CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

§2510. Definitions

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;

* * *

(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;

(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;

* * *

(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;

* * *

(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 . . . ; 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 [specific frequencies];

(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;

* * *

(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.
§2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
   (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
   (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
   (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
   (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
   (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

* * *

(2)

* * *

4
(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

* * *

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—
   (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

   (ii) [to intercept a public safety-related radio communication];

   (iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

   (v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—
   (i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or
   (ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

* * *

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or
an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—
   (i) as otherwise authorized in . . . this title;
   (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
   (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
   (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

* * *
§2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

[I just want you to be aware that there are trafficking-like prohibitions on interception devices.]
§2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.
§2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

* * *

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

* * *
§2520. Recovery of civil damages authorized

(a) In General.—Except [for compliance with compelled government disclosure], any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter 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 an 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 punitive damages in appropriate cases; and

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

(c) Computation of Damages.— * * *

(2) [T]he court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.—A good faith reliance on [legal process or an emergency investigative request, or] a good faith determination that section 2511(3) or [the anti-hacking provisions] 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.

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

(e) Limitation.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

* * *
CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

§2701. Unlawful access to stored communications

(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—

[Omitted. The punishment varies by intent and prior violation.]

(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 [compelled stored communication disclosure to the government], 2704 [compelled backup in association with compelled stored communication disclosure to the government] or 2518 [compelled communication interception by the government] of this title.
§2702. Voluntary disclosure of customer communications or records

(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 . . . 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 . . . ;
(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
(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 [to the government];
   (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 . . . ; 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); and
   (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.
§2707. Civil action

(a) Cause of Action.—Except [when complying with valid government legal process], 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.

* * *

(e) Defense.—A good faith reliance on [legal process or an emergency investigative request, or] 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.

* * *
§2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system;

* * *

(4) the term “governmental entity” means a department or agency of the United States or any State or political subdivision thereof.
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 secret. We hold that this was error 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). 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.

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. 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.”

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 product was a breakout box for audio recording, compatible with Apple’s GarageBand mixing software. Sidenote: Asteroid was never actually released.]

***

[Apple alleged that the material was drawn from a confidential internal presentation, and sent a cease and desist letter to O’Grady.]

***

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.’” 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 . . . 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. [It did not address their SCA
arguments.]

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. After receiving preliminary opposition and numerous amicus curiae briefs on behalf of both sides, we issued an order to show cause.

DISCUSSION

* * *

*I440 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.° (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. * * *
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. 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.

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.

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
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. However, there appears **86 to be no judicial authority squarely addressing the issue.

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.]”

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. **88
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.)

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. **88

**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 **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.

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**

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.

***
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 **91identities 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.

***

*1451* We conclude that the outstanding subpoenas to Nfox and Kraft cannot be enforced without compelling them to violate the SCA. Since this would offend the principle of federal supremacy, the subpoenas are unenforceable, and should be quashed.

***

*1480 DISPOSITION*
Let a writ of mandate issue directing the court below to set aside its order denying petitioners’ motion for a protective order and to enter a new order granting that motion. Costs to petitioners.
KOZINSKI, Circuit Judge:

We consider whether defendants violated federal electronic privacy and computer fraud statutes when they used a “patently unlawful” subpoena to gain access to e-mail stored by plaintiffs’ Internet service provider.

**Background**

Plaintiffs Wolf and Buckingham, officers of Integrated Capital Associates, Inc. (ICA), are embroiled in commercial litigation in New York against defendant Farey–Jones. In the course of discovery, Farey–Jones sought access to ICA’s e-mail. He told his lawyer Iryna Kwasny to subpoena ICA’s ISP, NetGate.

Under the Federal Rules, Kwasny was supposed to “take reasonable steps to avoid imposing undue burden or expense” on NetGate. Fed.R.Civ.P. 45(c)(1). One might have thought, then, that the subpoena would request only e-mail related to the subject matter of the litigation, or maybe messages sent during some relevant time period, or at the very least those sent to or from employees in some way connected to the litigation. But Kwasny ordered production of “[a]ll copies of e-mails sent or received by anyone” at ICA, with no limitation as to time or scope.

NetGate, which apparently was not represented by counsel, explained that the amount of
e-mail covered by the subpoena was substantial. But defendants did not relent. NetGate
ten took what might be described as the “Baskin–Robbins” approach to subpoena
compliance and offered defendants a “free sample” consisting of 339 messages. It posted
copies of the messages to a NetGate website where, without notifying opposing counsel,
Kwasny and Farey–Jones read them. Most were unrelated to the litigation, and many
were privileged or personal.

When Wolf and Buckingham found out what had happened, they asked the court to quash
the subpoena and award sanctions. Magistrate Judge Wayne Brazil soundly roasted
Farey–Jones and Kwasny for their conduct, finding that “the subpoena, *1072 on its face,
was massively overbroad” and “patently unlawful,” that it “transparently and
egregiously” violated the Federal Rules, and that defendants “acted in bad faith” and
showed “at least gross negligence in the crafting of the subpoena.” He granted the motion
to quash and socked defendants with over $9000 in sanctions to cover Wolf and
Buckingham’s legal fees. Defendants did not appeal that award.

