

No. 07-56640

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JUSTIN BUNNELL, FORREST PARKER, WES
PARKER and VALENCE MEDIA, LTD.,
Plaintiffs-Appellants,

v.

MOTION PICTURE ASSOCIATION OF AMERICA,
Defendant-Appellee.

Appeal from Final Judgment of the
United States District Court for the Central District of California
The Honorable Florence-Marie Cooper

APPELLANTS' OPENING BRIEF

Ira P. Rothken (SBN 160029)
Robert L. Kovsky (SBN 61770)
ROTHKEN LAW FIRM LLP
3 Hamilton Landing, Suite 280
Novato, CA 94949
Telephone: (415) 924-4250
Facsimile: (415) 924-2905

Attorney for Appellants
Justin Bunnell, Forrest Parker, Wes
Parker and Valence Media, Ltd.

TABLE OF CONTENTS

	<u>page</u>
Corporate Disclosure Statement of Valence Media, Ltd.	1
Appellants’ Request for Oral Argument	1
Jurisdiction	2
Introduction	3
Issues Presented for Review	3
Statement of the Case	4
 STATEMENT OF FACTS	 5
A. MPAA and Its Involvement with Rob Anderson	5
B. The Vaga Ventures/MPAA Agreement and Negotiations Leading Thereto	8
C. The Anderson Documents	10
D. MPAA’s Review of the Anderson Documents	13
E. MPAA’s Disclosure and Use of the Anderson Documents	14
F. MPAA Paid For and Ratified its Acquisition of the Anderson Documents	15
G. The Real Rob Anderson and His Deeds	16
H. Details of the Means Used by Anderson to Acquire the Emails	19
 SUMMARY OF ARGUMENT	 25

LEGAL ARGUMENT	31
I. Anderson Intercepted Electronic Communications In Violation of the Wiretap Act.	31
A. Procedural Context and Standard of Review	31
B. The Definitional Problem in the ECPA	32
C. The <i>Konop</i> “Judicial Definition of ‘Intercept’,” Implicitly Approved by Congress, Stands Independent of Its Derivation From a Superseded Statute That Contained the Phrase “In Electronic Storage.”	35
D. Application of the <i>Konop</i> “Judicial Definition of ‘Intercept’” to the Facts of this Case Establishes that Anderson Violated the Wiretap Act When He Acquired Emails Through the Use of the Device He Set in Plaintiffs’ Computer System.	39
E. The District Court’s Interpretation of <i>Konop</i> Was Erroneous	42
II. The ECPA Does Not Preempt California’s Invasion of Privacy Act.	49
III. The District Court Erroneously Dismissed Plaintiffs’ Trade Secrets Claim.	53
A. Procedural Context and Standard of Review	53
B. The Anderson Documents Were Sufficiently Identified.	54
C. The Anderson Documents Qualify As Trade Secrets.	58
IV. The District Court Erroneously Dismissed Plaintiffs’ Claim Under California’s Unfair Competition Law.	62

CONCLUSION 64

Statement of Possibly Related Case 65

Certificate of Compliance 66

INDEX OF AUTHORITIES

page

DECISIONS OF THE UNITED STATES SUPREME COURT

<i>Kovacs v. Cooper, Judge</i> , 336 U.S. 77; 69 S. Ct. 448; 93 L. Ed. 513 (1948)	45
<i>Locke v. Davey</i> , 540 U.S. 712, 158 L. Ed. 2d 1, 124 S. Ct. 130 (2004)	56
<i>Towne v. Eisner</i> , 245 U.S. 418, 62 L. Ed. 372, 38 S. Ct. 158 (1918)	48

DECISIONS OF THE LOWER FEDERAL COURTS

<i>Apollo Technologies Corp. v. Centrosphere Indus. Corp.</i> , 805 F. Supp. 1157 (D.N.J. 1992)	60
<i>Black, Sivalls & Bryson, Inc. v. Keystone Steel Fabrication, Inc.</i> , 584 F.2d 946 (10th Cir. 1978)	60
<i>Chevron USA, Inc. v Cayetano</i> , 224 F3d 1030 (9 th Cir. 2000) <i>cert den</i> 532 US 942, 121 S Ct 1403, 149 L Ed 2d 346 (2001)	54
<i>Forro Precision, Inc. v. Intern. Business Machines</i> , 673 F.2d 1045 (9th Cir. 1982)	57
<i>Fraser v. Nationwide Mut. Ins. Co.</i> , 352 F.3d 107 (3d Cir. 2003)	44
<i>Garcia v. Haskett</i> , 2006 U.S. Dist. LEXIS 46303, No. C 05-3754 CW (N. D. Cal. June 30, 2006)	37

<i>Ideal Aerosmith, Inc. v. Acutronic United States, Inc.</i> , 2008 U.S. Dist. LEXIS 33463, No. 07-1029 (W. D. Pa., April 23, 2008)	52
<i>Imax Corp. v. Cinema Technologies, Inc.</i> , 152 F.3d 1161 (9 th Cir. 1998).....	53, 56, 57, 62
<i>In Re Pharmatrak, Inc. Privacy Litigation, Noah Blumofe</i> , 329 F.3d 9 (1 st Cir. 2003).....	21, 36
<i>In re Toys R Us, Inc., Privacy Litigation</i> , 2001 U.S. Dist. LEXIS 16947, MDL No. M-00-1381 MMC (N.D. Cal. 2001).....	44
<i>Ip v. United States</i> , 205 F.3d 1168 (9 th Cir. 2000).....	48
<i>Knudsen Corp. v. Ever-Fresh Foods, Inc.</i> , 336 F. Supp. 241 (C.D. Cal. 1971).....	58
<i>Konop v. Hawaiian Airlines</i> , 302 F.3d 868 (9 th Cir. 2002) <i>cert. denied</i> , 537 U.S. 1193, 154 L. Ed. 2d 1028, 123 S. Ct. 1292 (2003).....	passim
<i>Konop v. Hawaiian Airlines, Inc.</i> , 236 F.3d 1035 (9 th Cir. 2001) (withdrawn <i>Konop</i>).....	26, 29
<i>MAI Systems Corp. v Peak Computer, Inc.</i> , 991 F 2d 511 (9 th Cir 1993)	53, 60
<i>Mid-Michigan Computer Systems, Inc. v. Marc Glassman, Inc.</i> , 415 F.3d 505 (6 th Cir., 2005)	59
<i>Mixing Equipment Co. v. Philadelphia Gear, Inc.</i> , 312 F. Supp. 1269 (E.D. Pa. 1974) <i>modified</i> , 436 F.2d 1308 (3 ^d Cir. 1971)	59
<i>Peters v. Burlington N. R.R. Co.</i> , 914 F.2d 1294 (9 th Cir. 1990).....	32

<i>Quon v. Arch Wireless Operating Co.</i> , 445 F. Supp. 2d 1116 (C.D. Cal. 2006), affirmed in part and reversed in part by, remanded by <i>Quon v. Arch Wireless Operating Co.</i> , 2008 U.S. App. LEXIS 12766 (9th Cir. Cal., June 18, 2008).....	52
<i>Religious Technology Center v. Netcom On-Line Communication Services, Inc.</i> , 923 F. Supp. 1231 (N.D. 2005).....	59
<i>Smith v. United States</i> , 953 F.2d 1116 (9 th Cir. 1991).....	45
<i>Steve Jackson Games, Inc. v. United States Secret Service</i> , 36 F.3d 457 (5th Cir. 1994)	38
<i>Theofel v. Farey-Jones</i> , 341 F.3d 978 (9 th Cir. 2003) (withdrawn <i>Theofel</i>).....	26
<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9 th Cir. 2004) <i>cert. den. sub nom. Farey-Jones v. Theofel</i> , 543 U.S. 813, 125 S. Ct. 48, 160 L. Ed. 2d 17 (2004).....	26, 27, 35, 44
<i>United States of America v. Steiger</i> , 318 F.3d 1039 (11th Cir. 2003) <i>cert den.</i> 538 U.S. 1051, 123 S. Ct. 2120, 155 L. Ed. 2d 1095 (2003).....	21
<i>United States v Luong</i> 471 F3d 1107 (9th Cir. 2006), <i>cert. den.</i> 128 S Ct 532, 169 L Ed 2d 371 (2007).....	41, 44
<i>United States v. Councilman</i> , 373 F.3d 197 (1st Cir. Mass., 2004) (withdrawn <i>Councilman</i>).....	passim
<i>United States v. Councilman</i> , 418 F.3d 67 (1 st Cir. 2005).....	passim
<i>United States v. Hall</i> , 543 F.2d 1229 (9 th Circuit 1976).....	52

<i>United States v. Little</i> , 753 F.2d 1420, 1434 (9 th Cir. 1984).....	52
<i>United States v. Smith</i> , 155 F.3d 1051 (9 th Cir. 1998) <i>cert. denied</i> 525 U.S. 1071, 119 S. Ct. 804, 142 L. Ed. 2d 664 (1999).....	passim
<i>United States v. Smith</i> , 726 F.2d 852 (1 st Cir. 1984)	52
<i>United States v. Turk</i> , 526 F.2d 654 (5 th Cir. 1976)	40
<i>Universal Analytics v. MacNeal-Schwendler Corp.</i> , 707 F. Supp. 1170 (C.D. Cal. 1989), <i>aff'd</i> , 914 F.2d 1256 (9 th Cir. 1990)	57
<i>Vermont Microsystems v. Autodesk, Inc.</i> , 88 F.3d 142 (2 ^d Cir. 1996).....	59

FEDERAL STATUTES

7 USCS § 230(e)(4).....	50
15 U.S.C. §§ 2510 <i>et. seq.</i>	passim
18 U.S.C. § 2510(4)	33
18 U.S.C. § 2510(12)	33
18 U.S.C. § 2511(1)(c).....	31
18 U.S.C. § 2511(1)(d).....	31
18 U.S.C. § 2510(12)	33
18 U.S.C. § 2518	50
18 U.S.C. § 2518(1)(c).....	44

18 U.S.C. § 2518(10)(c).....	50, 52
18 U.S.C. § 2520(a)	31
18 U.S.C. §§ 2701 <i>et. seq.</i>	32, 33, 36, 43
18 U.S.C. § 2701(a)	33
18 U.S.C. § 2703(a)	44
18 U.S.C. § 2710(a)	33
28 U.S.C. § 1291	2
28 U.S.C. § 1331	2
28 U.S.C. § 1367(a)	2
USA PATRIOT Act § 209, 115 Stat. at 283.....	38

FEDERAL RULES

Fed.R.Evid. 201	12
-----------------------	----

STATE COURT CASES

<i>Abba Rubber Co. v. Seaquist</i> , 235 Cal. App. 3d 1, 235 Cal. App. 3d 1	58
<i>Cadence Design Systems, Inc. v. Avant! Corp.</i> , 29 Cal. 4th 215, 127 Cal. Rptr. 2d 169 (2002)	60
<i>Flanagan v. Flanagan</i> , 27 Cal. 4th 766, 117 Cal. Rptr. 2d 574 (2002)	49
<i>Kearney v. Salomon Smith Barney, Inc.</i> , 39 Cal. 4th 95; 45 Cal. Rptr. 3d 730 (2006)	51
<i>People v. Conklin</i> , 12 Cal.3d 259, 114 Cal. Rptr. 241 (1974)	51
<i>Ribas v. Clark</i> , 38 Cal. 3d 355, 212 Cal. Rptr. 143 (1985)	49
<i>Schnall v. Hertz Corp.</i> , 78 Cal. App. 4th 1144, 93 Cal. Rptr. 2d 439 (2000)	63

STATE STATUTES

Cal. Bus. & Prof. Code §§ 17200 <i>et. seq.</i>	30, 62
Cal. Civil Code §§ 3426.1 <i>et. seq.</i>	53, 62
Cal. Civil Code § 3426.1(d)	58, 60
Cal. Code Civ. Proc. § 2019.210	55
Cal. Penal Code §§ 630 <i>et. seq.</i>	3, 25, 29, 49
Cal. Penal Code § 631	49

OTHER AUTHORITIES AND REFERENCES

Brief of Senator Patrick Leahy (<i>amicus curiae</i> in <i>Councilman</i>) (available at http://www.eff.org/cases/us-v-councilman).....	44
Frank, <i>Law and the Modern Mind</i> (rev. printing 1935).....	45
H. L. A. Hart, <i>The Concept of Law</i> (1975 reprint)	45
Houser et al., RFC 1865: EDI Meets the Internet (Jan. 1996), at http://www.ietf.org/rfc/rfc1865.txt	40
Merriam-Webster Online Dictionary at http://mw1.merriam- webster.com/dictionary/contemporaneous	41
Popper, <i>The Open Society and Its Enemies</i> (1950).....	46
Wikipedia, "The Pirate Bay," http://en.wikipedia.org/wiki/The_Pirate_Bay	12

**CORPORATE DISCLOSURE STATEMENT
OF VALENCE MEDIA, LTD.**

Pursuant to Federal Rule of Appellate Procedure 26.1 and Circuit Rule 26-1, appellant Valence Media, Ltd. states that it has no parent corporation and that there is no publicly held corporation that owns 10% or more of its stock.

APPELLANTS' REQUEST FOR ORAL ARGUMENT

The issues are complex and important for the protection of Internet privacy; and appellants request oral argument.

JURISDICTION

Plaintiffs/appellants Justin Bunnell, Forrest Parker, Wes Parker and Valence Media, Ltd. (hereinafter “plaintiffs”) allege that defendant/appellee Motion Picture Association of America (“hereinafter “MPAA”) violated the Wiretap Act (15 U.S.C. §§ 2510 *et. seq.*) when it paid [REDACTED] for emails and other confidential materials from an intruder into plaintiffs’ computer system who had acquired them through a continually operating software device and when MPAA circulated those materials internally and to consultants who were helping MPAA prepare to sue plaintiffs in a “copyright action.” Federal question jurisdiction was therefore established pursuant to 28 U.S.C. § 1331; and pendant and supplemental jurisdiction was established pursuant to 28 U.S.C. § 1367(a) over state law claims for invasion of privacy, misappropriation of trade secrets and unfair competition.

On September 7, 2007, the District Court filed a Final Judgment and Dismissal of All Claims. Excerpts of Record (hereinafter “ER”) at 19. Plaintiffs’ Notice of Appeal was filed on October 5, 2007. (ER 13.) Appeal is taken from said Final Judgment pursuant to 28 U.S.C. § 1291.

INTRODUCTION

This case will help define privacy protections for emails and other Internet communications under the Electronic Communications Privacy Act and under California’s Invasion of Privacy Act. There is no dispute about the concrete, material facts. The intruder – who broke into plaintiffs’ computers, acquired emails and other documents and sold them to MPAA – confessed and was deposed during trial court proceedings. The area of law has been described by this Court as complex and convoluted.

