and that numerous emails in the account contained the word " 'Asteroid.' "[7] He said he would forward copies of these messages, and other relevant documents, to counsel. Apple sought to subpoena the materials, declared counsel, because Kraft had failed to send them voluntarily. Apple sought leave to subpoena "those materials and any other documents revealing the identities of the defendants in this case."

The trial court granted the application, authorizing issuance of subpoenas requiring Nfox.com and Karl Kraft to produce "[a]ll documents relating to the identity of any person or entity who supplied information regarding an unreleased Apple product code-named 'Asteroid' or 'Q97,' " all documents identifying any such disclosing persons, all communications to or from them relating to the product, and all images received from or sent to them. The clerk duly issued a commission for such subpoenas. Counsel for Apple caused subpoenas and deposition notices to issue against Nfox and Kraft under both California and Nevada law. The parties later stipulated that these instruments were served on Nfox and Kraft on February 4 and 10, 2005, commanding compliance on February 24 and 25, 2005.

On February 14, 2005, petitioners Monish Bhatia, Jason O'Grady, and "Kasper Jade" moved for a protective order to prevent the discovery sought by Apple on the grounds that (1) their "sources and unpublished information" were "protected under the reporter's shield embodied in both Article I, section 2(b) of the California Constitution and in California Evidence Code Section 1070"; (2) the information was also protected by "the reporter's privilege under the First Amendment of the United States Constitution," which excused petitioners "from disclosing the source of any information procured in connection with [their] journalistic endeavors"; and (3) the subpoenas already issued against Nfox and Kraft could not be enforced without violating the Stored Communications Act (18 U.S.C. § 2702(a)(1)). In support of the motion, O'Grady and Jade each declared that he had "received information about Asteroid contained in my article from a confidential source or sources."

Apple opposed the motion on the grounds that (1) the newsgatherer's privilege does not apply to trade secret misappropriation as described in the ***1438** complaint; (2) if the privilege applies, it is overcome by Apple's compelling need for the information; (3) the California reporter's shield provides only an immunity from contempt, not a ground for opposing ****82** discovery; (4) petitioners are not protected by the California shield law in any event; (5) there was no right to anonymous speech under the circumstances; and (6) insofar as petitioners' motion concerned discovery other than

the subpoenas to Kraft and Nfox, it was premature, and sought an advisory opinion, because no other discovery had actually been undertaken.

The court denied petitioners' motion for a protective order. In a written statement of reasons, the court first declined to reach the merits with respect to any discovery other than the subpoena served on Nfox and Kraft. It noted that no other discovery was "currently outstanding," and opined that any determination as to the propriety of such discovery would constitute an " 'advisory ruling.' " With respect to the Nfox/Kraft subpoenas, the court found that much of the information posted on PowerPage had been "taken from a confidential set of slides clearly labeled 'Apple Need–to–Know Confidential,' " and that therefore, "this action has passed the thresholds necessary for discovery to proceed." The court found petitioners' assertion of a constitutional privilege "overstated" because "[r]eporters and their sources do not have a license to violate criminal laws such as Penal Code [section] 499c."[8] The court assumed petitioners to be journalists, but wrote that "this is not the equivalent of a free pass" and that they could still be compelled to reveal information relating to a crime. The court repeatedly alluded to the supposed presence of criminal or larcenous conduct. The court also faulted petitioners for failing to establish "what public interest was served" by the publications in question. While acknowledging evidence that thousands of people were interested in the information in question, the court opined that "an *interested public* is not the same as the *public interest.*" The court implied that the publications in question were not " 'protected speech.' "

Petitioners brought this proceeding for a writ of mandate or prohibition to compel the trial court to set aside its denial of the motion for protective order. ***1439** After receiving preliminary opposition and numerous amicus curiae briefs on behalf of both sides, we issued an order to show cause.

DISCUSSION

I. *Appropriateness of Writ Review*

[1] Rulings on discovery matters are rarely the subject of review by extraordinary writ. Such rulings are typically vested in the trial court's discretion, and even if an abuse can be shown it is often impossible for the aggrieved party to establish grounds for interlocutory intervention. At the same time, discovery issues are often vigorously contested, raising a well-grounded concern that too great a willingness to grant extraordinary review would quickly magnify appellate caseloads beyond any level that could be justified by corresponding benefits. Accordingly, the review of discovery rulings by extraordinary writ is disfavored. (*Raytheon Co. v.* ****83** *Superior Court* (1989) 208 Cal.App.3d 683, 686, 256 Cal.Rptr. 425; see *Oceanside Union School Dist. v. Superior Court* (1962) 58 Cal.2d 180, 185–186, fn. 4, 23 Cal.Rptr. 375, 373 P.2d 439.)