Wolf, Buckingham and other ICA employees whose e-mail was included in the sample
also filed this civil suit against Farey–Jones and Kwasny. They claim defendants violated
2511 et seq., and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, as well as
various state laws. The district court held that none of the federal statutes applied, and
dismissed the claims without leave to amend. It declined jurisdiction over the state law

**Analysis**

1. The Stored Communications Act provides a cause of action against anyone who
“intentionally accesses without authorization a facility through which an electronic
communication service is provided ... and thereby obtains, alters, or prevents authorized
access to a wire or electronic communication while it is in electronic storage.” 18 U.S.C.
§§ 2701(a)(1), 2707(a). “[E]lectronic storage” means either “temporary, intermediate
storage ... incidental to ... electronic transmission,” or “storage ... for purposes of backup
protection.” *Id.* § 2510(17). The Act exempts, inter alia, conduct “authorized ... by the
person or entity providing a wire or electronic communications service,” *id.* § 2701(c)(1),
or “by a user of that service with respect to a communication of or intended for that user,”
*id.* § 2701(c)(2).

The district court dismissed on the ground that NetGate had authorized defendants’
access. It held that this consent was not coerced, because the subpoena itself informed
NetGate of its right to object. Plaintiffs contend that NetGate’s authorization was
nonetheless invalid because the subpoena was patently unlawful. Their claim turns on the
meaning of the word “authorized” in section 2701. We have previously reserved
judgment on this question, *see Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 n. 8
(9th Cir.2002), while other circuits have considered related issues, see, e.g., EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n. 10 (1st Cir.2001) (holding access might be “unauthorized” under the Computer Fraud and Abuse Act if it is “not in line with the reasonable expectations” of the party granting permission (internal quotation marks omitted)); United States v. Morris, 928 F.2d 504, 510 (2d Cir.1991) (holding access unauthorized where it is not “in any way related to[the system’s] intended function”).

We interpret federal statutes in light of the common law. See Beck v. Prupis, 529 U.S. 494, 500–01, 120 S.Ct. 1608, 146 L.Ed.2d 561 (2000). Especially relevant here is the common law of trespass. Like the tort of trespass, the Stored Communications Act protects individuals’ privacy and proprietary interests. The Act reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, cf. Prosser and Keeton on the Law of Torts § 13, at 78 (W. Page Keeton ed., 5th ed.1984), the Act protects users whose electronic communications *1073 are in electronic storage with an ISP or other electronic communications facility.

A defendant is not liable for trespass if the plaintiff authorized his entry. See Prosser & Keeton § 13, at 70. But “an overt manifestation of assent or willingness would not be effective ... if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended.” Id. § 18, at 119; cf. Restatement (Second) of Torts §§ 173, 892B(2). Thus, the busybody who gets permission to come inside by posing as a meter reader is a trespasser. J.H. Desnick, M.D., Eye Servs., Ltd. v. ABC, 44 F.3d 1345, 1352 (7th Cir.1995). So too is the police officer who, invited into a home, conceals a recording device for the media. Cf. Berger v. Hanlon, 129 F.3d 505, 516–17 (9th Cir.1997), vacated, 526 U.S. 808, 119 S.Ct. 1706, 143 L.Ed.2d 978 (1999), reinstated in relevant part, 188 F.3d 1155, 1157 (9th Cir.1999).

Not all deceit vitiates consent. “[T]he mistake must extend to the essential character of the act itself, which is to say that which makes it harmful or offensive, rather than to some collateral matter which merely operates as an inducement.” Prosser & Keeton § 18, at 120 (footnote omitted). In other words, it must be a “substantial mistake[ ] ... concerning the nature of the invasion or the extent of the harm.” Restatement (Second) of Torts § 892B(2) cmt. g. Unlike the phony meter reader, the restaurant critic who poses as an ordinary customer is not liable for trespass, Desnick, 44 F.3d at 1351; nor, unlike the wired cop, is the invitee who conceals only an intent to repeat what he hears, cf. Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir.1971) (invasion of privacy claim). These results hold even if admission would have been refused had all the facts been known.
These are fine and sometimes incoherent distinctions. See Med. Lab. Mgmt. Consultants v. ABC, 30 F.Supp.2d 1182, 1201–04 (D.Ariz.1998), aff’d, 306 F.3d 806 (9th Cir.2002). But the theory is that some invited mistakes go to the essential nature of the invasion while others are merely collateral. Classification depends on the extent to which the intrusion trenches on “the specific interests that the tort of trespass seeks to protect.” Desnick, 44 F.3d at 1352; see also Lewis v. United States, 385 U.S. 206, 211, 87 S.Ct. 424, 17 L.Ed.2d 312 (1966); Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505, 517–18 (4th Cir.1999).

We construe section 2701 in light of these doctrines. Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances. Section 2701(c)(1) therefore provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access.

Under this standard, plaintiffs have alleged facts that vitiate NetGate’s consent. NetGate disclosed the sample in response to defendants’ purported subpoena. Unbeknownst to NetGate, that subpoena was invalid. This mistake went to the essential nature of the invasion of privacy. The subpoena’s falsity transformed the access from a bona fide state-sanctioned inspection into private snooping. See Restatement (Second) of Torts § 174 (addressing “consent induced by fraud or mistake as to the validity of purported legal authority”); cf. Bumper v. North Carolina, 391 U.S. 543, 549, 88 S.Ct. 1788, 20 L.Ed.2d 797 (1968) (“A search conducted in reliance upon a warrant cannot later be justified on the basis of consent if it *1074 turns out that the warrant was invalid.”). The false subpoena caused disclosure of documents that otherwise would have remained private; it effected an “invasion ... of the specific interests that the [statute] seeks to protect.” Desnick, 44 F.3d at 1352.

Defendants had at least constructive knowledge of the subpoena’s invalidity. It was not merely technically deficient, nor a borderline case over which reasonable legal minds might disagree. It “transparently and egregiously” violated the Federal Rules, and defendants acted in bad faith and with gross negligence in drafting and deploying it. They are charged with knowledge of its invalidity. See Prosser & Keeton § 18, at 119 (consent likely vitiated where defendants “ought to have known in the exercise of reasonable care” of the mistake).