ISSUES PRESENTED FOR REVIEW

1. Whether “interceptions” were committed under the Wiretap Act (Title I of the Electronics Communications Privacy Act or ECPA) by an unauthorized intruder into plaintiffs’ email server who re-configured a standard feature of operating software so that, from that moment forward, on each occasion that an authorized user of the system sent or received an email, an unauthorized copy of the email (including attachments) was also made and sent to the intruder at a remote email address the intruder had established.
2. Whether California’s Invasion of Privacy Act, Cal. Penal Code §§ 630 *et. seq.*, a state law version of the Wiretap Act, with broader reach than the federal version, is preempted by the ECPA.
3. Whether “trade secret” status may be accorded to a specific set of 28

pages of emails, financial records and other materials misappropriated by an intruder from computers belonging to plaintiffs, for which an investigator paid ██████████ when the documents were selected by the intruder from a far larger body of misappropriated documents according to the investigator's criteria so as to include private emails involving potential business deals between plaintiffs as investigative targets and other potential investigative targets supposedly engaged in a "conspiracy" and also to include private technical information about plaintiffs' computer arrangements, plus other financial records and personal information about plaintiffs.

4. Whether there was sufficient evidence of an "unlawful, unfair or fraudulent business practice" to support plaintiffs' claim under California's Unfair Competition Law.

STATEMENT OF THE CASE

Plaintiffs filed their Complaint in the District Court on May 24, 2006. (ER 101-116.) In July of 2007, Plaintiffs and Defendant each filed a Motion for Summary Judgment. (ER 451-455, 2597-98.) The district court granted defendant MPAA's motion for summary judgment and denied plaintiffs' motion for partial summary judgment. (ER 1-12.) This appeal followed.

STATEMENT OF FACTS

A. MPAA and Its Involvement with Rob Anderson

MPAA is a trade association with offices in Encino, California. (ER 103:24-25, 120:5-7.) Its members include movie studios and television producers who sued plaintiffs in a separate “copyright action” for operating TorrentSpy, a BitTorrent search engine, which “allegedly enables and encourages Internet users to locate and download unauthorized copies of copyrighted motion pictures and television shows for free.” (Order of the District Court at ER 2: 7-14 and 2:26-28; please see Statement of Possibly Related Case.)

In June of 2005, Dean C. Garfield, a lawyer, was MPAA’s “Vice-President, Director of Legal Affairs, World-Wide Anti-Piracy.” Garfield directed and supervised investigations of Internet copyright infringement, including investigations of TorrentSpy that would lead to the filing of the copyright action. (ER 184:20-19:4, 188:16-21:14, 143:10-17, 167:26-168:17.) MPAA has admitted that it is responsible for the acts of Garfield at issue herein. (ER 143:1-145:17.)

In June 2005, Rob Anderson came via email to MPAA, offering to shut down TorrentSpy and claiming to have “an insider viewpoint.” (ER 2056.) Anderson dealt principally with Garfield, communicating via voice telephone and the Internet. (ER 2054-56, 204:1-6, 208:4-19.)

The origin, development and fruition of the Anderson-Garfield relationship

is shown in a string of emails set forth in full at ER 2046 - 2056, in reverse chronological order. Anderson first wrote to MPAA Vice-President John Malcolm on June 7, 2005, claiming to represent “Vaga Global” and “Vaga Ventures, LLC” and to “offer our services in shutting down BitTorrent search engines.” (ER 2056.) Anderson declared that “we would like to target torrents.py.com (current largest) and their surrounding network for MPAA.” “Vaga Global spent six months investigating torrents.py.com/ircspy on behalf of our clients and found it to be generating six figures of monthly income ... They also supply ad revenue and management for nearly every BitTorrent search engine - including SuprNova.org before it was shutdown.” (*Ibid.*)

“Vaga Ventures” was a figment of Rob Anderson’s imagination. “It’s a company that I started, but it’s not registered; so it’s not an official company, but it was going to be.” (ER 308:11-14.) [REDACTED]

[REDACTED] (ER 197:14-199:4, 207:15-208:19, 253:3-25.)

Malcolm immediately sent copies of Anderson’s inquiry to Garfield and soon Garfield took over. (ER 2054-2056.) Garfield and Anderson spoke by telephone on Wednesday, June 15, 2005 and Anderson sent Garfield a written proposal offering to provide “Anti-Piracy Information Services” for \$15,000.00 and “Ad Campaign Creatives” for \$12,000.00. (ER 2053, 299-300.) Anderson wrote: “As for the information services: We can provide the names, address, &

phone of the owners of torrents.py.com and thepiratebay.org - along with evidence, including correspondence between the two companies.” (ER 299, 2051.) “My hope is that in the future you’ll keep us near the top of the list for any additional work that the MPAA might have.” (ER 2051.)

On the following Monday, June 20, 2005. Garfield inquired: “Are you available for an in person meeting in LA next week or a videoconference?” (ER 2050.)

Responding to Garfield’s invitation to meet “in person,” Anderson wrote back: “Not sure about meeting in LA.” Anderson wrote nothing about a videoconference. (ER 2050.)

While declining to face Garfield, Anderson wrote in the same message:

“
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]”

(ER 2050.)

Garfield replied: “We can meet or not, I am not committed to a meeting.”

Garfield was interested in [REDACTED]

[REDACTED]

[REDACTED].” (ER 2050.)

When Anderson pressed Garfield about “the creative campaign,” (ER 2050), Garfield responded:

“I am not interested in wasting your or my time. [REDACTED] [REDACTED] if you would like to proceed on that basis. Great. If not no loss. We can put together a contract on that information by Thursday.” (ER 2049.)

B. The Vaga Ventures/MPAA Agreement and Negotiations Leading Thereto

On June 30, 2005, as “Director of Business Development” of “Vaga Ventures, LLC,” Rob Anderson signed a Written Agreement prepared by MPAA and signed by Dean C. Garfield as MPAA Vice-President & Director, Legal Affairs. (ER 263-64, 192:3-192:24, 239:8-240:22.)

In paragraph 1, Vaga Ventures promised to provide [REDACTED]

[REDACTED]

[REDACTED]. In paragraph 2, Vaga Ventures expressly represented and warranted that it was in lawful possession of the Information and that it had obtained such Information by legal means. [REDACTED]

[REDACTED]

[REDACTED]

that the MPAA is [REDACTED]

[REDACTED]

MPAA would pay [REDACTED] to Anderson. (ER 263-264.)

During negotiations over a draft of the agreement, Anderson objected to a provision that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (ER at 205:11-206:23, 209:9-16, 210:23-211:17, 212:1-214:10, 231:23-232:2, 238:24-240:22, 263-267.)

Garfield testified that, prior to entering into the Agreement, he thought it was important to establish that the information had been obtained legally, as stated in paragraph 2 in the Agreement. (ER 1113:15-25.) The steps that Garfield took were by speaking with Mr. Anderson, by having him attest to lawful possession and distribution of the information to MPAA and by memorializing that fact in writing. (ER 1115:8-19.) [REDACTED]

[REDACTED]

(ER 1117:13-16.)

According to Garfield, Anderson told him of having worked for Apple, Take Two and Toshiba. "...they were companies I was generally aware of. And they had a certain air of credibility to them." (ER 1119:1-9.) [REDACTED]

[REDACTED]

[REDACTED]. (ER 197:22-24, 198:24-199:4.) Garfield could not recall having attempted to learn any information about Vaga Ventures. (ER 199:5-22.) [REDACTED]

[REDACTED]. (ER 207:15-22.) He has never [REDACTED]

[REDACTED]. (ER 208:4-16.)

Garfield testified: “[REDACTED]

[REDACTED].” (ER 199:2-4.)

C. The Anderson Documents

On or about June 30, 2005, “contemporaneous” with the signing of the Vaga Ventures/MPAA agreement, Anderson sent to Garfield an email with documents attached, called “the Anderson Documents” herein. (ER 195:1-16, 216:19 - 224:2 and Exhibit 6).

The record¹ contains multiple sets of the Anderson Documents; we refer to a set submitted by MPAA in support of its Motion for Summary Judgment located at ER 1165-1199; this is the only set with the page at ER 1195.

Anderson testified that he selected documents based on discussions with

¹ In general, the record is highly repetitious, but with variant versions of document packages; and there does not appear any way to clarify the record that would be approved by both sides.

Garfield:

“we had an oral discussion by telephone about money. And in that regard, he made it very clear by the telephone - Dean Garfield did - about -- that [REDACTED]

[REDACTED]

“So then I inquired what -- what is useful to him or what does he consider useful, and he basically gave me [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]” (ER 316:1-317:17.)

Examination of the entire document package, infra, shows that the Anderson Documents [REDACTED] [REDACTED]. Here, attention is directed at documents ER 1188-1199, which consist of emails between Justin Bunnell and other persons and organizations, along with supplementary materials that were apparently obtained and/or prepared by Anderson.

The emails within ER 1188-1199 document past, present and possible future financial involvement of Justin Bunnell and his associates with, among others,

[REDACTED], [REDACTED], [REDACTED], [REDACTED] or

[REDACTED], [REDACTED], [REDACTED] and [REDACTED].

[REDACTED] wrote: “[REDACTED]
[REDACTED]
[REDACTED]” (ER 1191-1192)

Supplementary materials identify the corporate/principal identities of [REDACTED] and [REDACTED] (ER 1195-1198) and identify [REDACTED] and [REDACTED] as officers of [REDACTED], which is supposedly owned by [REDACTED] (ER 1190).²

[REDACTED]’s monetary transactions with plaintiffs are documented in plaintiffs’ cash flow statements at ER 1166-1167, showing receipt of \$ [REDACTED] in [REDACTED]. Transactions with [REDACTED] also appear.³

The Anderson Documents include email communications between Bunnell and the purported principals of [REDACTED] that discuss ongoing use of an [REDACTED]

² According to the online common-knowledge resource, Wikipedia, “[REDACTED] is known in the online file sharing community as one of the more prominent websites which distributes torrents that point to unlicensed copies of copyrighted material as well as open source free content.”

[REDACTED] Please see Fed.R.Evid. 201.

³ [REDACTED] is a provider of online services to the BitTorrent technology community that is being sued in another action pending in the District Court for the [REDACTED] District of California. [REDACTED] presiding, entitled “[REDACTED]

[REDACTED] Plaintiffs’ complaints in the two cases are closely similar, plaintiffs there are identical to those in this case and counsel between the cases are overlapping. Please see Fed.R.Evid. 201.

“ [REDACTED]

[REDACTED]

[REDACTED].” (ER 1191-1194.)

Garfield testified that his understanding was:

“we were going to get information about the location and identity of the people who were running Torrentspy. T-o-r-r-e-n-t-s-p-y, as well as information related to a general conspiracy and relationship between Torrentspy and a number of other prominent services including ThePirateBay.” (ER 197:7-13.)

Anderson testified that, in pre-contractual discussions with Garfield:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].” (ER 319:11-29:5.)

D. MPAA’s Review of the Anderson Documents

Anderson testified that, in a telephone discussion with Garfield immediately after Garfield had received the documents, Garfield went through the documents with him “page by page.” Anderson testified that:

“I think he was under the assumption we had these documents already. And when he saw that -- these dates of the e-mails that were on the header of the e-mail saying they were from this date, he asked me, ‘These are very recent.’ He said, ‘How did you get them?’ And I basically said that you can get -- I -- I told him -- I said, ‘I knew you’d want the latest information, and -- and we can get really whatever we want from our informant.’”

(ER 321:23-322:22, 350:9-1; see also the top of ER 2046, Garfield setting up the call.)

What appear to be important emails involving possible business dealings between TorrentSpy and [REDACTED] (ER 1191-1192) are dated June 7, 2005, the same date as Anderson’s first email to Malcolm. Three significant emails are dated June 20, 2005 (ER 1189, 1194). The most recent email is dated June 24, 2005 (Bunnell to [REDACTED] and [REDACTED] “[REDACTED] [REDACTED]”) (ER 1193.)

Garfield recalled the June 30, 2005 telephone conversation with Anderson immediately after the documents were delivered and testified: “We discussed the information he faxed on Torrentspy. [REDACTED].” (ER 197:6-19.)

E. MPAA’s Disclosure and Use of the Anderson Documents

Thereafter, Garfield sent copies of the Anderson Documents to Chad Tilbury

their dealings with Rob Anderson. After dealing with Anderson, Garfield was promoted by MPAA. (ER 188:16-189:5.)

G. The Real Rob Anderson and His Deeds

Plaintiffs submit that Rob Anderson did not acquire the Anderson Documents by lawful means. Rather, Rob Anderson got the Anderson Documents by invading the privacy of and betraying his former employer, Justin Bunnell, along with similar invasions and betrayals of Wes Parker and Forrest Parker, whom Anderson called his friends.

Starting in 2001, Anderson had been employed by BA Ventures, a company run by plaintiff Justin Bunnell. Anderson worked as an independent contractor, earning commissions on online advertising deals, with the title “Director of Business Development.” (ER 86:10-15.) Anderson named his phony company, Vaga Ventures, after Bunnell’s BA Ventures and took his phony title from the title he used while working for Bunnell.

Anderson testified that he wanted “to get information from those parties that I had stopped working with and basically see sort of, you know, if -- if -- sort of what they were talking about after I left, and numerous other things like that. And that was basically the original intent.” (ER 311:25-312:8.)

Anderson testified: “I provided Dean with information under the pretext that

at the time me and Justin Bunnell, who were previous -- previously in business together, that both his partners, new partners, Wesley -- Forrest Parker and Wes Parker, who were previously friends of mine and people who did work for me, who I introduced to Justin, that they had stopped doing business with me and he had left with them.” (ER 351:24-352:6.)

Anderson testified that, months later, after he was estranged from MPAA, Justin had friendly communications with him, he regretted his deal with MPAA and he confessed to Justin. (ER 352:7-353:13.)

Anderson testified that he acquired the documents he sent to Garfield after he learned how:

“to get into the e-mail servers of Valence Media or Justin Bunnell, whoever, and into their e-mail servers; and basically configuring their e-mail server to intercept them and -- intercept all information that they were sending back and forth between each other - Justin Bunnell, Forrest Parker, Wes Parker - and forward it to a Gmail account under my control.”

(ER 309:5-121, 310:7-20, Exhibit 3, ER 366-371, Anderson’s confession and declaration.)

“Gmail” is a popular, free service offered by Google. Any person can obtain an email address that preserves anonymity. (ER 86:20-28.)

Anderson never had any authorization to get into plaintiffs’ email servers or

to alter their configurations. (ER 86:14-19, 94:2-5, 312:14-24.). Anderson used his previous knowledge of plaintiffs, their computer system and their old passwords to guess the password that gave him access to the email server. (ER 311:1-13.)

Anderson got into plaintiffs' email servers and set up the Gmail account at some point about April of 2005. (ER 311:15-24.) During his deposition, as an exemplar, Anderson identified "a typical printout of a Gmail page that's related to this account with an e-mail that appears to be ... an intercepted e-mail about financial information related to Justin and Forrest Parker and a attached document that has ... an Excel sheet about financial information." (ER 313:11-314:19 and Exhibit 4 at ER 384.)

Anderson testified: "My understanding was to intercept everything." (ER 314:24.) "Everything" for the time period between June 19, 2005 and July 9, 2005 is listed at ER 2499-2566, with approximately 2500 entries.

After selecting the materials to give to MPAA, Anderson prepared the Anderson Documents from Gmail materials by the technique of cut-and-paste. For example, an email from Justin Bunnell to [REDACTED] that appears in the Anderson Documents (ER 1188) was prepared from a larger Gmail document and, apparently, Anderson added the title [REDACTED] at the top of the document. (ER 337:1-338:4, 407-409.)