Extraordinary review will be granted, however, when a discovery ruling plainly threatens immediate harm, such as loss of a privilege against disclosure, for which there is no other adequate remedy (e.g., *Raytheon Co. v. Superior Court, supra,* 208 Cal.App.3d at p. 686, 256 Cal.Rptr. 425), or where the case presents an opportunity to resolve unsettled issues of law and furnish guidance applicable to other pending or anticipated cases (*Oceanside Union School Dist. v. Superior Court, supra,* 58 Cal.2d at pp. 185–186, fn. 4, 23 Cal.Rptr. 375, 373 P.2d 439; see *Toshiba America Electronic Components v. Superior Court* (2004) 124 Cal.App.4th 762, 767, 21 Cal.Rptr.3d 532).

[2] Both of these principles appear applicable here. This case raises several novel and important issues affecting the rights of web publishers to resist discovery of unpublished material, and the showing required of an employer who seeks to compel a newsgatherer to identify employees alleged by the employer to have wrongfully disclosed its trade secrets. In part because of these issues and their implications for the privacy of internet communications, the First Amendment status of internet news sites, and the protection of trade secrets, the case has generated widespread interest within the technology sector, the digital information industry, internet content providers, and web and email users. The case also involves an attempt to undermine a claimed constitutional privilege, threatening a harm for which petitioners, if entitled to the privilege, have no adequate remedy at law. (See *Rancho Publications v. Superior Court* (1999) 68 Cal.App.4th 1538, 1542, 81 Cal.Rptr.2d 274(*Rancho Publications*).) Accordingly, review by extraordinary writ is proper and warranted.

*1440 II. *Stored Communications Act*

A. Applicability

We first consider whether the trial court should have quashed, or granted a protective order against, the subpoenas Apple served on Nfox and Kraft, the email service providers for petitioners O'Grady and PowerPage. The dispositive issue

is whether the disclosures sought by those subpoenas are prohibited by the Electronic Communications Privacy Act (Pub. Law 99–508 (Oct. 21, 1986) 100 Statutes 1860 et seq.), and specifically the chapter thereof entitled Stored Wire and Electronic Communications and Transactional Records Access (Pub. Law 99–108 (Oct. 21, 1986) 100 Stats. 1848, 1860–1868, § 201; 18 U.S.C. §§ 2701–2712), often known as the Stored Communications Act (SCA or Act). (See Stuckey, Internet and Online Law (2005) § 5.03[1][a], pp. 5–24–5–24.1 (rel.18).)

The SCA declares that, subject to certain conditions and exceptions, "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service...." (18 U.S.C. § 2702(a)(1).) Similarly, but subject to certain additional conditions, "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service...." (18 U.S.C. § 2702(a)(2).)

Petitioners contend that these provisions invalidate the subpoena to Nfox and Kraft under the Supremacy Clause (U.S. Const., art. VI, cl.2). It seems plain, and Apple **84 does not appear to dispute, that the basic conditions for application of the SCA are present: Kraft is a person, and Nfox is an entity, "providing an electronic communication service to the public." (18 U.S.C. § 2702(a)(1); see 18 U.S.C. 2510(15).) Nor has Apple tried to show that the contents of PowerPage's email account were not "communication[s] ... in electronic storage by" Nfox and Kraft. [9] (18 U.S.C. § 2701(a)(1); see 18 U.S.C. § 2510(17).) We therefore turn to Apple's contentions that the disclosures *1441 sought here come within enumerated exceptions to the SCA, and that the SCA should be understood not to apply to civil discovery, which it was not intended to impede.

Because the issues thus joined are entirely ones of law, we exercise our independent judgment in addressing them, and accord no deference to the trial court's ruling. (*People ex rel. Lockyer v. Sun Pacific Farming Co.* (2000) 77 Cal.App.4th 619, 632, 92 Cal.Rptr.2d 115; see *Enea v. Superior Court* (2005) 132 Cal.App.4th 1559, 1563, 34 Cal.Rptr.3d 513.)

B. Protection of Service Provider's Interests

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)).