That NetGate could have objected is immaterial. The subpoena may not have been coercive, but it was deceptive, and that is an independent ground for invalidating consent. See Restatement (Second) of Torts § 892B(2)-(3). It was a piece of paper masquerading as legal process. NetGate produced the sample in response and doubtless would not have done so had it known the subpoena was void—particularly in light of its own legal obligation not to disclose such messages to third parties, see 18 U.S.C. § 2702(a)(1). That NetGate could have objected proves disclosure was not an inevitable consequence, but it
was still a foreseeable one (and the intended one).

Allowing consent procured by known mistake to serve as a defense would seriously impair the statute’s operation. A hacker could use someone else’s password to break into a mail server and then claim the server “authorized” his access. Congress surely did not intend to exempt such intrusions—indeed, they seem the paradigm of what it sought to prohibit. Cf. Morris, 928 F.2d at 510 (access gained by guessing someone else’s password is not “authorization” under the Computer Fraud and Abuse Act).

The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure it is not abused. Informing the person served of his right to object is a good start, see Fed.R.Civ.P. 45(a)(1)(D), but it is no substitute for the exercise of independent judgment about the subpoena’s reasonableness. Fighting a subpoena in court is not cheap, and many *1075 may be cowed into compliance with even overbroad subpoenas, especially if they are not represented by counsel or have no personal interest at stake. Because defendants procured consent by exploiting a mistake of which they had constructive knowledge, the district court erred by dismissing based on that consent.

Defendants ask us to affirm on the alternative ground that the messages they accessed were not in “electronic storage” and therefore fell outside the Stored Communications Act’s coverage. See 18 U.S.C. § 2701(a)(1). The Act defines “electronic storage” as “(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.” Id. § 2510(17), incorporated by id. § 2711(1). Several courts have held that subsection (A) covers e-mail messages stored on an ISP’s server pending delivery to the recipient. See In re DoubleClick, Inc. Privacy Litig., 154 F.Supp.2d 497, 511–12 (S.D.N.Y.2001); Fraser v. Nationwide Mut. Ins. Co., 135 F.Supp.2d 623, 635–36 (E.D.Pa.2001); cf. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir.1994) (messages stored on a BBS pending delivery). Because subsection (A) applies only to messages in “temporary, intermediate storage,” however, these courts have limited that subsection’s coverage to messages not yet delivered to their intended recipient. See DoubleClick, 154 F.Supp.2d at 512; Fraser, 135 F.Supp.2d at 636.

Defendants point to these cases and argue that messages remaining on an ISP’s server after delivery no longer fall within the Act’s coverage. But, even if such messages are not within the purview of subsection (A), they do fit comfortably within subsection (B). There is no dispute that messages remaining on NetGate’s server after delivery are stored “by an electronic communication service” within the meaning of 18 U.S.C. § 2510(17)(B). Cf. DoubleClick, 154 F.Supp.2d at 511 (holding that subsection (B) did not apply because the communications at issue were not being stored by an electronic communication service). The only issue, then, is whether the messages are stored “for
purposes of backup protection.” 18 U.S.C. § 2510(17)(B). We think that, within the ordinary meaning of those terms, they are.

An obvious purpose for storing a message on an ISP’s server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user’s own computer. The ISP copy of the message functions as a “backup” for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition. 3

One district court reached a contrary conclusion, holding that “backup protection” includes only temporary backup storage pending delivery, and not any form of “post-transmission storage.” See Fraser, 135 F.Supp.2d at 633–34, 636. We reject this view as contrary to the plain language of the Act. In contrast to subsection (A), subsection (B) does not distinguish between intermediate and post-transmission storage. Indeed, Fraser’s interpretation renders subsection (B) essentially superfluous, *1076 since temporary backup storage pending transmission would already seem to qualify as “temporary, intermediate storage” within the meaning of subsection (A). By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission.

The United States, as amicus curiae, disputes our interpretation. It first argues that, because subsection (B) refers to “any storage of such communication,” it applies only to backup copies of messages that are themselves in temporary, intermediate storage under subsection (A). The text of the statute, however, does not support this reading. Subsection (A) identifies a type of communication (“a wire or electronic communication”) and a type of storage (“temporary, intermediate storage ... incidental to the electronic transmission thereof”). The phrase “such communication” in subsection (B) does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A). The government’s argument would be correct if subsection (B) referred to “a communication in such storage,” or if subsection (A) referred to a communication in temporary, intermediate storage rather than temporary, intermediate storage of a communication. However, as the statute is written, “such communication” is nothing more than shorthand for “a wire or electronic communication.”

The government’s contrary interpretation suffers from the same flaw as Fraser’s: It drains subsection (B) of independent content because virtually any backup of a subsection (A) message will itself qualify as a message in temporary, intermediate storage. The government counters that the statute requires only that the underlying message be temporary, not the backup. But the lifespan of a backup is necessarily tied to that of the underlying message. Where the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as “backing up”
those messages.

The United States also argues that we upset the structure of the Act by defining “electronic storage” so broadly as to be superfluous and by rendering irrelevant certain other provisions dealing with remote computing services. The first claim relies on the argument that any copy of a message necessarily serves as a backup to the user, the service or both. But the mere fact that a copy could serve as a backup does not mean it is stored for that purpose. We see many instances where an ISP could hold messages not in electronic storage—for example, e-mail sent to or from the ISP’s staff, or messages a user has flagged for deletion from the server. In both cases, the messages are not in temporary, intermediate storage, nor are they kept for any backup purpose.