After delivering the Anderson Documents and receiving payment, Anderson maintained contact with Garfield for some time. Anderson testified that, in 2005, “There was a discussion maybe a month -- or, sorry, months - three months - after giving the information. [REDACTED]

[REDACTED] (ER 323:24-324:7.)

H. Details of the Means Used by Anderson to Acquire the Emails

Plaintiffs need to establish a violation of the Wiretap Act as to only a single email in order to prevail. For purposes here, we choose outgoing emails such as the email from Justin Bunnell to [REDACTED] discussed immediately supra. (See ER 1188 and 407-409.)

In the Spring of 2005, Plaintiff Valence Media maintained its email server – a computer dedicated to email service and permanently connected to the Internet – at a facility in Los Angeles run by an independent provider, “CalPop.” This server processed Internet communications for several email addresses used by Valence Media, Justin Bunnell, Forrest Parker, Wes Parker, Torrentspy, BA Ventures and other persons and organizations connected with plaintiffs. (ER 93:14-23.) It used a Windows operating system and an email service application known as “Merak Mail Server.” (ER 93:27-3:1.)

MPAA expert witness Ellis Horowitz described some details of Anderson’s

meddling with the server: (ER 1917:25-1918:2.)

“Mr. Anderson used an existing feature of the Merak e-mail server software operated by the Bunnell parties (the “copy and forward” feature) to configure the Bunnell parties’ server to send copies of messages to the Gmail account he had opened.” (ER 1919:7-10.)

Matthew Curtin, plaintiffs’ expert witness declared that the Merak Mail Server is a typical member of a class of email server software suites used in internet operations, providing all the functions and features that would be expected in software in the class. What Anderson did to acquire emails could likely be reproduced on any member of the class of email server programs.

“The key conclusion - that email messages were copied and forwarded to an interloper's email mailbox while the messages were in transit - would, with a high degree of likelihood, be much the same for any typical member of the class.”
(ER 447:17-448:3.)

Curtin’s Declaration (ER 444-450) described email transmission as a series of functional processes, chiefly the transformation of a message into uniform “packets” of information, the sending out of packets, the guided travels of separate packets through the Internet, the receipt of packets at the other end and the reconstitution of a message. (ER 446:19-447:447:10.) Separate software modules, e.g., “mail transfer agents” and “local delivery agents” carry out particular

functions. (ER 448:4-449:13.)

Mr. Curtin concluded that the means that Anderson used to acquire emails “was equivalent to an automatic routing program. That is, it was equivalent to a program that automatically receives and copies each message it encounters and sends a duplicate of each message to a specific addressee.”⁴

MPAA’s expert, Prof. Horowitz, on the other hand, emphasized the word “*storage*,” e.g., at 1923:23-24. In deposition, however, Prof. Horowitz acknowledged that the time spent “in storage” was very short.

When asked to confirm a time difference of five thousandths (.005) of a second between steps in a process, Prof. Horowitz stated:

⁴ In *United States of America v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003) *cert den.* 538 U.S. 1051, 123 S. Ct. 2120, 155 L. Ed. 2d 1095 (2003), the court quoted from a law review article that identified the ultimate limit point of strictness and narrowing:

“There is only a narrow window during which an E-mail interception may occur--the seconds or milliseconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of *automatic routing software* is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.” (Emphasis added.)

The court in *In Re Pharmatrak, Inc. Privacy Litigation, Noah Blumofe*, 329 F.3d 9, 22 (1st Cir. 2003) (“*Pharmatrak*”) quoted from *Steiger* and stated:

“NETcompare was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third party (Pharmatrak).”

“A. Yeah. Which could be a very long time in computer terms. A very short time in human terms.

Q. That would be considered to be transient?

A. No. I disagree with the word ‘transient.’

Q. This would be the thing in transient memory.

[Objection]

A. The exchange is going to be occurring in random access memory.” (ER 2380:16-25.)

In his Declaration in the District Court, Prof. Horowitz further stated:

“While Bunnell parties’ expert, Matthew Curtin, and I may characterize certain facts differently, it appears that we agree on the underlying facts. For example, while Mr. Curtin characterizes an e-mail message that is in temporary memory, incidental to an e-mail’s transmission, as both ‘in storage’ and ‘in transit,’ [citation], I here characterize the message as ‘in storage’ while it was in temporary memory, and then ‘in transit’ when it passed from the server’s memory onto the wires. But we agree that, however characterized, the Merak mail server copies the incoming and outgoing messages while those message are on the server, in server memory.” (ER 1928:2-11.)

Prof. Horowitz contrasted operations based on a “normal configuration” of plaintiffs’ system with operations during the period when the Anderson configuration was in place. Plaintiff submit that, during the Anderson period, operations were interwoven and were taking place concurrently.:

(1) “When the Bunnell parties’ Merak mail server was configured normally, a message would travel from the individual sender’s computer to the Bunnell parties’ Merak mail server, where it would be received and stored in server memory. While holding the message in storage, the Bunnell parties’ Merak mail server would then make contact with the ‘destination’ e-mail server belonging to the intended recipient. Once the Bunnell parties’ Merak mail server established contact with the recipient’s e-mail server, and the recipient’s server acknowledged that it was prepared to receive the e-mail, the Bunnell parties’ Merak mail server would transmit the message over the Internet to the recipient’s e-mail server.” (ER 1921:9-17.)

(2) “During the time that Mr. Anderson had configured the plaintiffs’ Merak mail server to forward copies of messages to his Gmail account, a message would still travel from the individual sender’s computer to the Bunnell parties’ Merak mail server computer, where it would be received by the server and maintained in storage. While so stored on the Bunnell parties’ Merak mail server, the Bunnell parties’ Merak mail server would contact both the intended recipient’s e-mail server and Mr. Anderson’s Gmail server. When the respective e-mail servers of the intended and of Mr. Andersons have acknowledged that they are prepared to receive the e-mail, the Bunnell parties’ Merak mail server would transmit the e-mail message to the servers in question (whether the intended recipient’s or Mr. Anderson’s).” (ER 1923:19-1924:2.)

Prof. Horowitz ran tests on a Merak Mail Server installed on his own computer “using the same function that Mr. Anderson used to copy all incoming and outgoing messages and send them to a Gmail account at ehorowitz1@gmail.com.” (ER 1921:18-25, 1924:3-6.)

According to Prof. Horowitz: “In my experiment, the Merak mail server sent the message to the ‘copy’ recipient 0.324 seconds, and 32 steps, after it sent the message to its intended recipient.” (ER 1927:1-2.)

SUMMARY OF ARGUMENT

1. Plaintiff contend that Anderson intercepted their emails and other communications in violation of the Wiretap Act. The District Court's contrary ruling should be reversed.

The District Court's ruling is contrary to the intent and purposes of the ECPA, which are to protect the privacy of electronic communications. Combined with the ruling that California's stronger Invasion of Privacy Act is preempted by the ECPA, the District Court's ruling turns the ECPA on its head so that it shows a way to invade privacy.

The case involves a “complex, often convoluted, area of the law.” *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998) *cert. denied* 525 U.S. 1071, 119 S. Ct. 804, 142 L. Ed. 2d 664 (1999) (hereinafter “*Smith*”) cited and quoted in *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002) *cert. denied*, 537 U.S. 1193, 154 L. Ed. 2d 1028, 123 S. Ct. 1292 (2003) (hereinafter “*Konop*”) and in *United States v. Councilman*, 418 F.3d 67, 80 (1st Cir. 2005) (hereinafter “*Councilman*”).

The problems were sufficiently severe that the initial opinion in *Councilman* was withdrawn⁵ and replaced by an *en banc* decision, a course of action resembling

⁵ *United States v. Councilman*, 373 F.3d 197 (1st Cir. Mass., 2004) (hereinafter “withdrawn *Councilman*”).

that which led to the withdrawal of the original *Konop* decision, *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001) (hereinafter “withdrawn *Konop*”). Similarly, a “withdrawn *Theofel*”⁶ preceded the amended *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) *cert. den. sub nom. Farey-Jones v. Theofel*, 543 U.S. 813, 125 S. Ct. 48, 160 L. Ed. 2d 17 (2004) (hereinafter “*Theofel*”). The foregoing opinions, including withdrawn opinions, are the principal opinions that show a number of separate approaches to this “complex, often convoluted, area of the law.”

The District Court ruled:

“For purposes of the ECPA, at any given time, an electronic communication may either be intercepted and actionable under the Wiretap Act or acquired while in electronic storage and actionable under the SCA.” (ER 6:2-4, emphasis in original.)

The District Court followed a ***technical approach***, which hinges on whether, at an isolated moment in the processing of the email, there is a copying of the email while the email is in “electronic storage.” The technical approach is based on a “universal criterion” that separates moments when the email might be subject to the SCA from moments when the email might be subject to the Wiretap Act. Hence, “the Court’s inquiry begins with whether said communications were

⁶ *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003).

‘intercepted’ or acquired while in ‘electronic storage.’” (ER 5:27-6:1.)

Because technical experts use the word “storage” to refer to computer memory devices, e.g. to random access memory, “the Court’s inquiry” is answered by an expert, who thereby supplies meaning for the statutory language.

The technical approach finds support in language from *Konop*, quoted in *Theofel*, that the District Court cited at ER 7:11-25. See also the “withdrawn *Councilman*” at 373 F.3d 197, 200-204, which sets forth a detailed justification for the technical approach.

Plaintiffs submit that the technical approach is contrary to the intent of the ECPA and contrary to *Konop* and *Smith*. It would substitute a technical determination for judicial judgment. It would impose a universal criterion that is unsuited to the multiple functions of the ECPA that include national security protections, judicial oversight of law enforcement, definitions of crimes and protections against private invasions of privacy, as in this case.

Instead, plaintiffs advocate a ***practical approach*** that we submit follows *Smith* and *Konop*, namely reliance on “the judicial definition of ‘intercept’ as acquisition contemporaneous with transmission.” *Konop*, supra, 302 F.3d at 878. The added, distinctive element, “contemporaneous with transmission” is sometimes called “the contemporaneity requirement.” (See, e.g., *Smith* at 155 F.3d 1056.) This is a “practical approach” because a judicial determination of

“contemporaneity” in the trial court can potentially accommodate multiple functions of the ECPA and the unique features of a case, and can also potentially adapt to changes in technology and legal environments.

Applying the judicial definition of “intercept” to the specific facts of this case, plaintiffs are entitled to a ruling that Anderson intercepted emails. The chief fact is that Anderson’s unlawful acquisition of email communications occurred during every single episode of processing by the email server over a period of several months. There were many thousands of such episodes. As to outgoing emails, during each such episode, the system generated two copies of the communication and sent one to Anderson and the other to the intended recipient. As shown by the Horowitz experiment, the two transmissions were interwoven and concurrent. They occurred closely coupled in time and both might be completed in less than a second or within a few seconds of each other. As a practical matter, there is no significant time difference between the generation of an unlawful copy to Anderson and the generation of the intended transmission. Often, both emails will be in flight at the same time, or contemporaneously. Plaintiffs submit that an ongoing accumulation of emails by means of a device set by an intruder was precisely what Congress intended to prohibit.

In addition to the technical and practical approaches, there is the approach of *Councilman* that emphasizes public policies of privacy protection and that

contemplates an ongoing process of statutory construction advancing those policies. Please see 418 F.3d at 80 where the court declines to address the issue of a “contemporaneity requirement;” and please see 418 F.3d at 82, where the court quotes another case for the proposition that “the overlapping coverage of the Wiretap Act and the Communications Act presents no problem.”

The “withdrawn *Konop*” approach, referenced *supra*, adopts expansive definitions of “interception” and “electronic communication” such that the Wiretap Act covers the field. (“We hold that the Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit.” (236 F.3d at 1046.))

Plaintiffs welcome the participation of *amici curiae* who are ably presenting privacy concerns to the court. The District Court’s ruling should be reversed because it is contrary to the ECPA, because it is impractical and because, if allowed to stand, it will shield not only those who invade the privacy of others, but also those who pay for the fruits of such invasions, as MPAA did in this case.

2. The District Court was in error when it held that plaintiffs’ claims under California’s Invasion of Privacy Act, Cal. Penal Code §§ 630-638 had been preempted by the ECPA. Evidence of Congressional intent and the overwhelming weight of case law show that no preemption occurred.

3. The District Court erroneously dismissed plaintiffs’ state law Trade Secrets

Claim for lack of specificity. The 28 pages of documents were highly specific.

MPAA paid ██████████ to get private information about plaintiffs' business dealings and internal computer arrangements that MPAA wanted for its investigation.

4. The District Court erroneously dismissed plaintiffs' claim under California's Unfair Competition Law. Even if this Court should hold that the ECPA provides no relief to plaintiffs for what MPAA did, and even if this Court should hold that plaintiffs' state law claims are preempted by the ECPA or otherwise invalid, a California state court might still find that the acts of the MPAA constituted unfair competition under California law.

LEGAL ARGUMENT

I. Anderson Intercepted Electronic Communications In Violation of the Wiretap Act.

A. Procedural Context and Standard of Review

Title 18 U.S.C. § 2520(a), part of the Wiretap Act, authorizes recovery in a civil action brought by “any person whose ... electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.” Plaintiffs allege that MPAA violated the Wiretap Act, 18 U.S.C. § 2511(1)(c) and (d), which prohibit intentionally using, disclosing or endeavoring to use or disclose any electronic communication knowing or having reason to know that the information was obtained through the unlawful interception.

The District Court stated the rule: “if Anderson acquired Plaintiffs’ emails while they were in ‘electronic storage,’ Plaintiffs’ claim under the Wiretap Act necessarily fails.” (ER 6:12-14.)

The District Court then applied the rule:

“In the instant case, Anderson’s actions necessarily fall outside the scope of the Wiretap Act. Anderson configured the Bunnell parties’ email server so that all Plaintiffs’ messages were copied and forwarded from the server to his Google email account. If the emails had not been stored on the server, Anderson would not have acquired copies of them.” (ER 8:11-15.)

The District Court concluded that “Anderson’s acquisition of the emails did not violate the Wiretap Act.” (ER 9:12-13.)

The parties are in agreement that there is no dispute over the concrete facts and that the question is one of interpretation of the facts and of the law. This Court reviews *de novo* a summary judgment and determines whether the district court properly applied the relevant substantive law. *Peters v. Burlington N. R.R. Co.*, 914 F.2d 1294, 1298 (9th Cir. 1990).

B. The Definitional Problem in the ECPA.

“[T]he intersection of the Wiretap Act (18 U.S.C. §§ 2510-2520) and the Stored Communications Act (18 U.S.C. §§ 2701-2710) is a complex, often convoluted, area of the law. This case turns, at least in part, on issues at the very heart of that intersection.”

Smith supra at 155 F.3d 1055 quoted in *Konop*, supra, at 302 F.3d at 874 and in *Councilman*, supra, at 418 F.3d at 80.

This case returns to the area of law that beset the *Smith*, *Konop* and *Councilman* courts. The problem arises from the fact that the Wiretap Act and the

Stored Communications Act (hereinafter “SCA”)⁷ share a common set of definitions, e.g., “electronic communication,”⁸ that use broad and elastic terms. The SCA incorporates definitions from the Wiretap Act. (18 U.S.C. § 2710(a)).