Apple contends that compliance with a civil discovery subpoena falls within the SCA's exception for disclosures that "may be necessarily incident ... to the protection of the rights or property of the provider of that service...." (18 U.S.C. § 2702(b)(5).) The argument apparently proceeds as follows: (1) Noncompliance with a subpoena would expose the service provider to contempt or other sanctions; (2) such exposure is a threat to the provider's rights or property; (3) therefore, compliance with a subpoena tends to protect the provider's rights or property. The first premise introduces a circularity by supposing that noncompliance with the subpoena can support legal sanctions. **85 This premise is sound only where the subpoena is enforceable. A subpoena is not enforceable if compliance would violate the SCA. Any disclosure violates the SCA unless it falls within an enumerated exception to general prohibition. The exception posited by Apple necessarily presupposes that the disclosure falls within an exception. In logical terms, the antecedent assumes the consequents.

*1442 Ironically, Apple accuses petitioners of circular reasoning when they point out that if a contemplated disclosure is not authorized by the Act, the refusal to disclose cannot subject Nfox and Kraft to sanctions, and the disclosure cannot be incidental to the protection of their interests. This is at best a "tu quoque" argument, seeking to excuse the circularity in Apple's argument by accusing petitioners of the same vice. But in fact petitioners' argument is sound, while Apple's is not.

[3] The most that could be said in Apple's support is that a service provider might incur *costs* in defending against an invalid subpoena, and that compliance might be viewed as

"necessarily incident" to protecting the provider's "property" by avoiding such costs. (18 U.S.C. § 2702(b)(5).) We seriously doubt that the language of the statute could support such a reading, which is nowhere expressly urged by Apple or its amici. The effect of such an interpretation would be to permit disclosure whenever someone threatened the service provider with litigation. Arguably even a subpoena would be unnecessary; the mere threat would be enough. Further, it is far from apparent that compliance with an invalid subpoena would save the provider any money, since it might expose the provider to a civil suit by an aggrieved user. (See 18 U.S.C. § 2707(e).) There is no reason to suppose that the defense of such a suit would be less expensive than resistance to an invalid subpoena.

C. Safe Harbor

[4] Apple also invokes the safe harbor provisions of the SCA, under which a service provider's "good faith reliance on ... [¶] a court warrant or order ... [¶] is a complete defense to any civil or criminal action brought under" the SCA. (18 U.S.C. § 2707.) This provision is obviously intended to protect service providers who would otherwise find themselves between the Scylla of seemingly valid coercive process and the Charybdis of liability under the Act. It does not make compliance with such process lawful; it excuses the provider from the consequences of an unlawful act taken in good faith. In light of the legal uncertainties we here address, this provision might have afforded Nfox and Kraft a defense had they voluntarily complied with the subpoenas and then been charged with a violation of the Act. That hypothesis does not entitle Apple to invoke this provision to compel disclosures otherwise prohibited by the Act.

D. Implied Exception for Civil Discovery

Apple's primary argument for enforcing the subpoenas appears to be that Congress did not intend to "preempt" civil discovery of stored communications, and the Act should not be given that effect. Such commentary as we ***1443** have found supports a contrary conclusion. [10] However, there appears ****86** to be no judicial authority squarely addressing the issue. [11]

[5] Apple makes no attempt to persuade us that the language of the SCA can be read to expressly authorize disclosure pursuant to civil subpoenas like those served on Nfox and Kraft. This omission is telling, because "[t]he starting point in discerning congressional intent is the existing statutory text [citation].... '[W]hen the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.' [Citations.]" (*Lamie v. U.S. Trustee* (2004) 540 U.S. 526, 534, 124 S.Ct. 1023, 157 L.Ed.2d 1024; see *Helvering v. N.Y. Trust Co.* (1934) 292 U.S. 455, 464, 54 S.Ct. 806, 78 L.Ed. 1361 [in general, "where the statute contains no ambiguity, it must be taken literally and given effect according to its language"].)