Our interpretation also does not render irrelevant the more liberal access standards governing messages stored by remote computing services. See 18 U.S.C. §§ 2702(a)(2), 2703(b). The government’s premise is that a message stored by a remote computing service “solely for the purpose of providing storage or computer processing services to [the] subscriber,” id. §§ 2702(a)(2)(B), 2703(b)(2)(B), would also necessarily be stored for purposes of backup protection under section 2510(17)(B), and thus would be subject to the more stringent rules governing electronic storage. But not all remote computing services are also electronic communications services and, as to those that are not, section 2510(17)(B) is by its own terms inapplicable. The government notes that remote computing services and electronic communications services are “often the same entities,” but “often” is not good enough to make the government’s point. Even as to remote computing services that are also electronic communications services, not all storage covered by sections 2702(a)(2)(B) and 2703(b)(2)(B) is also covered by section 2510(17)(B). A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes.

Finally, the government invokes legislative history. It cites a passage from a 1986 report indicating that a committee intended that messages stored by a remote computing service would “continue to be covered by section 2702(a)(2)” if left on the server after user access. H.R.Rep. No. 647, 99th Cong., at 65 (1986). The cited discussion addresses provisions relating to remote computing services. We do not read it to address whether the electronic storage provisions also apply. See id. at 64–65. The committee’s statement that section 2702(a)(2) would “continue” to cover e-mail upon access supports our reading. If section 2702(a)(2) applies to e-mail even before access, the committee could not have been identifying an exclusive source of protection, since even the government concedes that unopened e-mail is protected by the electronic storage provisions.

The government also points to a subsequent, rejected amendment that would have made explicit the electronic storage definition’s coverage of opened e-mail. See H.R.Rep. No. 932, 106th Cong., at 7 (2000). This sort of legislative history has very little probative value; Congress might have rejected the amendment precisely because it thought the
definition already applied.

Finally, the government points to a passing reference in another recent report. H.R.Rep. No. 236(I), 107th Cong., at 57 (2001). The discussion addresses an unrelated issue and merely assumes that the definition only applies to unopened e-mail. This assumption was natural given that Fraser had recently been decided.

We acknowledge that our interpretation of the Act differs from the government’s and do not lightly conclude that the government’s reading is erroneous. Nonetheless, for the reasons above, we think that prior access is irrelevant to whether the messages at issue were in electronic storage. Because plaintiff’s e-mail messages were in electronic storage regardless of whether they had been previously delivered, the district court’s decision cannot be affirmed on this alternative ground.

2. Plaintiffs also claim a violation of the Wiretap Act, which authorizes suit against those who “intentionally intercept[ ... ] any wire, oral, or electronic communication.” 18 U.S.C. §§ 2511(1)(a), 2520(a). We recently held in Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), that the Act applies only to “acquisition contemporaneous with transmission.” Id. at 878. Specifically, “Congress did not intend for “intercept” to apply to “electronic communications” when those communications are in “electronic storage.” ‘ ” Id. at 877 (quoting Steve Jackson Games, 36 F.3d at 462). Konop is dispositive, *1078 and the district court correctly dismissed the claim.

3. Plaintiffs finally claim a violation of the Computer Fraud and Abuse Act, which provides a cause of action against one who, inter alia, “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer if the conduct involved an interstate or foreign communication.” 18 U.S.C. § 1030(a)(2)(C), (g). The conduct must involve one of five factors listed in 18 U.S.C. § 1030(a)(5)(B), which include a loss in excess of $5000. Id. § 1030(a)(5)(B)(i), (g).5

The district court dismissed without leave to amend on the theory that the Act does not apply to unauthorized access of a third party’s computer. It also dismissed for failure to allege damages or loss, though it noted that this omission might be cured by amendment. Plaintiffs do not dispute the latter defect, but urge us to reverse as to the former ground so they can amend.

The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to “[a]ny person who suffers damage or loss by reason of a violation of this section.” 18 U.S.C. § 1030(g) (emphasis added). “[T]he word “any” has an expansive meaning, that is, “one or some indiscriminately of whatever kind.” ’ ” HUD v. Rucker, 535 U.S. 125, 131, 122 S.Ct. 1230, 152 L.Ed.2d 258 (2002) (quoting United States v. Gonzales, 520 U.S. 1, 5, 117 S.Ct. 1032, 137 L.Ed.2d 132 (1997)). Nothing in
the provision’s language supports the district court’s restriction. Individuals other than the computer’s owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.

***

5. Having dismissed all the federal claims, the district court declined jurisdiction over the pendent state law claims under 28 U.S.C. § 1367(c)(3). Because we reverse dismissal of some of the federal claims, we also reinstate the state claims.

We REVERSE dismissal of the Stored Communications Act claim, AFFIRM dismissal of the Wiretap Act claim, and REVERSE dismissal with prejudice of the Computer Fraud and Abuse Act claim with instructions to dismiss with leave to amend. We also REVERSE dismissal of the state claims.

AFFIRMED in part, REVERSED in part and remanded. Costs to appellants.
In this consolidated multi-district litigation, Plaintiffs . . . individually and on behalf of those similarly situated (collectively, “Plaintiffs”), allege that Defendant Google, Inc., has violated state and federal antiwiretapping laws in its operation of Gmail, an email service. See ECF No. 38–2. Before the Court is Google’s Motion to Dismiss Plaintiffs’ Consolidated Complaint. See ECF No. 44. For the reasons stated below, the Court DENIES in part and GRANTS in part Google’s Motion to Dismiss with leave to amend.

I. BACKGROUND

A. Factual Allegations

Plaintiffs challenge Google’s operation of Gmail under state and federal anti-wiretapping laws. The Consolidated Complaint seeks damages on behalf of a number of classes of Gmail users and non–Gmail users for Google’s interception of emails over a period of several years. All the class periods span from two years prior to the filling of the actions to the date of class certification, if any. Because the first of these consolidated actions was filed in 2010, the Consolidated Complaint taken as a whole challenges the operations of Gmail from 2008 to the present.