The operative word defining an “interception” under the Wiretap Act is “acquisition.”⁹

The operative word defining a violation under the SCA is that an unauthorized person “accesses” a facility providing communications services.¹⁰

In an era of rapid innovation in electronic services and increasing complexity in electronic communication, the boundaries of such generally-defined categories become fluid, with a tendency to expand and merge.

⁷ The Electronic Communications Privacy Act (“ECPA”) subsumes both the Wiretap Act (18 U.S.C. §§ 2510 *et. seq.*) as Title I and also the SCA (18 U.S.C. §§ 2701 *et. seq.*) as Title II. *Konop* at 302 F.3d at 874.

⁸ According to 18 U.S.C. § 2510(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 [exceptions not pertinent here].”

⁹ 18 U.S.C. § 2510(4) states that “ ‘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.”

¹⁰ 18 U.S.C. § 2701(a) provides that “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.

The tendency to merge the categories runs counter to the need to maintain functional distinctions. As to many matters, a violation of the Wiretap Act is of weightier importance than a violation of the SCA, matters that include judicial oversight of law enforcement investigations, punishments for violations, and exceptions from coverage.¹¹ If every invasion of electronic privacy can be charged under the Wiretap Act, the SCA fades into insignificance. To give effect to the SCA, it is necessary to define a class of acts that trigger the SCA but that do not trigger the Wiretap Act.

As analyzed in *Smith*, 155 F.3d at 1055-56, *Konop*, 302 F.3d at 877-78 and *Councilman*, 418 F.3d 72-76, the root problem is definitional. Various approaches to the problem of definitions are described in the Summary of Argument, *supra*.

¹¹ Numerous differences between the two Acts are set forth at length in the dissent to the withdrawn *Councilman*, 373 F.3d 204, 207-209 and 218-219. See also *Smith* at 155 F.3d at 1056 and 1059.

C. The *Konop* “Judicial Definition of ‘Intercept’,” Implicitly Approved by Congress, Stands Independent of Its Derivation From a Superseded Statute That Contained the Phrase “In Electronic Storage.”

In *Konop*, supra, at 302 F.3d at 878, the Court held:

“Congress, therefore, accepted and implicitly approved the judicial definition of ‘intercept’ as acquisition contemporaneous with transmission.

“We therefore hold that for a website such as *Konop*'s to be ‘intercepted’ in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage.” (Footnote omitted.)

Two definitions stand next to each other, one stating “the judicial definition of ‘intercept’ as acquisition contemporaneous with transmission” and the other stating that ‘intercepting’ a website requires acquisition during transmission, not while it is in electronic storage. The two definitions coincide for a “website” where “transmission” and “storage” are separated in time. The two definitions also coincide when applied to “messages remaining on an ISP’s server after delivery,” the situation addressed in *Theofel* (359 F.3d at 1075). The two definitions clash, however, when applied to email that is being processed, such as email here, where

“transmission” and “storage” occur together during a single process.¹²

As set forth, supra, plaintiffs’ expert Matthew Curtin opined that “email messages were copied and forwarded to an interloper's email mailbox while the messages were *in transit*.” (ER 447:28-44:1, emphasis added.) MPAA’s expert, Ellis Horowitz, on the other hand, emphasized the word “*storage*,” e.g., at 1923:23-24. At 1928:2-11, Prof. Horowitz notes that “While ... Matthew Curtin and I may characterize certain facts differently, it appears we agree on the underlying facts. ... we agree that, however characterized, the Merak mail server software copies the incoming and outgoing messages while those messages are on the server, in server memory.”

Plaintiffs submit that, during Anderson’s acquisition of its contents, an

¹² In *Smith* at 155 F.3d at 1056, this Court stated: “Congress seems to have defied the laws of semantics and managed to make the voicemail here at issue simultaneously subject to both” the Wiretap Act and the SCA despite their being “mutually exclusive statutes (with mutually exclusive remedial schemes).” The resolution was that a violation of the SCA might be a “lesser included offense” of a violation of the Wiretap Act. The different classes of acts that are respectively violative of the Wiretap Act and the SCA “are not...temporally different...rather the terms are conceptually or qualitatively different.” See also 155 F.3d at 1059 (“Third, our reading of the Acts explains their contrasting penalty schemes.”)

In *Pharmatrak*, supra, at 329 F.3d 21-22, the court quoted from the District Court decision in *Councilman*:

“The storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems. As one court recently observed, ‘technology has, to some extent, overtaken language. Traveling the internet, electronic communications are often -- perhaps constantly -- both ‘in transit’ and ‘in storage’ simultaneously, a linguistic but not a technological paradox.’”

outgoing email was on the server “being transmitted,” not “in storage.” Cf. *Garcia v. Haskett*, 2006 U.S. Dist. LEXIS 46303, No. C 05-3754 CW (N. D. Cal. June 30, 2006) (emails accessed while permanently stored on server – no claim under the Wiretap Act).

Here, there is a conflict between the “judicial definition of ‘intercept’ as acquisition contemporaneous with transmission” and a requirement that “it must be acquired during transmission, not while it is in electronic storage.” Two phrases that are synonymous for the website in *Konop*, – namely, “in electronic storage” and “stored electronic communications”¹³ – have clashing meanings here. Regardless of whether they were in “electronic storage” while they were being copied, plaintiffs’ emails were not “stored electronic communications;” rather, they were electronic communications in the process of being transmitted.

Plaintiffs therefore submit that the second sentence in *Konop* quoted above – stating the requirement of “acquisition while not in electronic storage” – applies “for a website such as Konop’s” but not necessarily to other forms of electronic communications. It is not a general principle. Rather, the “judicial definition of ‘intercept’ as acquisition contemporaneous with transmission” states the general

¹³ See, e.g., *Konop* at 302 F.3d 878-879, which states that the SCA [Stored Communications Act] was created “for the express purpose of addressing ‘access to stored...electronic communications and transactional records.’ S. Rep. No. 99-541 at 3 (emphasis added [by the court]).”

principle, the principle that should be applied to this case.

Plaintiffs suggest that the courts in *Smith* and *Konop* partially overcame the difficulties of this “complex, often convoluted area of law” through a process of construction. The product of that construction was stated provisionally (and in dictum) in *Smith* and then affirmatively applied in *Konop*, namely the “judicial definition of ‘intercept.’” The process of construction involved references to “in electronic storage,” but those references were folded into the process of construction and are now subordinated to the “judicial definition of ‘intercept.’”

Plaintiffs’ suggestion is based on *Konop*, 302 F.3d at 878 where the court, referring to *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994) (“*Steve Jackson*”), stated:

“Congress has since amended the Wiretap Act to eliminate storage from the definition of wire communication, see USA PATRIOT Act § 209, 115 Stat. at 283, such that the textual distinction relied upon by the *Steve Jackson* and *Smith* courts no longer exists. Congress, therefore, accepted and implicitly approved the judicial definition of ‘intercept’ as acquisition contemporaneous with transmission.”

The construction carried out in *Steve Jackson* was criticized in detail in the

final *Councilman* opinion at 418 F.3d 73-76.¹⁴ The author of the final *Councilman* opinion also wrote the dissent in the withdrawn *Councilman* opinion at 373 F.3d 197, 200-204. The “textual difference” (*Konop* at 302 F.3d 877) based on the phrase “in electronic storage,” that served as an original foundation for the contemporaneity requirement was a weak foundation and has ~~not~~^{now} been superseded and supplanted by a strong foundation.

D. Application of the *Konop* “Judicial Definition of ‘Intercept’” to the Facts of this Case Establishes that Anderson Violated the Wiretap Act When He Acquired Emails Through the Use of the Device He Set in Plaintiffs’ Computer System.

According to MPAA’s expert witness, Prof. Horowitz: “In my experiment, the Merak mail server sent the message to the ‘copy’ recipient 0.324 seconds, and 32 steps, after it sent the message to its intended recipient.” (ER 1927:1-2.)

In other words, the second copy was transmitted 0.324 seconds after the first copy. Which copy was transmitted first apparently depended on which receiver’s computer acknowledged readiness first. (ER 1923:23-1924:2.) In view of the time

¹⁴ “The question, then, is whether Councilman's inferential leap, based on a canon of construction, is justified. The Russello maxim -- which is simply a particular application of the classic principle *expressio unius est exclusio alterius* -- assumes that Congress acts carefully and deliberately in including terms in one part of a statute and omitting them in another. [Citation and quotation omitted.] ¶ Sometimes that is a reasonable assumption; sometimes it is not...” 418 F.3d at 74.

required for the email to travel from sender to recipient, “a matter of seconds,”¹⁵ it is likely that, at least on many occasion, both emails were in flight at the same time. This is factual and prior to any definition of “acquisition” or “delivery” or other terms which may be subject to disputatious interpretations.

The twinned transmission of a legitimate and a purloined email occurred within less than a second. Then, in normal course, the email server processed another email and another twinned transmission occurred. Then another, and another, and another. The episodes of twinned transmissions cycled over and over again, day after day, month after month, gradually accumulating thousands of acquired emails in a hoard that Anderson could cherry-pick for the benefit of MPAA.

Plaintiffs contend that Anderson’s ongoing acquisition of emails is exactly the kind of conduct that should be reached by the Wiretap Act. The only difference between his acquisitions and a telephone tap is the technology. Anderson’s Gmail account was the updated equivalent of a wiretapper’s tape recorder. See *United States v. Turk*, 526 F.2d 654, 657-58 (5th Cir. 1976).

¹⁵ As stated in *Councilman* at 418 F.3d 70: “While the journey from sender to recipient may seem rather involved, it usually takes just a few seconds, with each intermediate step taking well under a second. See, e.g., W. Houser et al., RFC 1865: EDI Meets the Internet (Jan. 1996), at <http://www.ietf.org/rfc/rfc1865.txt> (‘For a modest amount of data with a dedicated connection, a message transmission would occur in a matter of seconds’).”

The nature of Anderson’s “configuration” of plaintiffs’ email server resulted in two transmissions that were closely coupled in time. The closely-coupled transmissions fit the dictionary definition of “contemporaneous,” namely, “existing, occurring, or originating during the same time.”¹⁶

The District Court implicitly defined “interception” as occurring entirely during the few thousandths of a second that the email was in random access memory. The definition of “interception” cannot be so confined. In *United States v Luong* 471 F3d 1107, 1109 (9th Cir. 2006), *cert. den.* 128 S Ct 532, 169 L Ed 2d 371 (2007) (“*Luong*”), the court held was faced with a jurisdictional issue that called for a wider view:

“The most reasonable interpretation of the statutory definition of interception is that an interception occurs where the tapped phone is located and where law enforcement officers first overhear the call. We join at least three of our sister circuits in so holding.”

Following *Luong*, the most reasonable interpretation of the statutory definition of interception of an electronic communication, as applied to this case, is that an interception was occurring both at the time that the purloined copy was being made, while it was being delivered via the Internet to Anderson’s Gmail

¹⁶ Merriam-Webster Online Dictionary at <http://mw1.merriam-webster.com/dictionary/contemporaneous>.

account and throughout that period. This activity was occurring at the same time as – “contemporaneous” with – the transmission and delivery of the email to the intended recipient. Accordingly, the “contemporaneity requirement” was satisfied and Anderson’s acquisitions were interceptions as a matter of law.

E. The District Court’s Interpretation of *Konop* Was Erroneous.

From an analytic perspective, the District Court erroneously concluded that *Konop* defined a universal criterion. The District Court erroneously stated a definition of “intercept” in terms of the phrase of “not in electronic storage” and made that phrase into a principle of construction. It was error to begin by defining what is “in electronic storage” and separating that from what is “not in electronic storage.” Such definition and separation are not appropriate here because multiple processes are occurring at the same time, e.g., Internet handling of the first copy while the second copy is just getting ready to emerge from the email server.

The District Court erroneously presumed that what is “in electronic storage” and what is “not in electronic storage” can be organized through a common frame of time. The organization presumes that one can follow the life history of an email as it passes into “electronic storage” and out of “electronic storage.” In the imagination, a time line is perfectly partitioned or dissected into intervals according to a principle of exclusion. These images do not match the reality of

concurrent operations nor will they adapt easily to future developments in the technology of packetized internet transmissions.

The District Court's approach disregards the teachings of the *Smith*:

“we conclude that the government's attempt to divide the statutory provisions cleanly between those concerning in-progress wire communications (e.g., § 2515) and those concerning in-storage wire communications (e.g., § 2701) is not a viable one.”

155 F.3d at 1058.

“The terms ‘intercept’ and ‘access’ are not, as the government claims, temporally different, with the former, but not the latter, requiring contemporaneity; rather, the terms are conceptually, or qualitatively, different. The word ‘intercept’ entails *actually* acquiring the contents of a communication, whereas the word ‘access’ merely involves *being in position* to acquire the contents of a communication. In other words, ‘access[]’ is, for all intents and purposes, a lesser included offense (or tort, as the case may be) of ‘interception.’”

155 F.3d at 1059 (emphasis and editing in original).

As shown in final *Councilman* opinion at 418 F.3d 73-76 and the dissent in the withdrawn *Councilman* opinion at 373 F.3d 197, 200-204, the principle of exclusion did not come from the statutes. Rather, it came from a need to justify a legal difference that was felt to be necessary to give effect to the SCA. It was a **logical** exclusion principle introduced for a functional purpose that was said to be

an intention of Congress on the basis of a purely verbal distinction.¹⁷

As shown in *Luong*, supra, the word “interception” cannot be confined to some crucial moment. Similarly, the phrase “in electronic storage” may become a token in word games if made into a talisman for immunity from the Wiretap Act. See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) and cf. mention of the *Fraser* district court opinion in *Theofel* at 359 F.3d at 1075-1076; *In re Toys R Us, Inc., Privacy Litigation*, 2001 U.S. Dist. LEXIS 16947, MDL No. M-00-1381 MMC (N.D. Cal. 2001).

The deep error of the District Court’s Order is the disregard of modern principles of jurisprudence and the apparent return to discredited principles of “mechanical jurisprudence.” *Kovacs v. Cooper, Judge*, 336 U.S. 77, 96-97; 69 S.

¹⁷Please see the Brief of Senator Patrick Leahy (available at <http://www.eff.org/cases/us-v-councilman>) that was submitted as *amicus curiae* in the re-hearing in *Councilman* and received by the District Court here (ER 33:24-34:14.). Senator Leahy was the original sponsor of the ECPA and, at the time of the brief, the ranking Democrat on the Senate Committee on the Judiciary. The brief states at 10-11 (emphasis in original):

“the position of the DOJ, an opponent of early versions of ECPA, provides telling evidence of all parties’ shared view that the prospective acquisition of electronic communications during transmission would be intrusive and that Title III’s basic protections should apply. If communications in transmission move in and out of Title III’s protection, then law enforcement officials could access those communications under the lesser (search warrant) standard of the SCA at any one of many points of storage along the transmission path. See 18 U.S.C.A. § 2703(a) (West 2000 & Supp.. 2004). Under this theory, the procedural provisions of Title III are of virtually no relevance, for the SCA provides a ready alternative—indeed, in light of Title III’s requirement of exclusion of other investigative methods, see 18 U.S.C. § 2518(1)(c)(2000), a *mandatory* alternative to Title III’s procedures.”