Here there is no pertinent ambiguity in the language of the statute. It clearly prohibits any disclosure of stored email other than as authorized by enumerated exceptions. Apple would apparently have us declare an *implicit* exception for civil discovery subpoenas. But by enacting a number of quite particular exceptions to the rule of non-disclosure, Congress demonstrated that it knew quite well how to make exceptions to that rule. The treatment of rapidly developing new technologies profoundly affecting not only commerce but countless other aspects of individual and collective life is not a matter on which courts should lightly engraft exceptions to plain statutory language without a clear warrant to do so. We should instead stand aside and let the representative branch of government do its job. Few cases have provided a more appropriate occasion to apply the maxim *expressio unius exclusio alterius est,* under which the enumeration of things to which a statute applies is presumed to exclude things not mentioned. This principle was applied to a similar issue in *F.T.C. v. Netscape Communications Corp.* (N.D.Cal.2000) 196 F.R.D. 559, 561, where the court held that the Act's authorization for the disclosure of certain information to government agencies ***1444** under a *trial* subpoena did not permit disclosure under a civil *discovery* subpoena. Noting the well-recognized distinctions between trial and discovery subpoenas, the court found "no reason ... to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to. See *Leatherman v. Tarrant County Narcotics Intelligence and Coordination Unit,* 507 U.S. 163, 168, 113 S.Ct. 1160, 122 L.Ed.2d 517 (1993) (applying maxim of *expressio unius est exclusio alterius*)." (*Ibid.*)

[6] Of course, a statute must be read as a whole and in light of its " 'objects and policy' " so as to " 'carry into execution the will of the Legislature, as thus ascertained, according to its true intent and meaning.' " ****87** (*Helvering v. N.Y. Trust Co., supra,* 292 U.S. at p. 464, 54 S.Ct. 806.) If giving the statutory terms their " 'natural significance' " produces " 'an unreasonable result plainly at variance with

the policy of the legislation as a whole,' " then courts will " 'examine the matter further,' " " 'look[ing] to the reason of the enactment and inquir[ing] into its antecedent history and giv[ing] it effect in accordance with its design and purpose, sacrificing, if necessary, the literal meaning in order that the purpose may not fail.' " (*Id.* at pp. 464–465, 54 S.Ct. 806.) [12]

Apple provides no persuasive basis to conclude that the refusal of civil discovery would constitute an " 'unreasonable result plainly at variance with the policy of the legislation as a whole.' " (*Helvering v. N.Y. Trust Co., supra,* 292 U.S. at p. 464, 54 S.Ct. 806.) Apple asserts that the denial of civil discovery will not further the purpose of the SCA, which according to Apple is to "regulate governmental searches of email communications." But this is an unduly narrow reading of the legislative history. Apple quotes Congress's expressed intention "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." (Sen.Rep. No. 99–541, 2d Sess. (1986) reprinted in 1986 U.S.Code Cong. & Admin. News, p. 3557.) But the concluding phrase does not condition the opening one; on the contrary, it suggests an intent to protect the privacy of stored electronic communications *except where* legitimate law enforcement needs justify its infringement. The same report noted the desirability of inhibiting the "possible wrongful use and public disclosure [of stored information] by law enforcement authorities *as well as unauthorized private parties.*" (*Ibid.,* italics added.)

The report indicated that a fundamental purpose of the SCA is to lessen the disparities between the protections given to established modes of private communication and those accorded new communications media. It observed that while mail and telephone communications had long enjoyed a variety of ***1445** legal protections, there were no "comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology ... even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services." (Sen.Rep. No. 99–541, 2d Sess. (1986) reprinted in 1986 U.S.Code Cong. & Admin. News at p. 3559.) Among other ill effects, this absence of standards produced "legal uncertainty" and might operate to "unnecessarily discourage potential customers from using innovative communications systems" as well as to "discourage American businesses from developing new innovative forms of telecommunications and computer technology." (*Ibid.*) Congress thus sought not only to shield private electronic communications from government intrusion but also to encourage "innovative forms" of communication by granting them protection against unwanted disclosure *to anyone.* In the absence of a degree of privacy at least roughly comparable to that accompanying more traditional modes of communication, potential users might be deterred from using the new forms merely out of a feared inability to communicate in confidence.

****88** It bears emphasis that the discovery sought here is theoretically possible only because of the ease with which digital data is replicated, stored, and left behind on various servers involved in its delivery, after which it may be retrieved and examined by anyone with the appropriate "privileges" under a host system's security settings. Traditional communications rarely afforded any comparable possibility of discovery. After a letter was delivered, all tangible evidence of the communication remained in the sole possession and control of the recipient or, if the sender retained a copy, the parties. A telephone conversation was even less likely to be discoverable from a third party: in addition to its intrinsic privacy, it was as ephemeral as a conversation on a street corner; no facsimile of it existed unless a party recorded it—itself an illegal act in some jurisdictions, including California. (See Pen.Code, § 632.)