1. Google’s Processing of Emails

Google’s processing of emails to and from its users has evolved over the putative class periods. Plaintiffs allege, however, that in all iterations of Google’s email routing processes since 2008, Google has intercepted, read and acquired the content of emails that were sent or received by Gmail user while the emails were in transit. Plaintiffs allege that before [redacted] 20 [redacted], a Gmail device intercepted, read, and acquired the content of each email for the purposes of sending an advertisement relevant to that email communication to the recipient, sender, or both. ECF No. 38–2 ¶¶ 26–27, 33. According to the Consolidated Complaint, this interception and reading of the email was separate from Google’s other processes, including spam and virus filtering. Id. ¶ 5.

After [redacted] 20[redacted], Plaintiffs allege that Google continued to intercept, read,
and acquire content from emails that were in transit even as Google changed the way it transmit emails. Plaintiffs allege that after [redacted] 20[redacted], Google continued to intercept, read, and acquire content from emails to provide targeted advertising. *Id.* ¶¶ 62–63. Moreover, Plaintiffs allege that post-[redacted] 20[redacted], targeted advertising was not the sole purpose of the interception. Rather, during this time period, Plaintiffs allege that a number of Google device intercepted the emails, read and collected content as well as affiliated data, and [redacted] these emails and data. *Id.* ¶¶ 47–56. Plaintiffs further allege that Google used these [redacted] data to create user profiles and models. *Id.* ¶¶ 74–79. Google then allegedly used the emails, affiliated data, and user profiles to serve their profit interests that were unrelated to providing email services to particular users. *Id.* ¶¶ 97–98. Accordingly, Plaintiffs allege that Google has, since 20 [redacted], intercepted emails for the dual purposes of providing advertisements and creating user profiles to advance Google’s profit interests.

2. Types of Gmail Services

*2* Gmail implicates several different, but related, systems of email delivery, three of which are at issue here. The first is a free service, which allows any user to register for an account with Google to use Gmail. *Id.* ¶ 99. This system is supported by advertisements, though users can opt-out of such advertising or access Gmail accounts in ways that do not generate advertising, such as accessing email on a smartphone. *Id.* ¶ 70.

The second is Google’s operation of email on behalf of Internet Service Providers ("ISPs"). *Id.* ¶ 100. Google, through its Google Apps Partner program, enters into contracts with ISPs, such as Cable One, to provide an email service branded by the ISP. *Id.* The ISP’s customers can register for email addresses from their ISP (such as “@mycableone.com”), but their email is nevertheless powered by Google through Gmail.

Third, Google operates Google Apps for Education, through which Google provides email on behalf of educational organizations for students, faculty, staff, and alumni. *Id.* ¶ 101. These users receive “@name.institution.edu” email addresses, but their accounts are also powered by Google using Gmail. *Id.* Universities that are part of Google Apps for Education require their students to use the Gmail–provided service. *Id.*

Google Apps users, whether through the educational program or the partner program, do not receive content-based ads but can opt in to receiving such advertising. Google processes emails sent and received from all Gmail users, including Google Apps users, in the same way except that emails of users who do not receive advertisements are not processed through Google’s advertising infrastructure, which attaches targeted advertisements to emails. *Id.* ¶¶ 57, 72–73. This means that users who do not receive advertisements would not have been subject to the pre-[redacted] 20[redacted] interceptions, as during that period, interceptions were for the sole purpose of attaching
targeted advertisements to emails. After [redacted] 20[redacted], Google separated its interception of emails for targeted advertising from its interception of emails for creating user profiles. *Id.* ¶ 72. As a result, After [redacted] 20[redacted], emails to and from users who did not receive advertisements are nevertheless intercepted to create user profiles. *Id.* ¶¶ 73, 85. Accordingly, these post-[redacted]20[redacted]interceptions impacted all Gmail and Google Apps users, regardless of whether they received advertisements.

3. Google’s Agreements with Users
The operation of the Gmail service implicates several legal agreements. Gmail users were required to agree to one of two sets of Terms of Service during the class periods. The first Terms of Service was in effect from April 16, 2007, to March 1, 2012, and the second has been in effect since March 1, 2012. *Id.* ¶ 102. The 2007 Terms of Service stated that:

> Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings.... In addition, there are commercially available services and software to limit access to material that you may find objectionable.

*3 Id.* ¶ 104. A subsequent section of the 2007 Terms of Service provided that “[s]ome of the Services are supported by advertising revenue and may display advertisements and promotions” and that “[t]hese advertisements may be content-based to the content information stored on the Services, queries made through the Service or other information.” *Id.* ¶¶ 107–08.

The 2012 Terms of Service deleted the above language and stated that users “give Google (and those [Google] work[s] with) a worldwide license to use ..., create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), ... and distribute such content.” See ECF No. 46–6 at 3.

Both Terms of Service reference Google’s Privacy Policies, which have been amended three times thus far during the putative class periods. See ECF Nos. 46–7, 46–8, 46–9, 46–10. These Policies, which were largely similar, stated that Google could collect information that users provided to Google, cookies, log information, user communications to Google, information that users provide to affiliated sites, and the links that a user follows. See ECF No. 46–7. The Policies listed Google’s provision of “services to users, including the display of customized content and advertising” as one of the reasons for the collection of this information. *Id.*

Google also had in place Legal Notices, which stated that “Google does not claim any ownership in any of the content, including any text, data, information, images,
photographs, music, sound, video, or other material, that [users] upload, transmit or store in [their] Gmail account.” ECF No. 38–2 ¶ 118. The Notices further stated that Google “will not use any of [users’] content for any purpose except to provide [users] with the service.” Id. ¶ 121.