Ct. 448; 93 L. Ed. 513 (1948) (J. Frankfurter concurring opinion); *Smith v. United States*, 953 F.2d 1116, 1118 (9th Cir. 1991); J. Frank, *Law and the Modern Mind* (rev. printing 1935) (denouncing “Legal Fundamentalism,” “word-magic,” and “Mechanistic Law”).

Disputes over interpretations of statutes arise from the:

“feature of the human predicament (and so of the legislative one) that we labour under two connected handicaps whenever we seek to regulate, unambiguously and in advance, some sphere of conduct by means of general standards to be used, without further official direction on particular occasions. The first handicap is our relative ignorance of fact; the second is our relative indeterminacy of aim. If the world in which we live were characterized only by a finite number of features, and these together with all the modes in which they could combine were known to us, then provision could be made in advance for every possibility. ... This would be a world fit for ‘mechanical’ jurisprudence. ... Plainly this is not our world.”

“In fact, all systems, in different ways, compromise between two social needs: the need for certain rules which can, over great areas of conduct, safely be applied by private individuals to themselves without fresh official guidance or weighing up of social issues, and the need to leave open, for later settlement by an informed, official choice, issues which can only be properly appreciated and settled when they arise in a concrete case.”

H. L. A. Hart, *The Concept of Law* (1975 reprint) at 125 and 127.

In our legal system, definition is carried out in the style of the logic of Aristotle where “a definition ... first pointed to an essence –perhaps by naming it– and that we then describe [] with the help of the defining formula.” K. Popper, *The Open Society and Its Enemies* (1950) at 210.

“And he [Aristotle] taught that by thus describing the essence to which the term points which is to be defined, we determine or explain the *meaning* of the term also. Accordingly, the definition may at one time answer two very closely related questions. The one is ‘What is it?’ ... The other is ‘What does it mean?’ ... *both terms are raised by the term that stands, in the definition, on the left side and answered by the defining formula which stands on the right side.* This fact characterizes the essentialist view, from which the scientific method of definition radically differs.”

(*Id.*, at 210-211, emphases in original, footnote omitted.)

“In modern science, only nominalist definitions occur, that is to say, shorthand symbols or labels are introduced in order to cut a long story short. And we can see at once from this that definitions do *not* play any very important part in science.”

(*Id.*, at 211, emphasis in original, footnote omitted.)

In footnote 38 to this text, Popper contrasted the scientific definition with the Aristotlean or essentialist definition: “in other words, whether it replaces a long story by a short one, or a short story by a long one.”

This principle applies here, where, presented with the same “long story” in the form of computer operations, the two retained experts came up with different short stories. Plaintiffs’ expert, Matthew Curtin, described the operations in terms of ongoing processes that sometimes occurred in sequential order and sometimes overlapped in time, and in which the acquisition of an email by Anderson occurred while the message was “in transit.” Defendant’s expert, Ellis Horowitz, described the operations in terms of steps, states and conditions of devices, leading to the conclusion of “storage.”

For one following the technical approach, the “right” expert’s description becomes a principle of law.

Plaintiffs suggest that the technical approach was the wrong approach. Plaintiffs submit that the practical approach suggested herein was the right approach. The practical approach turns a short story into a long one, by traditional legal methodology illustrated in the preceding points of this Argument. That methodology takes the phrase “acquisition contemporaneous with transmission,” sets forth the relevant factual details of the particular case, organizes the details with respect to the phrase, and shows how the details fit the meaning that has been packed into the phrase by prior opinions of the courts, with awareness of possible consequences involving other functions of the phrase, e.g., functions of national security protections and judicial regulation of law enforcement.

Plaintiffs submit that the practical approach works here and that it furthers the work of *Smith* and *Konop*.

Justice Holmes famously wrote:

"A word is not a crystal, transparent and unchanged, it is the skin of a living thought and may vary greatly in color and content according to the circumstances and the time in which it is used."

Towne v. Eisner, 245 U.S. 418, 425, 62 L. Ed. 372, 38 S. Ct. 158 (1918).

This principle was one among many that this Court quoted in support of the conclusion that "the masters of the American legal tradition have warned us not to become strict literalists in construing the language of statutes." (*Ip v. United States*, 205 F.3d 1168, 1174-75 (9th Cir. 2000).)

"Indeed, proper statutory construction, in the dominant modern view, requires recognition and implementation of the underlying legislative intention or purpose, and the court, the theory holds, must accommodate the societal claims and demands reflected in that inquiry." *Id.*, at 1175.

The principles stated by the "masters of the American legal tradition" cited and quoted in *Ip* further confirm that a technical approach cannot accommodate societal claims and demands. For those reasons and for the reasons hereinabove set forth, plaintiffs submit that the Order of the District Court should be reversed

and that the action should be remanded to the District Court to re-consider plaintiffs' Motion using the "judicial definition of 'intercept' as acquisition contemporaneous with transmission."

II. The ECPA Does Not Preempt California's Invasion of Privacy Act.

Plaintiffs' Second Claim for Relief seeks statutory damages and/or other relief under California's Invasion of Privacy Act, Cal. Penal Code §§ 630-638, because, in violation of Cal. Penal Code § 631, MPAA willfully, intentionally and without the consent of plaintiffs, or any party to the communications, and in an unauthorized manner, obtained, read and learned or attempted to read and learn, the contents and meaning of plaintiffs' electronic communications while they were in transit in or through California. (ER 109:25-111:2, esp. 110:8-13.)

The terms of definition in § 631 are decidedly different from those in the federal Act and the reach of the State Act is broader than that of the federal Act, as held by State courts. *Flanagan v. Flanagan*, 27 Cal. 4th 766, 117 Cal. Rptr. 2d 574 (2002); *Ribas v. Clark*, 38 Cal. 3d 355, 212 Cal. Rptr. 143 (1985). In *Ribas*, the court rejected the theory that only an "in-transit" message could be intercepted. Rather, non-consensual acquisition was wrongful if occurring while a message is "received at any place with this state." *Ribas*, 38 Cal.3d at 358-359.

Here, the District Court held that plaintiffs' "parallel state wiretap claim" had been preempted by the ECPA which includes 18 U.S.C. § 2518(10)(c):

"The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications." (ER 9:17-22.)

The District Court further held that "Plaintiffs' state wiretap claim is preempted by 'field preemption'," based on an inferred Congressional intent to "leave no room" for supplementary state regulation. (ER 9:17-10:9.)

The District Court was in error. Section 2518(10)(c) is stated within the context of the subject of 18 U.S.C. § 2518, namely "Procedure for interception of wire, oral, or electronic communications." It is directed at limiting remedies and sanctions for violations of such procedures by law enforcement. It does not preempt civil actions between private parties under state law.

Congressional intent to permit separate state laws is shown by the 1998 Communications Decency Act, where 47 USCS § 230(e)(4) provides:

"No effect on communications privacy law. Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, *or any similar State law.*" (Emphasis added.)

In *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 105; 45 Cal. Rptr.

3d 730 (2006), the California Supreme Court held:

“In *People v. Conklin* (1974) 12 Cal.3d 259, 270-273 [114 Cal. Rptr. 241, 522 P.2d 1049], this court specifically addressed the question whether the provisions of title III of the federal Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§ 2510-2520, hereafter title III)--relating to the wiretapping or recording of telephone conversations--preempted the application of the more stringent provisions embodied in California's invasion-of-privacy law. Reviewing the legislative history of title III, the court in *Conklin* determined that ‘Congress intended that the states be allowed to enact more restrictive laws designed to protect the right of privacy’ (12 Cal.3d at p. 271), pointing out that a legislative committee report prepared in conjunction with the consideration of title III specifically observed that ‘[t]he proposed provision envisions that States would be free to adopt *more restrictive* legislation, or no legislation at all, but not less restrictive legislation.’” (12 Cal.3d at p. 272.) Accordingly, the court in *Conklin* rejected the preemption claim.”

Finding no reason to change the prior determination, the *Kearney* court cited “numerous sister-state and federal decisions that have reached the same conclusion as *Conklin* with regard to the preemption issue.” *Id.*, at 39 Cal.4th 106.

There is one issue on which courts have issued rulings that have appearances suggesting preemption. When evidence is obtained in violation of state law but within the requirements of federal law, that evidence will be admitted in federal

court regardless of whether it is admissible in state court. As the court stated in *United States v. Little*, 753 F.2d 1420, 1434 (9th Cir. 1984):

“In this circuit, the rule regarding admissibility of evidence in a federal prosecution is clear and simple. Evidence obtained in violation of neither the Constitution nor federal law is admissible in federal court proceedings *without regard to state law.*”

(Emphasis in original.)

See also *United States v. Hall*, 543 F.2d 1229 (9th Circuit 1976); *United States v. Smith*, 726 F.2d 852, 859 (1st Cir. 1984) (saving state police wiretap statute and rejecting preemption argument); *Ideal Aerosmith, Inc. v. Acutronic United States, Inc.*, 2008 U.S. Dist. LEXIS 33463, No. 07-1029 (W. D. Pa., April 23, 2008) (rejecting parallel argument of express, field and conflict preemption of state law by the SCA); *cf. Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116 (C.D. Cal. 2006), affirmed in part and reversed in part by, remanded by *Quon v. Arch Wireless Operating Co.*, 2008 U.S. App. LEXIS 12766 (9th Cir. Cal., June 18, 2008).

Ideal Aerosmith included the following legislative history pertinent to this case, showing that the 18 U.S.C. § 2518(10)(c) was intended to apply to the evidence exclusion issue:

“As both parties have recognized, the Senate Report on the bill does not address the language of 2708, but does discuss identical language in section 2518 of the Wiretap Act, explaining that “[t]he purpose of this provision is to underscore that, as a result of discussions with the Justice Department, the Electronic Communications Privacy Act does not apply the statutory exclusionary rule contained in title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the interception of electronic communications.” S. Rep. 99-541, at 23.”

For the foregoing reasons, the Order of the District Court finding preemption should be reversed and the case should be remanded for trial on plaintiffs’ claim.

III. The District Court Erroneously Dismissed Plaintiffs’ Trade Secrets Claim.

A. Procedural Context and Standard of Review

In their Third Claim for Relief, plaintiffs seek damages and injunctive relief for MPAA’s misappropriation of trade secrets under California’s version of the Uniform Trade Secrets Act, Cal. Civil Code §§ 3426.1 *et. seq.*¹⁸ (ER 111:3-12:18.)

The District Court dismissed the Claim, relying on *Imax Corp. v. Cinema Technologies, Inc.*, 152 F.3d 1161 (9th Cir. 1998) (hereinafter “*Imax*”):

¹⁸ A plaintiff need only show that “a defendant has been unjustly enriched by the improper appropriation, use or disclosure of a ‘trade secret.’” *MAI Systems Corp. v Peak Computer, Inc.*, 991 F 2d 511, 520 (9th Cir 1993)

“Plaintiffs have failed to identify exactly what the trade secret is and apparently expect the Court to determine how the documents delivered to the MPAA constitute a trade secret. Anderson’s one time deliverance of 34 documents to the MPAA does not in and of itself constitute a trade secret violation. Plaintiffs claim that said documentation ‘as a whole’ derives value. The *Imax* plaintiffs also tried to refer to range of documents when asked to identify their trade secrets, to no avail. Plaintiffs in this case have not identified with any measure of particularity what trade secrets the documents given to MPAA contain. As such they have failed to meet their burden.” (ER 11:24-12:5.)

Plaintiffs submit that the District Court was in error on the facts, and the law and on the application of law to fact. Accordingly, the Order of the District Court should be reversed and the claim remanded for trial. *Chevron USA, Inc. v Cayetano*, 224 F3d 1030, 1039-1040 (9th Cir. 2000) *cert den* 532 US 942, 121 S Ct 1403, 149 L Ed 2d 346 (2001).

B. The Anderson Documents Were Sufficiently Identified.

In part C., *infra*, plaintiffs argue that the Anderson Documents qualify under the statutory definition as trade secrets. Here, we focus on what the District Court held was a failure of specification as the grounds for dismissing the claim.

The 34 pages of the Anderson Documents (ER 1166-1199) are specific in

and of themselves. As noted supra, 28 pages are made up of materials taken directly or indirectly from plaintiffs' computer system and the other pages (ER 1174, 1190, 1195-1198) are apparently generated by Anderson. At the lowest level, most everything taken from plaintiffs' computers is digitalized and therefore mathematically specific, e.g., emails, Excel files holding the cashflow statements, .txt files, orders sent by facsimile and screenshots that represent digital information being read to a computer screen.

Plaintiffs also submit that the District Court misread *Imax*. Background comes from *Advanced Modular Sputtering, Inc. v. Superior Court* 132 Cal App 4th 826, 833, 33 Cal Rptr 3d 901 (2005) (hereinafter "AMS"), where the court construed "the mandate, imposed by [California Code of Civil Procedure] section 2019.210, that trade secrets be identified with reasonable particularity before discovery commences."

Under *AMS*, the purpose of section 2019.210 is as follows:

"First, it promotes well-investigated claims and dissuades the filing of meritless trade secret complaints. Second, it prevents plaintiffs from using the discovery process as a means to obtain the defendant's trade secrets. Third, the rule assists the court in framing the appropriate scope of discovery and in determining whether plaintiff's discovery requests fall within that scope. Fourth, it enables defendants to form complete and well-reasoned defenses..." *Id.*

The *AMS* court reversed “the discovery referee and the trial court[, which] have taken a rather stingy view of the trade secret designations, harkening back to the days of strict code pleading.” 132 Cal.App.4th at 835. “The law is flexible enough for the referee or the trial court to achieve a just result depending on the facts, law, and equities of the situation.” *Ibid.* Citing *Locke v. Davey*, 540 U.S. 712, 718, 158 L. Ed. 2d 1, 124 S. Ct. 130 (2004), the court relied on the principle that “the law is purposely vague in some areas so that there is ‘play in the joints.’”

None of the purposes set forth in *AMS* is served by an overly strict application of the identification requirement in this case. Not knowing with confidence what information had been stolen and sold to MPAA, plaintiffs had to file and pursue a claim in order to investigate its merits. There were no trade secrets of defendant that were at issue. There were no discovery disputes that turned on identification. Defendant MPAA’s Answer (ER 118-128) did not mention lack of identification.

In the light of flexibility and purposeful vagueness in the law, a plaintiff who has been subjected to espionage, such as plaintiffs in this case, should not be deterred from filing a trade secrets claim because of an inability to specify with sharp particularity the trade secrets that have been misappropriated.

Imax, *supra*, is consistent with the foregoing principles. Plaintiff’s problem

in *Imax* was that it publicly disclosed its technology in its patents (which had expired prior to the operative events) and plaintiff had to identify something additional to bring a trade secrets action, which it could not do. Plaintiff did not “describe the subject matter of the trade secret with *sufficient particularity* to separate it from matters of general knowledge in the trade or of special knowledge of those persons . . . skilled in the trade,” quoting from and adding emphasis to *Universal Analytics v. MacNeal-Schwendler Corp.*, 707 F. Supp. 1170, 1177 (C.D. Cal. 1989), *aff’d*, 914 F.2d 1256 (9th Cir. 1990). *Imax* at 152 F.3d at 1164 -65.