If an employee wished to disclose his employer's trade secrets in the days before digital communications, he would have to either convey the secret orally, or cause the delivery, by mail or otherwise, of written documents. In the case of oral communications there would be no facsimile to discover; in the case of written communication, the original and any copies would remain in the hands of the recipient, and perhaps the sender, unless destroyed or otherwise disposed of. In order to obtain them, a civil litigant in Apple's position would have had to identify the parties to the communication and seek copies directly from them. Only in unusual circumstances would there be any third party from whom such discovery might be sought.

***1446** Given these inherent traits of the traditional media of private communication, it would be far from irrational for Congress to conclude that one seeking disclosure of the contents of email, like one seeking old-fashioned written correspondence, should direct his or her effort to the parties to the communication and not to a third party who served only as

a medium and neutral repository for the message. Nor is such a regime as restrictive as Apple would make it sound. Copies may still be sought from the intermediary if the discovery can be brought within one of the statutory exceptions—most obviously, a disclosure with the consent of a party to the communication. (18 U.S.C. § 2702(b)(3).) Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions. (See U.S. Internet Service Providers Assn., Electronic Evidence Compliance—A Guide for Internet Service Providers, *supra,* 18 Berkeley Tech. L.J. 945, 965;*Miranda v. 21st Century Ins. Co.* (2004) 117 Cal.App.4th 913, 929, 12 Cal.Rptr.3d 159 [judgment of dismissal affirmed after claimant refused discovery order to sign authorization for release of medical records]; *Emerson Electric Co. v. Superior Court* (1997) 16 Cal.4th 1101, 1112, 68 Cal.Rptr.2d 883, 946 P.2d 841 [sanctions available against deponent who refuses to comply with order requiring him to perform demonstration or reenactment of accident].)

We also note the assertion by amicus United States Internet Industry Association (USIIA) that civil subpoenas are often served on service providers and that compliance with them would impose severe administrative burdens, interfering with the manifest congressional intent to encourage development and use of digital communications. The severity of this burden cannot be determined from this record, but the threat of routine discovery requests seems inherent in the implied exception sought by Apple, which would seemingly permit civil discovery from the ****89** service provider whenever its server is thought to contain messages relevant to a civil suit. Thus if a plaintiff had sent email to family members about injuries that later became the subject of a negligence case, the defendant could subpoena copies of the messages from not only the service provider for the plaintiff (who might be compelled to consent) but from those of the various family members. Responding to such routine subpoenas would indeed be likely to impose a substantial new burden on service providers. Resistance would likely entail legal expense, and compliance would require devoting some number of person-hours to responding in a lawful and prudent manner. Further, routine compliance might deter users from using the new media to discuss any matter that could conceivably be implicated in litigation—or indeed, corresponding with any person who might appear likely to become a party to litigation.

It would hardly be irrational of Congress to deflect such hazards by denying civil discovery of stored messages and relegating civil litigants to such discovery as they can obtain from or through their adversaries. On the ***1447** contrary, Congress could reasonably conclude that to permit civil discovery of stored messages from service providers without the consent of subscribers would provide an informational windfall to civil litigants at too great a cost to digital media and their users. Prohibiting such discovery imposes no new burden on litigants, but shields these modes of communication from encroachments that threaten to impair their utility and discourage their development. The denial of discovery here makes Apple no worse off than it would be if an employee had printed the presentation file onto paper, placed it in an envelope, and handed it to petitioners.

In other words, Congress could quite reasonably decide that an email service provider is a kind of data bailee to whom email is entrusted for delivery and secure storage, and who should be legally disabled from disclosing such data in response to a civil subpoena without the subscriber's consent. This does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data, not the bailee to whom it was entrusted.

[7] Since the Act makes no exception for civil discovery and no repugnancy has been shown between a denial of such discovery and congressional intent or purpose, the Act must be applied, in accordance with its plain terms, to render unenforceable the subpoenas seeking to compel Kraft and Nfox to disclose the contents of emails stored on their facilities.

E. Disclosure Limited to Sender's Identity

[8] Amicus curiae Genentech, Inc. (Genetech), argues that the SCA does not impede enforcement of the subpoenas to Kraft and Nfox because it prohibits only the disclosure of "contents of a communication" (18 U.S.C. § 2702(a)(1)) and explicitly permits a service provider to disclose, to a non-governmental entity, "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)). According to Genentech, the subpoenas here do not offend the Act's prohibitions because (1) they seek only the identity of an author of a stored communication and (2) the Act expressly authorizes such disclosure.