In addition, Google entered into contractual agreements with ISPs and educational institutions as part of its Google Apps Partner and Google Apps for Education programs. These agreements require Google to “protect against unauthorized access to or use of Customer data.” Id. ¶¶ 137, 161. In turn, “Customer data” is defined as “data, including email, provided, generated, transmitted, or displayed via the Services by Customers or End Users.” Id. ¶¶ 138, 162. Further, the Terms of Service applicable to Google Apps Cable One users states that “Google may access, preserve, and disclose your account information and any Content associated with that account if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary” to satisfy applicable law, enforce the Terms of Service, detect or prevent fraud, or protect against imminent harm to the rights of Google, its users, or the public. ECF No. 46–2 at 2–3.

Importantly, Plaintiffs who are not Gmail or Google Apps users are not subject to any of Google’s express agreements. Because non-Gmail users exchange emails with Gmail users, however, their communications are nevertheless subject to the alleged interceptions at issue in this case.

***

IV. MOTION TO DISMISS

The Wiretap Act, as amended by the ECPA, generally prohibits the interception of “wire, oral, or electronic communications.” 18 U.S.C. § 2511(1); see also Joffe v. Google, Inc., No. 11–17483, 2013 WL 4793247, at *3 (9th Cir. Sept. 10, 2013). More specifically, the Wiretap Act provides a private right of action against any person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a); see id. § 2520 (providing a private right of action for violations of § 2511). The Act further defines “intercept” as “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.” Id. § 2510(4).

Plaintiffs contend that Google violated the Wiretap Act in its operation of the Gmail system by intentionally intercepting the content of emails that were in transit to create profiles of Gmail users and to provide targeted advertising. Google contends that Plaintiffs have not stated a claim with respect to the Wiretap Act for two reasons. First, Google contends that there was no interception because there was no “device.” Specifically, Google argues that its reading of any emails would fall within the “ordinary course of business” exception to the definition of device. ECF No. 44 at 6–13. Under that
exception, “any telephone or telegraph instrument, equipment or facility, or any component thereof ... being used by a provider of wire or electronic communication service in the ordinary course of its business” is not a “device,” and the use of such an instrument accordingly falls outside of the definition of “intercept.” 18 U.S.C. § 2510(5)(a)(ii). Second, Google contends that all Plaintiffs have consented to any interception. ECF No. 44 at 13–20. Under the statute, it is not unlawful “to intercept a wire, oral, or electronic communication ... where one of the parties to the communication has given prior consent to such interception.” 18 U.S.C. § 2511(2)(d).

1. “Ordinary Course of Business” Exception

*8 Google first contends that it did not engage in an interception because its reading of users’ emails occurred in the ordinary course of its business. ECF No. 44 at 6–13. Conversely, Plaintiffs contend that the ordinary course of business exception is narrow and applies only when an electronic communication service provider’s actions are “necessary for the routing, termination, or management of the message.” See ECF No. 53 at 7. The Court finds that the ordinary course of business exception is narrow. The exception offers protection from liability only where an electronic communication service provider’s interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication. Specifically, the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email. Plaintiffs have alleged, however, that Google’s interception is not an instrumental component of Google’s operation of a functioning email system. ECF No. 38–2 ¶ 97. In fact, Google’s alleged interception of email content is primarily used to create user profiles and to provide targeted advertising—neither of which is related to the transmission of emails. See id. ¶¶ 26–27, 33, 57, 65, 84, 95. The Court further finds that Plaintiffs’ allegations that Google violated Google’s own agreements and internal policies with regard to privacy also preclude application of the ordinary course of business exception.

[The court construes the exception narrowly, relying on statutory text, judicial interpretation, the statutory scheme, and legislative history. I haven’t given you this portion because it’s lengthy, questionably reasoned, and not particularly generalizable.]

Furthermore, the D.C. Circuit has held in a section 2510(5)(a)(i) case that a defendant’s actions may fall outside the “ordinary course of business” exception when the defendant violates its own internal policies. * * *

*12 The Court finds that the reasoning of the D.C. Circuit applies equally in the section 2510(5)(a)(ii) context. Here, Plaintiffs allege that Google has violated its own policies and therefore is acting outside the ordinary course of business. Specifically, Plaintiffs allege that Google’s Privacy Policies explicitly limit the information that Google may collect to an enumerated list of items, and that this list does not include content of emails.
ECF No. 38–2 ¶¶ 187–91. Plaintiffs point to the language of the Privacy Policy that states that Google “may collect the following types of information” and then lists (1) information provided by the user (such as personal information submitted on the sign-up page), (2) information derived from cookies, (3) log information, (4) user communications to Google, (5) personal information provided by affiliated Google services and sites, (6) information from third party applications, (7) location data, and (8) unique application numbers from Google’s toolbar. Id. ¶ 187; ECF No. 46–7. Plaintiffs further note that the updated Privacy Policy also stated that Google “collected information in two ways”: “(1) information the user gives to Google—the user’s personal information; and, (2) information Google obtains from the user’s use of Google services, wherein Google lists: (a) the user’s device information; (b) the user’s log information; (c) the user’s location information; (d) the user’s unique application number; (e) information stored locally on the user’s device; and, (e) [sic] information derived from cookies placed on a user’s device.” ECF No. 38–2 ¶ 189; ECF No. 46–10. Because content of emails between users or between users and non-users was not part of either list, Plaintiffs allege that Google “violates the express limitations of its Privacy Policies.” Id. ¶¶ 191, 195. The Court need not determine at this stage whether Plaintiffs will ultimately be able to prove that the Privacy Policies were intended to comprehensively list the information Google may collect. Rather, Plaintiffs’ plausible allegations that the Privacy Policies were exhaustive are sufficient. Because Plaintiffs have alleged that Google exceeded the scope of its own Privacy Policy, the section 2510(5)(a)(ii) exception cannot apply.