The *Imax* court distinguished *Forro Precision, Inc. v. Intern. Business Machines*, 673 F.2d 1045, 1057 (9th Cir. 1982), where the circumstances were different because there had been no public disclosures prior to defendant’s use of the information. 152 F.3d at 1166. “We found IBM's identification of its trade secret sufficient because it clearly referred to trade secret material, i.e., engineering drawings and blueprints.” *Id.*, at 1167. Plaintiffs contend that this case is closer to *Ferro Precision* than to *Imax*. For this reason, the District Court’s Order should be reversed and the case should be remanded for trial.

C. The Anderson Documents Qualify As Trade Secrets.

Cal. Civil Code § 3426.1(d) provides the pertinent definition:

“ ‘Trade secret’ means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
(1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

“ Thus, the definition consists of three elements: (a) information (b) which is valuable because unknown to others and (c) which the owner has attempted to keep secret.”

Abba Rubber Co. v. Seaquist, 235 Cal. App. 3d 1, 18, 235 Cal. App. 3d 1 (1991)

“ [U]nder California law, information can be a trade secret even though it is readily ascertainable, so long as it has not yet been ascertained by others in the industry.” (*Id.*, at 21.)

“[T]hat which constitutes a trade secret must be determined from the facts of each case.” *Knudsen Corp. v. Ever-Fresh Foods, Inc.*, 336 F. Supp. 241, 244 (C.D. Cal. 1971).

There is clearly a genuine issue of material fact as to element (c), secrecy .

Rob Anderson had to use personal knowledge of plaintiffs, their system and their old passwords to guess a password that would give him unauthorized access to plaintiffs' computer system. There had not been a previous known break-in to plaintiffs' email system and plaintiffs used standard security practices. (ER 1005:13-18.)

As to element (b) MPAA contends that the Anderson documents had no value because plaintiffs did not show value in the marketplace. Neither the law nor the facts supports MPAA's contention; the weight is to the contrary.

In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 923 F. Supp. 1231, 1253 (N.D. 2005), the court rejected defendant's argument that "to constitute a trade secret, information must give its owner a *competitive advantage*." (Emphasis in original.) See also *Vermont Microsystems v. Autodesk, Inc.*, 88 F.3d 142, 149-150 (2d Cir. 1996) (computer algorithm had value because it saved development time); *Mid-Michigan Computer Systems, Inc. v. Marc Glassman, Inc.*, 415 F.3d 505, 510 (6th Cir., 2005).

Although no authorities address the issue directly, several support plaintiffs' contentions that the information stolen by Anderson and sold to MPAA qualifies for trade secret status, *Mixing Equipment Co. v. Philadelphia Gear, Inc.*, 312 F. Supp. 1269, 1274 (E.D. Pa. 1974) *modified*, 436 F.2d 1308 (3d Cir. 1971) (trade secrets included "confidential data concerning plaintiff's operating and pricing

policies” and research results in the “form of charts, graphs, tables and the like for [plaintiff’s] day-to-day use”); *Black, Sivalls & Bryson, Inc. v. Keystone Steel Fabrication, Inc.*, 584 F.2d 946, 952 (10th Cir. 1978); *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 2007 U.S. Dist. LEXIS 15216, (D.N.J. 2002) at *36 (“financial information, customer data, merchandise information, and vendor information”); *Apollo Technologies Corp. v. Centrosphere Indus. Corp.*, 805 F. Supp. 1157, 1204 (D.N.J. 1992) (“information on pricing, discounts and other relevant customer data”), in addition to *MAI Systems*, supra.

See also *Cadence Design Systems, Inc. v. Avant! Corp.*, 29 Cal. 4th 215, 127 Cal. Rptr. 2d 169 (2002) deciding a related question certified by this Court.

Plaintiffs’ confidential information fits the plain meaning of the textual definition of trade secret and is well within the intended reach of Uniform Trade Secrets Act. The Anderson documents had actual value in the amount of [REDACTED] to MPAA, a “person[] who can obtain economic value from its disclosure or use.” Cal. Civil Code § 3426.1(d). It was MPAA that set the value, after negotiations; and it was MPAA that chose to pay Anderson for the value, after having had three weeks to review the documents. According to Anderson, Garfield said that the documents were “very useful” and Garfield does not contradict Anderson.

The Anderson Documents were not simply 28 pages of documents that

happened to come together; nor did MPAA pay [REDACTED] for an accidental collection. Anderson reviewed thousands of emails and other documents and

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(ER 317:9-13.)

Review of the Anderson Documents shows that, in addition to the emails discussed above, Anderson gave Garfield [REDACTED]

[REDACTED]
[REDACTED]. The

information included current cashflow statements, showing sources of income and payees (ER 1166-1167) and technical information about internal computer addresses, application interfaces and directory listings (ER 1173, 1182, 1185-86). The value of the technical information “to an enemy, a hacker or a competitor” is declared by plaintiff Wes Parker. (ER 1005:19-1006:5.)

Garfield himself said he desired: [REDACTED]

[REDACTED]

[REDACTED].” (ER 197:10-13.) The emails between Justin Bunnell and [REDACTED] apparently satisfied this desire. The

information had unique value to MPAA, known only to MPAA. MPAA got what it desired and paid a price it found satisfactory. MPAA should not be rewarded for its pretense that the information was valueless.

For the foregoing reasons, plaintiffs submit that there were triable issues of fact involved in plaintiffs trade secrets claim and that the District Court erroneously granted plaintiffs' Motion for Summary Judgment. The District Court's Order should be reversed and the case remanded for trial.

IV. The District Court Erroneously Dismissed Plaintiffs' Claim Under California's Unfair Competition Law.

Plaintiffs sued MPAA pursuant to California's Unfair Competition Law, Business & Professions Code § 17200 *et. seq.*, which provides for injunctive and other relief against any "unlawful, unfair or fraudulent business act or practice." (ER 114:3-115:3.)

The District Court held:

"As Plaintiffs have not shown any violation of law under either the Wiretap Act or the Trade Secrets Act, their §§ 17200 claim fails as well." (ER 12:8-13.)

This Circuit recognizes Unfair Competition claims that are not grounded in a specific statute. See *Imax*, *supra*, at 152 F.3d 1169-1170.

“Unlike ‘unlawfulness,’ ‘unfairness’ is an equitable concept that cannot be mechanistically determined.” *Schnall v. Hertz Corp.*, 78 Cal. App. 4th 1144, 1167, 93 Cal. Rptr. 2d 439 (2000). Accordingly, if a “pleading states a prima facie case of harm, having its genesis in an apparently unfair business practice, the defendant should be made to present its side of the story.” *Ibid.*

As shown supra in point III.C, MPAA, a dedicated enemy of plaintiffs, purchased documents that it knew had been obtained by improper means, documents that were selected to [REDACTED]
[REDACTED]
[REDACTED]. Acting in the guise of a law enforcement organization, MPAA encouraged and paid a computer hacker for his ill-gotten gains. Clearly, if any law has been broken or trade secrets have been misappropriated, plaintiffs may proceed on their Unfair Competition claim. Assuming this Court has ruled that MPAA did not violate the ECPA, that the ECPA preempts California’s Invasion of Privacy Act and that trade secret protections are not available, it might still happen that a California state court would decide that MPAA’s conduct constituted an unfair business practice and that MPAA ought to be stopped from such conduct in the future.

CONCLUSION

For the foregoing reasons, plaintiffs respectfully request that this Court

reverse the Order of the District Court and remand the case to the District Court for further consideration of plaintiffs' Motion for partial Summary Judgment and for trial.

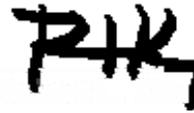
Dated: July 22, 2008

Respectfully submitted,

ROTHKEN LAW FIRM

A handwritten signature in black ink, appearing to read "Ira Rothken".

Ira P. Rothken, Esq.,

Handwritten initials "RIK" in a bold, blocky font.

Robert L. Kovsky,

Attorneys for Plaintiffs

STATEMENT OF POSSIBLY RELATED CASE.

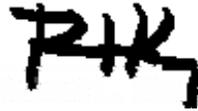
The following case, called “the copyright action” herein, now on appeal to this Court, Appellate No. 08-55940, involves some of the events and/or transactions at issue herein. (Circuit Rule 28-2.6(d)).

“Columbia Pictures Industries, Inc., Disney Enterprises, Inc., Paramount Pictures Corporation, Tristar Pictures, Inc., Twentieth Century Fox Film Corporation, Warner Bros. Entertainment Inc., Universal City Studios LLLP and Universal City Studios Productions LLLP, Plaintiffs, v. Justin Bunnell, Forrest Parker, Wes Parker, Valence Media, LLC, and Does 1-10.”

There are no other potentially related cases pending in this Court.

CERTIFICATE OF COMPLIANCE

Pursuant to Fed.R.App.Proc. 32(a)(7)(C), the undersigned certifies that the foregoing Appellants' Opening Brief complies with the type-volume limitation set forth in Rule 32(a)(7). The foregoing brief (excluding the corporate disclosure statement, request for oral argument, table of contents and index of authorities, but including footnotes) contains 13,643 words. In preparing this certificate, I relied on the word count generated by Microsoft Word.

A handwritten signature in black ink, appearing to read 'RLK', positioned above the printed name.

Robert L. Kovsky

Index Of Statutes (Local Rule 28-2.7)

I. Electronic Communications Privacy Act

A. WIRETAP ACT	<u>page</u>
18 U.S.C. § 2510. Definitions.....	4
18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited	8
18 U.S.C. § 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited	5
18 U.S.C. § 2513. Confiscation of wire, oral, or electronic communication intercepting devices	17
18 U.S.C. § 2515. Prohibition of use as evidence of intercepted wire or oral communications.....	18
18 U.S.C. § 2516. Authorization for interception of wire, oral, or electronic communications	18
18 U.S.C. § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications	23
18 U.S.C. § 2518. Procedure for interception of wire, oral, or electronic communications	25
18 U.S.C. § 2519. Reports concerning intercepted wire, oral, or electronic communications	33
18 U.S.C. § 2520. Recovery of civil damages authorized.....	35
18 U.S.C. § 2521. Injunction against illegal interception.....	37
18 U.S.C. § 2522. Enforcement of the Communications Assistance for Law Enforcement Act.....	38

B. STORED COMMUNICATIONS ACT	<u>page</u>
18 U.S.C. § 2701. Unlawful access to stored communications.....	39
18 U.S.C. § 2702. Voluntary disclosure of customer communications or records.....	40
18 U.S.C. § 2703. Required disclosure of customer communications or records.....	43
18 U.S.C. § 2704. Backup preservation.....	46
18 U.S.C. § 2705. Delayed notice	49
18 U.S.C. § 2706. Cost reimbursement	51
18 U.S.C. § 2707. Civil action.....	52
18 U.S.C. § 2708. Exclusivity of remedies	53
18 U.S.C. § 2709. Counterintelligence access to telephone toll and transactional records	54
18 U.S.C. § 2710. Wrongful disclosure of video tape rental or sale records.....	56
18 U.S.C. § 2711. Definitions for chapter	59
18 U.S.C. § 2712. Civil actions against the United States	59

WIRETAP ACT

18 U.S.C. § 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;

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

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

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

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

investigative or law enforcement officer in the ordinary course of his duties;

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

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

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

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

(9) “Judge of competent jurisdiction” means--

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

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

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

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

(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does

not include--

(A) any wire or oral communication;

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

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

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

(13) “user” means any person or entity who--

(A) uses an electronic communication service; and

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

(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

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

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

(A) scrambled or encrypted;

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

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

transmission;

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

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

(17) “electronic storage” means--

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

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

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

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

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

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

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

(B) information, whether or not concerning a United States person, with

respect to a foreign power or foreign territory that relates to--

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

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

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

(21) “computer trespasser”--

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

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

18 U.S.C. § 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

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a

switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against

any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(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.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter

or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(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 any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services;
or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(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.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(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 section 2511(2)(a) or 2517 of 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.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

- (i)** to a broadcasting station for purposes of retransmission to the general public; or
- (ii)** as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

[(c) Redesignated (b)]

(5)(a)(i) If the communication is--

- (A)** a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for

purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

18 U.S.C. § 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally--

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful

for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of--

(i) any electronic, mechanical, or other device knowing the content of the advertisement and knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for--

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

18 U.S.C. § 2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

18 U.S.C. § 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.

18 U.S.C. § 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of--

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 (relating to biological weapons) chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor

organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections

2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 956 (conspiracy to harm persons or property overseas), section a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents, section 1028A (relating to aggravated identity theft)) of this title or a violation of section 274, 277, or 278 of the

Immigration and Nationality Act (relating to the smuggling of aliens); or

(q) any criminal violation of section 229 (relating to chemical weapons): or sections 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism);

(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, 2, 3); or

(s) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

18 U.S.C. § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(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.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to

such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

18 U.S.C. § 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

- (a)** the identity of the person, if known, whose communications are to be intercepted;
- (b)** the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
- (c)** a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
- (d)** the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
- (e)** the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the

earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed

by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

- (1) the fact of the entry of the order or the application;
- (2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
- (3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above

information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that--

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if--

(a) in the case of an application with respect to the interception of an oral communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

18 U.S.C. § 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts--

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts--

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

18 U.S.C. § 2520. Recovery of civil damages authorized

(a) **In general.**--Except as provided in section 2511(2)(a)(ii), 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.**--(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court

shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$50 and not more than \$500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$100 and not more than \$1000.

(2) In any other action under this section, the 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--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

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

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;

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.

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

(g) Improper disclosure is violation.--Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

18 U.S.C. § 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

18 U.S.C. § 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) Enforcement by court issuing surveillance order.--If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) Enforcement upon application by Attorney General.--The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) Civil penalty.--

(1) In general.--A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to \$10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) Considerations.--In determining whether to impose a civil penalty and in determining its amount, the court shall take into account--

(A) the nature, circumstances, and extent of the violation;

(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

(C) such other matters as justice may require.

(d) Definitions.--As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

STORED COMMUNICATIONS ACT

18 U.S.C. § 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--

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

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

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

(2) in any other case--

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

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

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

- (1) by the person or entity providing a wire or electronic communications service;
- (2) by a user of that service with respect to a communication of or intended for that user; or
- (3) in section 2703, 2704 or 2518 of this title.

18 U.S.C. § 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 section 2517, 2511(2)(a), or 2703 of this title;

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

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

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

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency--

(A) if the contents--

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

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

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

[(C) Repealed. Pub.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

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

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

(1) as otherwise authorized in section 2703;

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

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

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

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); 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.

18 U.S.C. § 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held 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 remote computing service; and

(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.

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance

in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

18 U.S.C. § 2704. Backup preservation

(a) Backup preservation.--(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of--

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider--

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer challenges.--(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement--

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has

not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term “delivery” has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

18 U.S.C. § 2705. Delayed notice

(a) Delay of notification.--(1) A governmental entity acting under section 2703(b) of this title may--

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is--

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term “supervisory official” means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access.--A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2706. Cost reimbursement

(a) Payment.--Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount.--The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception.-- The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

18 U.S.C. § 2707. Civil action

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

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

- (1)** such preliminary and other equitable or declaratory relief as may be appropriate;
- (2)** damages under subsection (c); and
- (3)** a reasonable attorney's fee and other litigation costs reasonably incurred.