Both premises are incorrect. Apple seeks much more than the identity of the author or authors of specified emails. Its subpoenas to Nfox and Kraft demand "[a]ll ****90** *documents relating to* the identity of any person or

entity who supplied information regarding an unreleased Apple product code-named 'Asteroid' or 'Q97' ...," including not only "documents identifying ... individuals who provided information relating to the Product ('Disclosing ***1448** Person(s)')," but also "*all communications from or to any Disclosing Person(s)* relating to the Product." [13]

Moreover, the logical effect of *any* affirmative response to Apple's subpoena would be to disclose the contents of communications by confirming that there are in fact stored messages on the system relating to Asteroid. Conceptually the situation resembles one in which an attorney is asked to identify all persons who sought advice on a specified legal issue, or a doctor to identify all patients who sought treatment for a specified affliction. Compliance with such an inquiry operates by simple logic to disclose the contents of privileged communications. (See *Rosso, Johnson, Rosso & Ebersold v. Superior Court* (1987) 191 Cal.App.3d 1514, 1519, 237 Cal.Rptr. 242 [although client's identity usually not considered privileged, list of persons who contacted the firm about particular medical device was shielded from disclosure because it "would reveal the nature of a medical problem, ordinarily considered a confidential communication"].) Here, any identification of senders of messages concerning Asteroid would necessarily tend to disclose the "contents" of messages authored by those senders. (See 18 U.S.C. § 2510(8) [" 'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"].)

Further, the Act 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.) Apple already knows the identities of the subscribers to the Nfox accounts: O'Grady and PowerPage. By seeking to identify the sender of communications *to* the subscriber, or the addressee of communications *from* the subscriber, Apple steps well outside the statutory authorization.

Genentech's misreading of the Act is reflected in its attempt to analogize this case to *Jessup–Morgan v. America Online, Inc.* (E.D.Mich.1998) 20 F.Supp.2d 1105(*Jessup–Morgan*), where the court held that the SCA did not prevent a service provider from disclosing the identity of a *subscriber* who had "post[ed] publicly on the Internet" a malicious message about another person. (*Id.* at p. 1106, italics added.) Relying on the plain statutory language, the court distinguished between "[t]he 'content' of a communication" and "information identifying an ... account customer," which is what was disclosed there. (*Id.* at p. 1108.) The case differs starkly from this one. The party seeking disclosure there already knew the content of ***1449** the stored message, which an unidentified subscriber had broadcast to the world. The only information sought was the offending subscriber's identity. Here the situation is reversed. Apple already knows the identity of the *subscriber* whose messages are at issue. What it seeks to discover are the *contents* of *private messages* stored on Nfox/Kraft's facilities. Its main target may well be the ****91** *identities of correspondents* who discussed a particular subject, but that information cannot be disclosed without disclosing contents in violation of the Act.

Genentech again overlooks this crucial distinction when it alludes to "an entire class of so-called 'John Doe' lawsuits in which civil litigants have successfully subpoenaed ISPs to obtain the identities of subscribers who posted anonymous defamatory messages on the Internet," stating "[t]hese lawsuits simply could not occur if the Act barred the type of discovery sought here." We need not consider the weight to be given this *argumentum ad consequentiam* because its conclusion is a non sequitur. The subpoenas before us do *not* concern a "subscriber" who "posted anonymously" on the internet, but the stored private communications of known persons who openly posted news reports based on information from confidential sources.

Indeed, Genentech's assertions on this point, as well as Apple's pleadings and argument, betray a crucial confusion of terminology. In the world of digital communications, to "post" is "[t]o *send* (a message or data) to a mailing list, newsgroup, or other *online forum* on which it *will be* displayed; to *display or make available* online." [14] Posting thus consists of directly placing material on or in a Web site, bulletin board, discussion group, newsgroup, or similar internet site or "forum," where it will appear automatically and more or less immediately to be seen by anyone with access to that forum. In short, to "post" is to *directly publish content.* If the host system is accessible to the public, the act of "posting" constitutes publication to the world. [15]

***1450** To merely supply information to someone else, who may use it or not as he chooses, is not to "post." Thus if I give someone information about an unannounced new product, and he places that information on a Web site for the public to