Accordingly, the Court DENIES Google’s Motion to Dismiss based on the section 2510(5)(a)(ii) exception.

2. Consent

Google’s second contention with respect to Plaintiffs’ Wiretap Act claim is that all Plaintiffs consented to any interception of emails in question in the instant case. Specifically, Google contends that by agreeing to its Terms of Service and Privacy Policies, all Gmail users have consented to Google reading their emails. ECF No. 44 at 14–16. Google further suggests that even though non-Gmail users have not agreed to Google’s Terms of Service or Privacy Policies, all non-Gmail users impliedly consent to Google’s interception when non-Gmail users send an email to or receive an email from a Gmail user. Id. at 19–21.

If either party to a communication consents to its interception, then there is no violation of the Wiretap Act. 18 U.S.C. § 2511(2)(d). Consent to an interception can be explicit or implied, but any consent must be actual. See United States v. Van Poyck, 77 F.3d 285, 292 (9th Cir.1996); U.S. v. Amen, 831 F.2d 373, 378 (2d Cir.1987); U.S. v. Corona-Chavez. 328 F.3d 974, 978 (8th Cir.2003). Courts have cautioned that implied consent applies only in a narrow set of cases. See Watkins, 704 F.2d at 581 (holding that consent should not be “cavalierly implied”); In re Pharmatrack, 329 F.3d at 20. The critical
question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception. *Berry*, 146 F.3d at 1011. That the person communicating knows that the interceptor has the capacity to monitor the communication is insufficient to establish implied consent. *Id.* Moreover, consent is not an all-or-nothing proposition. Rather, “[a] party may consent to the interception of only part of a communication or to the interception of only a subset of its communications.” *In re Pharmatrack, Inc.*, 329 F.3d at 19.

*13* In its Motion to Dismiss, Google marshals both explicit and implied theories of consent. Google contends that by agreeing to Google’s Terms of Service and Privacy Policies, Plaintiffs who are Gmail users expressly consented to the interception of their emails. ECF No. 44 at 14–16. Google further contends that because of the way that email operates, even non-Gmail users knew that their emails would be intercepted, and accordingly that non-Gmail users impliedly consented to the interception. *Id.* at 19–20. Therefore, Google argues that in all communications, both parties—regardless of whether they are Gmail users—have consented to the reading of emails. *Id.* at 13–14. The Court rejects Google’s contentions with respect to both explicit and implied consent. Rather, the Court finds that it cannot conclude that any party—Gmail users or non-Gmail users—has consented to Google’s reading of email for the purposes of creating user profiles or providing targeted advertising.

Google points to its Terms of Service and Privacy Policies, to which all Gmail and Google Apps users agreed, to contend that these users explicitly consented to the interceptions at issue. The Court finds, however, that those policies did not explicitly notify Plaintiffs that Google would intercept users’ emails for the purposes of creating user profiles or providing targeted advertising.

Section 8 of the Terms of Service that were in effect from April 16, 2007, to March 1, 2012, stated that “Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service.” ECF No. 46–5 at 4. This sentence was followed by a description of steps users could take to avoid sexual and objectionable material. *Id.* (“For some of the Services, Google may provide tools to filter out explicit sexual content.”). Later, section 17 of the Terms of Service stated that “advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.” *Id.* at 8.

The Court finds that Gmail users’ acceptance of these statements does not establish explicit consent. Section 8 of the Terms of Service suggests that content may be intercepted under a different set of circumstances for a different purpose—to exclude objectionable content, such as sexual material. This does not suggest to the user that Google would intercept emails for the purposes of creating user profiles or providing targeted advertising. *Watkins*, 704 F.2d at 582 (“[C]onsent within the meaning of section 2511(2)(d) is not necessarily an all or nothing proposition; it can be limited. It is the task
of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent.”); In re Pharmatrack, Inc., 329 F.3d at 19 (“Thus, a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.”) (internal quotation marks omitted). Therefore, to the extent that section 8 of the Terms of Service establishes consent, it does so only for the purpose of interceptions to eliminate objectionable content. The Consolidated Complaint suggests, however, that Gmail’s interceptions for the purposes of targeted advertising and creation of user profiles was separate from screening for any objectionable content. See ECF No. 38–2 ¶¶ 5, 200. Because the two processes were allegedly separate, consent to one does not equate to consent to the other.

Section 17 of the Terms of Service—which states that Google’s “advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information”—is defective in demonstrating consent for a different reason: it demonstrates only that Google has the capacity to intercept communications, not that it will. Berry, 146 F.3d at 1011 (holding that knowledge of defendant’s capacity to monitor is insufficient to establish consent). Moreover, the language suggests only that Google’s advertisements were based on information “stored on the Services” or “queries made through the Services”—not information in transit via email. Plaintiffs here allege that Google violates the Wiretap Act, which explicitly protects communications in transit, as distinguished from communications that are stored. Furthermore, providing targeted advertising is only one of the alleged reasons for the interceptions at issue in this case. Plaintiffs also allege that Google intercepted emails for the purposes of creating user profiles. See ECF No. 38–2 ¶ 95. Section 17, to the extent that it suggests interceptions, only does so for the purposes of providing advertising, not creating user profiles. Accordingly, the Court finds that neither section of the Terms of Service establishes consent.