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

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

not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

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

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

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

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

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

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

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

18 U.S.C. § 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

18 U.S.C. § 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of certain disclosure.--

(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national

security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall

fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(f) Libraries.--A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) (“electronic communication service”) of this title.

18 U.S.C. § 2710. Wrongful disclosure of video tape rental or sale records

(a) Definitions.--For purposes of this section--

(1) the term “consumer” means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term “ordinary course of business” means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term “personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term “video tape service provider” means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video tape rental and sale records.--**(1)** A video tape service provider who knowingly discloses, to any person, personally identifiable information

concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer--

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if--

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if--

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the

claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil action.--(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages in an amount of \$2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally identifiable information.--Personally identifiable

information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, 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 of a State.

(e) Destruction of old records.--A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption.--The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

18 U.S.C. § 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;

(3) the term “court of competent jurisdiction” has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation; and

(4) the term “governmental entity” means a department or agency of the United States or any State or political subdivision thereof.

18 U.S.C. § 2712. Civil actions against the United States

(a) In general.--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United

States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

(1) actual damages, but not less than \$10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures.--(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or

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

(d) Exclusive remedy.--Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of proceedings.--(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms “related criminal case” and “related investigation” mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

Index Of Statutes (Local Rule 28-2.7)

**California's Invasion of Privacy Act
Penal Code Sections 630 et seq.**

	page
§ 630. Legislative finding and intent	3
§ 631. Wiretapping	3
§ 632. Eavesdropping on or recording confidential communications	4
§ 632.5. Cellular radio telephone interceptions; application of section	5
§ 632.6. Cordless or cellular telephones; interception or receipt of communications without consent; punishment; exceptions	6
§ 632.7. Cordless or cellular radio telephones; intentional recordation of communications without consent; punishment; exceptions	7
§ 633. Law enforcement officers; authorized use of electronic, etc., equipment	9
§ 633.1. Airport law enforcement officer telephone call; recording; admissibility of evidence; application of section	9
§ 633.5. Recording communications relating to commission of extortion, kidnapping, bribery, felony involving violence against the person, or violation of § 653m	10
§ 633.6. Domestic violence restraining order; permission to record prohibited communications by perpetrator	10
§ 634. Trespass for the purpose of committing prohibited acts; punishment	10
§ 635. Manufacture, sale and possession of eavesdropping devices;	11

punishment; recidivists; exceptions	
§ 636. Eavesdropping or recording conversation between prisoner and attorney, religious adviser, or physician; offenses; exceptions	12
§ 636.5. Public safety radio communications; prohibited interceptions; penalty	13
§ 637. Disclosure of telegraphic or telephonic message; punishment; exception	13
§ 637.1. Telegraphic or telephonic message; opening or procuring improper delivery; punishment	13
§ 637.2. Civil action by person injured; injunction	14
§ 637.3. Voice prints or other voice stress patterns; use of systems to record or examine without consent; damages	14
§ 637.4. Polygraph examination of complaining witness to sex offense as prerequisite to filing accusatory pleading; prohibition; damages	15
§ 637.5. Satellite or cable television corporations; use of electronic devices to observe, listen to, record or monitor events or conversations; use of information regarding subscribers; notice of right to privacy; civil liability; misdemeanor; punishment	15
§ 637.6. Personal information acquired to establish or implement carpooling or ridesharing programs; prohibition of disclosure; violations; penalties	18
§ 637.7. Electronic tracking device	18
§ 637.9. Mailing or reference list brokers and dealers; background information concerning customer; protection of children	19

§ 630. Legislative finding and intent

The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

The Legislature by this chapter intends to protect the right of privacy of the people of this state.

The Legislature recognizes that law enforcement agencies have a legitimate need to employ modern listening devices and techniques in the investigation of criminal conduct and the apprehension of lawbreakers. Therefore, it is not the intent of the Legislature to place greater restraints on the use of listening devices and techniques by law enforcement agencies than existed prior to the effective date of this chapter.

§ 631. Wiretapping

(a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment in the state prison, or by both a fine and imprisonment in the county jail or in the state prison. If the person has previously been convicted of a violation of this section or Section 632,

632.5, 632.6, 632.7, or 636, he or she is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the county jail not exceeding one year, or by imprisonment in the state prison, or by both a fine and imprisonment in the county jail or in the state prison.

(b) This section shall not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees or agents thereof, where the acts otherwise prohibited herein are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility, or (3) to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) Except as proof in an action or prosecution for violation of this section, no evidence obtained in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding.

(d) This section shall become operative on January 1, 1994.

§ 632. Eavesdropping on or recording confidential communications

(a) Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), or imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars (\$10,000), by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) The term “person” includes an individual, business association, partnership, corporation, limited liability company, or other legal entity, and

an individual acting or purporting to act for or on behalf of any government or subdivision thereof, whether federal, state, or local, but excludes an individual known by all parties to a confidential communication to be overhearing or recording the communication.

(c) The term “confidential communication” includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

(d) Except as proof in an action or prosecution for violation of this section, no evidence obtained as a result of eavesdropping upon or recording a confidential communication in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding.

(e) This section does not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees or agents thereof, where the acts otherwise prohibited by this section are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility, or (3) to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(f) This section does not apply to the use of hearing aids and similar devices, by persons afflicted with impaired hearing, for the purpose of overcoming the impairment to permit the hearing of sounds ordinarily audible to the human ear.

§ 632.5. Cellular radio telephone interceptions; application of section

(a) Every person who, maliciously and without the consent of all parties to the communication, intercepts, receives, or assists in intercepting or receiving a communication transmitted between cellular radio telephones or between any cellular radio telephone and a landline telephone shall be

punished by a fine not exceeding two thousand five hundred dollars (\$2,500), by imprisonment in the county jail not exceeding one year or in the state prison, or by both that fine and imprisonment. If the person has been previously convicted of a violation of this section or Section 631, 632, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars (\$10,000), by imprisonment in the county jail not exceeding one year or in the state prison, or by both that fine and imprisonment.

(b) In the following instances, this section shall not apply:

(1) To any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited are for the purpose of construction, maintenance, conduct, or operation of the services and facilities of the public utility.

(2) To the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of the public utility.

(3) To any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) As used in this section and Section 635, “cellular radio telephone” means a wireless telephone authorized by the Federal Communications Commission to operate in the frequency bandwidth reserved for cellular radio telephones.

§ 632.6. Cordless or cellular telephones; interception or receipt of communications without consent; punishment; exceptions

(a) Every person who, maliciously and without the consent of all parties to the communication, intercepts, receives, or assists in intercepting or receiving a communication transmitted between cordless telephones as defined in subdivision (c), between any cordless telephone and a landline telephone, or between a cordless telephone and a cellular telephone shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), by imprisonment in the county jail not exceeding one year, or in

the state prison, or by both that fine and imprisonment. If the person has been convicted previously of a violation of Section 631, 632, 632.5, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) This section shall not apply in any of the following instances:

(1) To any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited are for the purpose of construction, maintenance, conduct, or operation of the services and facilities of the public utility.

(2) To the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of the public utility.

(3) To any telephonic communications system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) As used in this section and in Section 635, "cordless telephone" means a two-way low power communication system consisting of two parts--a "base" unit which connects to the public switched telephone network and a handset or "remote" unit--which are connected by a radio link and authorized by the Federal Communications Commission to operate in the frequency bandwidths reserved for cordless telephones.

§ 632.7. Cordless or cellular radio telephones; intentional recordation of communications without consent; punishment; exceptions

(a) Every person who, without the consent of all parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone, shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in a county jail not exceeding one year, or in

the state prison, or by both that fine and imprisonment. If the person has been convicted previously of a violation of this section or of Section 631, 632, 632.5, 632.6, or 636, the person shall be punished by a fine not exceeding ten thousand dollars (\$10,000), by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) This section shall not apply to any of the following:

(1) Any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited are for the purpose of construction, maintenance, conduct, or operation of the services and facilities of the public utility.

(2) The use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of the public utility.

(3) Any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(c) As used in this section, each of the following terms have the following meaning:

(1) "Cellular radio telephone" means a wireless telephone authorized by the Federal Communications Commission to operate in the frequency bandwidth reserved for cellular radio telephones.

(2) "Cordless telephone" means a two-way, low power communication system consisting of two parts, a "base" unit which connects to the public switched telephone network and a handset or "remote" unit, that are connected by a radio link and authorized by the Federal Communications Commission to operate in the frequency bandwidths reserved for cordless telephones.

(3) "Communication" includes, but is not limited to, communications transmitted by voice, data, or image, including facsimile.

§ 633. Law enforcement officers; authorized use of electronic, etc., equipment

Nothing in Section 631, 632, 632.5, 632.6, or 632.7 prohibits the Attorney General, any district attorney, or any assistant, deputy, or investigator of the Attorney General or any district attorney, any officer of the California Highway Patrol, any chief of police, assistant chief of police, or police officer of a city or city and county, any sheriff, undersheriff, or deputy sheriff regularly employed and paid in that capacity by a county, police officer of the County of Los Angeles, or any person acting pursuant to the direction of one of these law enforcement officers acting within the scope of his or her authority, from overhearing or recording any communication that they could lawfully overhear or record prior to the effective date of this chapter.

Nothing in Section 631, 632, 632.5, 632.6, or 632.7 renders inadmissible any evidence obtained by the above-named persons by means of overhearing or recording any communication that they could lawfully overhear or record prior to the effective date of this chapter.

§ 633.1. Airport law enforcement officer telephone call; recording; admissibility of evidence; application of section

(a) Nothing in Section 631, 632, 632.5, 632.6, or 632.7 prohibits any person regularly employed as an airport law enforcement officer, as described in subdivision (d) of Section 830.33, acting within the scope of his or her authority, from recording any communication which is received on an incoming telephone line, for which the person initiating the call utilized a telephone number known to the public to be a means of contacting airport law enforcement officers. In order for a telephone call to be recorded under this subdivision, a series of electronic tones shall be used, placing the caller on notice that his or her telephone call is being recorded.

(b) Nothing in Section 631, 632, 632.5, 632.6, or 632.7 renders inadmissible any evidence obtained by an officer described in subdivision (a) if the evidence was received by means of recording any communication which is received on an incoming public telephone line, for which the person initiating the call utilized a telephone number known to the public to be a means of contacting airport law enforcement officers.

(c) This section shall only apply to airport law enforcement officers who are employed at an airport which maintains regularly scheduled international airport service and which maintains permanent facilities of the United States Customs Service.

§ 633.5. Recording communications relating to commission of extortion, kidnapping, bribery, felony involving violence against the person, or violation of § 653m

Nothing in Section 631, 632, 632.5, 632.6, or 632.7 prohibits one party to a confidential communication from recording the communication for the purpose of obtaining evidence reasonably believed to relate to the commission by another party to the communication of the crime of extortion, kidnapping, bribery, any felony involving violence against the person, or a violation of Section 653m. Nothing in Section 631, 632, 632.5, 632.6, or 632.7 renders any evidence so obtained inadmissible in a prosecution for extortion, kidnapping, bribery, any felony involving violence against the person, a violation of Section 653m, or any crime in connection therewith.

§ 633.6. Domestic violence restraining order; permission to record prohibited communications by perpetrator

(a) Notwithstanding the provisions of this chapter, and in accordance with federal law, upon the request of a victim of domestic violence who is seeking a domestic violence restraining order, a judge issuing the order may include a provision in the order that permits the victim to record any prohibited communication made to him or her by the perpetrator.

(b) The Judicial Council shall amend its domestic violence prevention application and order forms to incorporate the provisions of this section.

§ 634. Trespass for the purpose of committing prohibited acts; punishment

Any person who trespasses on property for the purpose of committing any act, or attempting to commit any act, in violation of Section 631, 632, 632.5, 632.6, 632.7, or 636 shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), by imprisonment in the county jail not

exceeding one year or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars (\$10,000), by imprisonment in the county jail not exceeding one year or in the state prison, or by both that fine and imprisonment.

§ 635. Manufacture, sale and possession of eavesdropping devices; punishment; recidivists; exceptions

(a) Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones or between a cellular radio telephone and a landline telephone in violation of Section 632.5, or communications between cordless telephones or between a cordless telephone and a landline telephone in violation of Section 632.6, shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section, the person shall be punished by a fine not exceeding ten thousand dollars (\$10,000), by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) This section does not apply to either of the following:

(1) An act otherwise prohibited by this section when performed by any of the following:

(A) A communication utility or an officer, employee or agent thereof for the purpose of construction, maintenance, conduct, or operation of, or otherwise incident to the use of, the services or facilities of the utility.

(B) A state, county, or municipal law enforcement agency or an agency of the federal government.

(C) A person engaged in selling devices specified in subdivision (a) for use

by, or resale to, agencies of a foreign government under terms approved by the federal government, communication utilities, state, county, or municipal law enforcement agencies, or agencies of the federal government.

(2) Possession by a subscriber to communication utility service of a device specified in subdivision (a) furnished by the utility pursuant to its tariffs.

§ 636. Eavesdropping or recording conversation between prisoner and attorney, religious adviser, or physician; offenses; exceptions

(a) Every person who, without permission from all parties to the conversation, eavesdrops on or records, by means of an electronic device, a conversation, or any portion thereof, between a person who is in the physical custody of a law enforcement officer or other public officer, or who is on the property of a law enforcement agency or other public agency, and that person's attorney, religious adviser, or licensed physician, is guilty of a felony.

(b) Every person who, intentionally and without permission from all parties to the conversation, nonelectronically eavesdrops upon a conversation, or any portion thereof, that occurs between a person who is in the physical custody of a law enforcement officer or other public officer and that person's attorney, religious adviser, or licensed physician, is guilty of a public offense. This subdivision applies to conversations that occur in a place, and under circumstances, where there exists a reasonable expectation of privacy, including a custody holding area, holding area, or anteroom. This subdivision does not apply to conversations that are inadvertently overheard or that take place in a courtroom or other room used for adjudicatory proceedings. A person who is convicted of violating this subdivision shall be punished by imprisonment in the state prison, or in the county jail for a term not to exceed one year, or by a fine not to exceed two thousand five hundred dollars (\$2,500), or by both that fine and imprisonment.

(c) This section shall not apply to any employee of a public utility engaged in the business of providing service and facilities for telephone or telegraph communications while engaged in the construction, maintenance, conduct, or operation of the service or facilities of that public utility who listens in to conversations for the limited purpose of testing or servicing equipment.

§ 636.5. Public safety radio communications; prohibited interceptions; penalty

Any person not authorized by the sender, who intercepts any public safety radio service communication, by use of a scanner or any other means, for the purpose of using that communication to assist in the commission of a criminal offense or to avoid or escape arrest, trial, conviction, or punishment or who divulges to any person he or she knows to be a suspect in the commission of any criminal offense, the existence, contents, substance, purport, effect or meaning of that communication concerning the offense with the intent that the suspect may avoid or escape from arrest, trial, conviction, or punishment is guilty of a misdemeanor.

Nothing in this section shall preclude prosecution of any person under Section 31 or 32.

As used in this section, “public safety radio service communication” means a communication authorized by the Federal Communications Commission to be transmitted by a station in the public safety radio service.

§ 637. Disclosure of telegraphic or telephonic message; punishment; exception

Every person not a party to a telegraphic or telephonic communication who willfully discloses the contents of a telegraphic or telephonic message, or any part thereof, addressed to another person, without the permission of such person, unless directed so to do by the lawful order of a court, is punishable by imprisonment in the state prison, or in the county jail not exceeding one year, or by fine not exceeding five thousand dollars (\$5,000), or by both fine and imprisonment.

§ 637.1. Telegraphic or telephonic message; opening or procuring improper delivery; punishment

Every person not connected with any telegraph or telephone office who, without the authority or consent of the person to whom the same may be directed, willfully opens any sealed envelope enclosing a telegraphic or telephonic message, addressed to another person, with the purpose of learning the contents of such message, or who fraudulently represents another person and thereby procures to be delivered to himself any

telegraphic or telephonic message addressed to such other person, with the intent to use, destroy, or detain the same from the person entitled to receive such message, is punishable as provided in Section 637.

§ 637.2. Civil action by person injured; injunction

(a) Any person who has been injured by a violation of this chapter may bring an action against the person who committed the violation for the greater of the following amounts:

(1) Five thousand dollars (\$5,000).

(2) Three times the amount of actual damages, if any, sustained by the plaintiff.

(b) Any person may, in accordance with Chapter 3 (commencing with Section 525) of Title 7 of Part 2 of the Code of Civil Procedure, bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages as provided by subdivision (a).

(c) It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.

§ 637.3. Voice prints or other voice stress patterns; use of systems to record or examine without consent; damages

(a) No person or entity in this state shall use any system which examines or records in any manner voice prints or other voice stress patterns of another person to determine the truth or falsity of statements made by such other person without his or her express written consent given in advance of the examination or recordation.

(b) This section shall not apply to any peace officer, as defined in Section 830, while he is carrying out his official duties.

(c) Any person who has been injured by a violator of this section may bring an action against the violator for his actual damages or one thousand dollars (\$1,000), whichever is greater.

§ 637.4. Polygraph examination of complaining witness to sex offense as prerequisite to filing accusatory pleading; prohibition; damages

(a) No state or local governmental agency involved in the investigation or prosecution of crimes, or any employee thereof, shall require or request any complaining witness, in a case involving the use of force, violence, duress, menace, or threat of great bodily harm in the commission of any sex offense, to submit to a polygraph examination as a prerequisite to filing an accusatory pleading.

(b) Any person who has been injured by a violator of this section may bring an action against the violator for his actual damages or one thousand dollars (\$1,000), whichever is greater.

§ 637.5. Satellite or cable television corporations; use of electronic devices to observe, listen to, record or monitor events or conversations; use of information regarding subscribers; notice of right to privacy; civil liability; misdemeanor; punishment

(a) No person who owns, controls, operates, or manages a satellite or cable television corporation, or who leases channels on a satellite or cable system shall:

(1) Use any electronic device to record, transmit, or observe any events or listen to, record, or monitor any conversations that take place inside a subscriber's residence, workplace, or place of business, without obtaining the express written consent of the subscriber. A satellite or cable television corporation may conduct electronic sweeps of subscriber households to monitor for signal quality.

(2) Provide any person with any individually identifiable information regarding any of its subscribers, including, but not limited to, the subscriber's television viewing habits, shopping choices, interests, opinions, energy uses, medical information, banking data or information, or any other personal or private information, without the subscriber's express written consent.

(b) Individual subscriber viewing responses or other individually identifiable

information derived from subscribers may be retained and used by a satellite or cable television corporation only to the extent reasonably necessary for billing purposes and internal business practices, and to monitor for unauthorized reception of services. A satellite or cable television corporation may compile, maintain, and distribute a list containing the names and addresses of its subscribers if the list contains no other individually identifiable information and if subscribers are afforded the right to elect not to be included on the list. However, a satellite or cable television corporation shall maintain adequate safeguards to ensure the physical security and confidentiality of the subscriber information.

(c) A satellite or cable television corporation shall not make individual subscriber information available to government agencies in the absence of legal compulsion, including, but not limited to, a court order or subpoena. If requests for information are made, a satellite or cable television corporation shall promptly notify the subscriber of the nature of the request and what government agency has requested the information prior to responding unless otherwise prohibited from doing so by law.

Nothing in this section shall be construed to prevent local franchising authorities from obtaining information necessary to monitor franchise compliance pursuant to franchise or license agreements. This information shall be provided so as to omit individually identifiable subscriber information whenever possible. Information obtained by local franchising authorities shall be used solely for monitoring franchise compliance and shall not be subject to the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).

(d) Any individually identifiable subscriber information gathered by a satellite or cable television corporation shall be made available for subscriber examination within 30 days of receiving a request by a subscriber to examine the information on the premises of the corporation. Upon a reasonable showing by the subscriber that the information is inaccurate, a satellite or cable television corporation shall correct the information.

(e) Upon a subscriber's application for satellite or cable television service, including, but not limited to, interactive service, a satellite or cable television corporation shall provide the applicant with a separate notice in an appropriate form explaining the subscriber's right to privacy protection

afforded by this section.

(f) As used in this section:

(1) “Cable television corporation” shall have the same meaning as that term is given by Section 216.4 of the Public Utilities Code.

(2) “Individually identifiable information” means any information identifying an individual or his or her use of any service provided by a satellite or cable system other than the mere fact that the individual is a satellite or cable television subscriber. “Individually identifiable information” shall not include anonymous, aggregate, or any other information that does not identify an individual subscriber of a video provider service.

(3) “Person” includes an individual, business association, partnership, corporation, limited liability company, or other legal entity, and an individual acting or purporting to act for or on behalf of any government, or subdivision thereof, whether federal, state, or local.

(4) “Interactive service” means any service offered by a satellite or cable television corporation involving the collection, reception, aggregation, storage, or use of electronic information transmitted from a subscriber to any other receiving point under the control of the satellite or cable television corporation, or vice versa.

(g) Nothing in this section shall be construed to limit the ability of a satellite or cable television corporation to market satellite or cable television or ancillary services to its subscribers.

(h) Any person receiving subscriber information from a satellite or cable television corporation shall be subject to the provisions of this section.

(i) Any aggrieved person may commence a civil action for damages for invasion of privacy against any satellite or cable television corporation, service provider, or person that leases a channel or channels on a satellite or cable television system that violates the provisions of this section.

(j) Any person who violates the provisions of this section is guilty of a misdemeanor punishable by a fine not exceeding three thousand dollars

(\$3,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(k) The penalties and remedies provided by subdivisions (i) and (j) are cumulative, and shall not be construed as restricting any penalty or remedy, provisional or otherwise, provided by law for the benefit of any person, and no judgment under this section shall preclude any person from obtaining additional relief based upon the same facts.

(l) The provisions of this section are intended to set forth minimum state standards for protecting the privacy of subscribers to cable television services and are not intended to preempt more restrictive local standards.

§ 637.6. Personal information acquired to establish or implement carpooling or ridesharing programs; prohibition of disclosure; violations; penalties

(a) No person who, in the course of business, acquires or has access to personal information concerning an individual, including, but not limited to, the individual's residence address, employment address, or hours of employment, for the purpose of assisting private entities in the establishment or implementation of carpooling or ridesharing programs, shall disclose that information to any other person or use that information for any other purpose without the prior written consent of the individual.

(b) As used in this section, “carpooling or ridesharing programs” include, but shall not be limited to, the formation of carpools, vanpools, buspools, the provision of transit routes, rideshare research, and the development of other demand management strategies such as variable working hours and telecommuting.

(c) Any person who violates this section is guilty of a misdemeanor, punishable by imprisonment in the county jail for not exceeding one year, or by a fine of not exceeding one thousand dollars (\$1,000), or by both that imprisonment and fine.

§ 637.7. Electronic tracking device

(a) No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.

(b) This section shall not apply when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle.

(c) This section shall not apply to the lawful use of an electronic tracking device by a law enforcement agency.

(d) As used in this section, “electronic tracking device” means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.

(e) A violation of this section is a misdemeanor.

(f) A violation of this section by a person, business, firm, company, association, partnership, or corporation licensed under Division 3 (commencing with Section 5000) of the Business and Professions Code shall constitute grounds for revocation of the license issued to that person, business, firm, company, association, partnership, or corporation, pursuant to the provisions that provide for the revocation of the license as set forth in Division 3 (commencing with Section 5000) of the Business and Professions Code.

§ 637.9. Mailing or reference list brokers and dealers; background information concerning customer; protection of children

(a) Any person who, in the course of business, provides mailing lists, computerized or telephone-based reference services, or similar products or services utilizing lists, as defined, knowingly does any of the following is guilty of a misdemeanor:

(1) Fails, prior to selling or distributing a list to a first-time buyer, to obtain the buyer's name, address, telephone number, tax identification number if the buyer is a forprofit entity, a sample of the type of material to be distributed using the list, or to make a good-faith effort to verify the nature and legitimacy of the business or organization to which the list is being sold or distributed.

(2) Knowingly provides access to personal information about children to any

person who he or she knows is registered or required to register as a sex offender.

(b) Any person who uses personal information about a child that was obtained for commercial purposes to directly contact the child or the child's parent to offer a commercial product or service to the child and who knowingly fails to comply with the parent's request to take steps to limit access to personal information about a child only to authorized persons is guilty of a misdemeanor.

(c) Any person who knowingly distributes or receives any personal information about a child with knowledge that the information will be used to abuse or physically harm the child is guilty of a misdemeanor.

(d)(1) List brokers shall, upon a written request from a parent that specifically identifies the child, provide the parent with procedures that the parent must follow in order to withdraw consent to use personal information relating to his or her child. Any list broker who fails to discontinue disclosing personal information about a child within 20 days after being so requested in writing by the child's parent, is guilty of a misdemeanor.

(2) Any person who, through the mail, markets or sells products or services directed to children, shall maintain a list of all individuals, and their addresses, who have requested in writing that the person discontinue sending any marketing or sales materials to the individual or the individual's child or children. No person who is obligated to maintain that list shall cause any marketing or sales materials, other than those that are already in the process of dissemination, to be sent to any individual's child or children, after that individual has made that written request. Any person who is subject to the provisions of this paragraph, who fails to comply with the requirements of this paragraph or who violates the provisions of this paragraph is guilty of a misdemeanor.

(e) The following shall be exempt from subdivisions (a) and (b):

(1) Any federal, state, or local government agency or law enforcement agency.

(2) The National Center for Missing and Exploited Children.

(3) Any educational institution, consortia, organization, or professional association, which shall include, but not be limited to, the California community colleges; the California State University, and each campus, branch, and function thereof; each campus, branch, and function of the University of California; the California Maritime Academy; or any independent institution of higher education accredited by an agency recognized by the federal Department of Education. For the purposes of this paragraph, “independent institution of higher education” means any nonpublic higher education institution that grants undergraduate degrees, graduate degrees, or both undergraduate and graduate degrees, is formed as a nonprofit corporation in this state, and is accredited by an agency recognized by the federal Department of Education; or any private postsecondary vocational institution registered, approved, or exempted by the Bureau of Private Postsecondary Vocational Education.

(4) Any nonprofit organization that is exempt from taxation under Section 23701d of the Revenue and Taxation Code.

(f) As used in this section:

(1) “Child” means a person who is under 16 years of age.

(2) “Parent” shall include a legal guardian.

(3) “Personal information” means any information that identifies a child and that would suffice to locate and contact the child, including, but not limited to, the name, postal or electronic mail address, telephone number, social security number, date of birth, physical description of the child, or family income.

(4) “List” may include, but is not limited to, a collection of name and address records of individuals sharing a common interest, purchase history, demographic profile, membership, or affiliation.

§ 638. Purchase, sale or procurement of telephone calling pattern record or list without consent of subscriber; penalties; use as evidence; legislative intent

(a) Any person who purchases, sells, offers to purchase or sell, or conspires to purchase or sell any telephone calling pattern record or list, without the

written consent of the subscriber, or any person who procures or obtains through fraud or deceit, or attempts to procure or obtain through fraud or deceit any telephone calling pattern record or list shall be punished by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in a county jail not exceeding one year, or by both a fine and imprisonment. If the person has previously been convicted of a violation of this section, he or she is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in a county jail not exceeding one year, or by both a fine and imprisonment.

(b) Any personal information contained in a telephone calling pattern record or list that is obtained in violation of this section shall be inadmissible as evidence in any judicial, administrative, legislative, or other proceeding except when that information is offered as proof in an action or prosecution for a violation of this section, or when otherwise authorized by law, in any criminal prosecution.

(c) For purposes of this section:

(1) "Person" includes an individual, business association, partnership, limited partnership, corporation, limited liability company, or other legal entity.

(2) "Telephone calling pattern record or list" means information retained by a telephone company that relates to the telephone number dialed by the subscriber, or other person using the subscriber's telephone with permission, or the incoming number of a call directed to the subscriber, or other data related to such calls typically contained on a subscriber telephone bill such as the time the call started and ended, the duration of the call, any charges applied, and any information described in subdivision (a) of Section 2891 of the Public Utilities Code whether the call was made from or to a telephone connected to the public switched telephone network, a cordless telephone, as defined in Section 632.6, a telephony device operating over the Internet utilizing voice over Internet protocol, a satellite telephone, or commercially available interconnected mobile phone service that provides access to the public switched telephone network via a mobile communication device employing radiowave technology to transmit calls, including cellular radiotelephone, broadband Personal Communications Services, and digital Specialized Mobile Radio.

(3) “Telephone company” means a telephone corporation as defined in Section 234 of the Public Utilities Code or any other person that provides residential or commercial telephone service to a subscriber utilizing any of the technologies or methods enumerated in paragraph (2).

(4) For purposes of this section, “purchase” and “sell” shall not include information provided to a collection agency or assignee of the debt by the telephone corporation, and used exclusively for the collection of the unpaid debt assigned by the telephone corporation, provided that the collection agency or assignee of the debt shall be liable for any disclosure of the information that is in violation of this section.

(d) An employer of, or entity contracting with, a person who violates subdivision (a) shall only be subject to prosecution pursuant to that provision if the employer or contracting entity knowingly allowed the employee or contractor to engage in conduct that violated subdivision (a).

(e) It is the intent of the Legislature to ensure that telephone companies maintain telephone calling pattern records or lists in the strictest confidence, and protect the privacy of their subscribers with all due care. While it is not the intent of the Legislature in this act to preclude the sharing of information that is currently allowed by both state and federal laws and rules governing those records, it is the Legislature's intent in this act to preclude any unauthorized purchase or sale of that information.

(f) This section shall not be construed to prevent a law enforcement or prosecutorial agency, or any officer, employee, or agent thereof from obtaining telephone records in connection with the performance of the official duties of the agency consistent with any other applicable state and federal law.

(g) Nothing in this section shall preclude prosecution under any other provision of law.

(h) The Legislature hereby finds and declares that, notwithstanding the prohibition on specific means of making available or obtaining personal calling records pursuant to this section, the disclosure of personal calling records through any other means is no less harmful to the privacy and security interests of Californians. This section is not intended to limit the scope or force of Section 2891 of the Public Utilities Code in any way.