*14 The Privacy Policies in effect from August 8, 2008, to October 3, 2010, to which all Gmail users agreed and upon which Google now relies, do not clarify Google’s role in intercepting communications between its users. The Policies stated that Google may collect “[i]nformation you provide, [c]ookies [,][l]og information[,]u[ser] communications to Google[,]a[ffiliated sites, l]inks[,]o[ther sites.” See ECF No. 46–7 at 2–3. Google described that it used such information for the purposes of “[p]roviding our services to users, including the display of customized content and advertising.” Id. at 3. In 2010, Google later updated the Policy to state that the collected information would be used to “[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services.” See ECF No. 46–9 at 3. Nothing in the Policies suggests that Google intercepts email communication in transit between users, and in fact, the policies obscure Google’s intent to engage in such interceptions. The Privacy Policies explicitly state that Google collects “user communications ... to Google.” See ECF No. 46–7 at 3 (emphasis added). This could mislead users into believing that user communications to each other or to nonusers were
not intercepted and used to target advertising or create user profiles. As such, these Privacy Policies do not demonstrate explicit consent, and in fact suggest the opposite.

After March 1, 2012, Google modified its Terms of Service and Privacy Policy. The new policies are no clearer than their predecessors in establishing consent. The relevant part of the new Terms of Service state that when users upload content to Google, they “give Google (and those [Google] work[s] with) a worldwide license to use ..., create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), ... and distribute such content.” See ECF No. 46–6 at 3. The Terms of Service cite the new Privacy Policy, in which Google states to users that Google “may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes: [d]evice information[,] [l]og information[,] [l]ocation information[,] [u]nique application numbers[,] [l]ocal storage[,] [c]ookies[,] and anonymous identifiers.” ECF No. 46–10 at 3. The Privacy Policy further states that Google “use[s] the information [it] collect[s] from all [its] services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and [its] users. [Google] also use[s] this information to offer you tailored content—like giving you more relevant search results and ads.” See ECF No. 46–10 at 3. These new policies do not specifically mention the content of users’ emails to each other or to or from non-users; these new policies are not broad enough to encompass such interceptions. Furthermore, the policies do not put users on notice that their emails are intercepted to create user profiles. The Court therefore finds that a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements. Accordingly, the Court finds that it cannot conclude at this phase that the new policies demonstrate that Gmail user Plaintiffs consented to the interceptions.

Finally, Google contends that non-Gmail users—email users who do not have a Gmail account and who did not accept Gmail’s Terms of Service or Privacy Policies—nevertheless impliedly consented to Google’s interception of their emails to and from Gmail users, and to Google’s use of such emails to create user profiles and to provide targeted advertising. ECF No. 44 at 19–20. Google’s theory is that all email users understand and accept the fact that email is automatically processed. Id. However, the cases Google cites for this far-reaching proposition hold only that the sender of an email consents to the intended recipients’ recording of the email—not, as has been alleged here, interception by a third-party service provider. See State v. Townsend, 57 P.3d 255, 260 (Wash.2002) (finding consent and therefore no violation of Washington’s privacy act when email and instant message communications sent to an undercover police officer were used against criminal defendant); State v. Lott, 879 A.2d 1167, 1172 (N.H.2005) (same under New Hampshire law); Commonwealth v. Proetto, 771 A.2d 823, 829 (Pa.Super.Ct.2001) (holding that the Pennsylvania anti-wiretapping law was not violated when the recipient forwarded emails and chat messages to the police). Google has cited
no case that stands for the proposition that users who send emails impliedly consent to interceptions and use of their communications by third parties other than the intended recipient of the email. Nor has Google cited anything that suggests that by doing nothing more than receiving emails from a Gmail user, non–Gmail users have consented to the interception of those communications. Accepting Google’s theory of implied consent—that by merely sending emails to or receiving emails from a Gmail user, a non–Gmail user has consented to Google’s interception of such emails for any purposes—would eviscerate the rule against interception. See Watkins, 704 F.2d at 581 (“It would thwart th[e] policy [of protecting privacy] if consent could routinely be implied from circumstances.”). The Court does not find that non-Gmail users who are not subject to Google’s Privacy Policies or Terms of Service have impliedly consented to Google’s interception of their emails to Gmail users.

*15 Because Plaintiffs have adequately alleged that they have not explicitly or implicitly consented to Google’s interceptions, the Court DENIES Google’s Motion to Dismiss on the basis of consent.9

***

V. CONCLUSION

*24 For the foregoing reasons, the Court hereby GRANTS Google’s Motion to Dismiss with leave to amend with respect to Plaintiffs’ CIPA section 632 claims and Plaintiffs’ Pennsylvania law claim as it relates those who received emails from Gmail users. The Court DENIES Google’s Motion to Dismiss with respect to all other claims. Plaintiffs shall file any amended complaint within 21 days of this order. Plaintiffs may not add new causes of action or parties without a stipulation or order of the Court under Rule 15 of the Federal Rules of Civil Procedure. Failure to cure deficiencies will result in dismissal with prejudice.

IT IS SO ORDERED.

Footnotes

1 In this Order, the Court uses “Gmail users” to refer to individuals who send or receive emails using the free Gmail service or Google apps. “Non–Gmail users” refers to email users who do not themselves use Gmail (through the free service or Google Apps). “Google Apps users” refers to the subset of Gmail users who access Gmail through either the Google Apps Partner Program or Google Apps for Education.

4 The Court does not find persuasive Google’s slippery slope contention that a narrow interpretation of the ordinary course of business exception will make it impossible for electronic communication service providers to provide basic features, such as email searches or spam control. ECF No. 44 at 12–13. Some of these may fall within a narrow
definition of “ordinary course of business” because they are instrumental to the provision of email service. Further, a service provider can seek consent to provide features beyond those linked to the provision of the service.
