

1 I. NEEL CHATTERJEE (SBN 173985)
 nchatterjee@orrick.com
 2 GABRIEL M. RAMSEY (SBN 209218)
 gramsey@orrick.com
 3 JULIO C. AVALOS (SBN 255350)
 javalos@orrick.com
 4 ORRICK, HERRINGTON & SUTCLIFFE LLP
 1000 Marsh Road
 5 Menlo Park, CA 94025
 Telephone: 650-614-7400
 6 Facsimile: 650-614-7401

7 Attorneys for Defendant
 MICROSOFT CORPORATION

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 SAN JOSE DIVISION

HOLOMAXX TECHNOLOGIES, a
 Pennsylvania Corporation,

 Plaintiff,

 v.

 MICROSOFT CORPORATION, a Delaware
 Corporation,

 Defendant.

Case No. C 10-04924-JF

**DEFENDANT MICROSOFT
 CORPORATION'S NOTICE OF
 MOTION AND MOTION TO
 DISMISS COMPLAINT PURSUANT
 TO FED. R. CIV. P. 12(b)(6)**

Date: February 25, 2011
 Time: 9:00 a.m.
 Judge: Honorable Jeremy Fogel
 Courtroom: Courtroom 3, 5th Floor

TABLE OF CONTENTS

	PAGE
I. INTRODUCTION	1
II. FACTUAL BACKGROUND	2
III. ARGUMENT	4
A. Motion to Dismiss Standard.....	5
B. The Communications Decency Act Bars Holomaxx’s Third Through Sixth And Ninth Claims	6
1. Accepting Holomaxx’s Allegations As True, Microsoft Satisfies All Requirements Necessary For CDA Immunity	7
2. Because Microsoft Is Entitled To Immunity Under The CDA, The Court Must Dismiss Holomaxx’s Claims Three Through Six And Nine	9
3. Holomaxx’s Disagreement With Microsoft’s Filtering Methodology Is Legally Irrelevant And Does Not Save Holomaxx’s Claims	9
C. Each Of Holomaxx’s Claims Is Insufficiently Pled And Should Be Dismissed For Failure To State A Claim	11
1. Holomaxx Fails To State A Claim For Violation Of The Wiretap Act.....	11
2. Independent Of The CDA, Holomaxx Fails To State A Claim For Violation Of California Penal Code §§ 630, et seq.....	15
3. Holomaxx Fails To State A Claim For Violation Of The Stored Communications Act.....	15
4. Independent Of The CDA, Holomaxx Fails To State A Claim for Violation Of The Computer Fraud And Abuse Act.....	17
5. Independent Of The CDA, Holomaxx Fails To State A Claim For Intentional Interference With Contract And Intentional Interference With Prospective Business Advantage.....	18
6. Independent Of The CDA, Holomaxx Fails To State A Claim For Unfair Competition	22
7. Holomaxx Fails To State A Claim For Defamation And False Light	23
IV. CONCLUSION	25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 **TABLE OF AUTHORITIES**

2 **FEDERAL CASES**

	Page(s)
3	
4 <i>Accuimage Diagnostics Corp. v. Terarecon, Inc.</i> ,	
5 260 F. Supp. 2d 941 (N.D. Cal. 2003)	21
6 <i>Ashcroft v. Iqbal</i> ,	
7 129 S. Ct. 1937 (2009)	6
8 <i>Bell Atl. Corp. v. Twombly</i> ,	
9 550 U.S. 544 (2007)	5
10 <i>Black v. Google, Inc.</i> ,	
11 2010 U.S. Dist. LEXIS 82905 (N.D. Cal. Aug. 13, 2010)	5
12 <i>Bohach v. City of Reno</i> ,	
13 932 F. Supp. 1232 (D. Nev. 1996)	16
14 <i>Bradley v. Google</i> ,	
15 No. C06-05289-WHA, 2006 U.S. Dist. LEXIS 94455 (N.D. Cal. Dec. 22, 2006)	13
16 <i>Branch v. Tunnell</i> ,	
17 14 F.3d 449 (9th Cir. 1994)	13
18 <i>Bunnell v. Motion Picture Ass'n of Am.</i> ,	
19 567 F. Supp. 2d 1148 (C.D. Cal. 2007)	15
20 <i>Cardinal Health 414, Inc. v. Adams</i> ,	
21 582 F. Supp. 2d 967 (M.D. Tenn. 2008)	13
22 <i>Cont'l Grp., Inc. v. Kw Prop. Mgmt, LLC</i> ,	
23 622 F. Supp. 2d 1357 (S.D. Fla. 2009)	17
24 <i>Crowley v. Cybersource Corp.</i> ,	
25 166 F. Supp. 2d 1263 (N.D. Cal. 2001)	16
26 <i>Dodds v. Am. Broadcasting Co.</i> ,	
27 145 F.3d 1053 (9th Cir. 1998)	24
28 <i>Dworkin v. Hustler Magazine</i> ,	
867 F.2d 1188 (9th Cir. 1989)	25
<i>Ebay, Inc. v. Bidder's Edge</i> ,	
100 F. Supp. 2d 1058 (N.D. Cal. 2002)	17
<i>e360Insight, LLC v. Comcast Corporation</i> ,	
546 F. Supp. 2d 605 (N.D. Ill. 2008)	<i>passim</i>
<i>Fraser v. Nationwide Mut. Ins. Co.</i> ,	
352 F.3d 107 (3d Cir. 2003)	16

TABLE OF AUTHORITIES
(Cont.)

FEDERAL CASES

		Page(s)
1		
2		
3		
4		
5	<i>Galbraith v. County of Santa Clara,</i> 307 F.3d 1119 (9th Cir. 2002).....	13
6		
7	<i>Goddard v. Google, Inc.,</i> 640 F. Supp. 2d 1193 (N.D. Cal. 2009)	59
8	<i>Gordon v. Virtumundo, Inc.,</i> 575 F.3d 1040 (9th Cir. 2009).....	3, 24
9		
10	<i>Hotmail Corp. v. Van\$ Money Pie Inc.,</i> 47 U.S.P.Q. 2d 1020 (N.D. Cal. 1998)	18
11	<i>Howard v. America Online, Inc.,</i> 208 F.3d 741 (9th Cir. 2000).....	12
12		
13	<i>Ideal Aerosmith, Inc. v. Acutronic USA, Inc.,</i> 2007 U.S. Dist. LEXIS 91644 (W.D. Pa. Dec. 13, 2007).....	12
14	<i>Knievel v. ESPN,</i> 393 F.3d 1068 (9th Cir. 2005).....	23, 24
15		
16	<i>Konop v. Hawaiian Airlines, Inc.,</i> 302 F.3d 868 (9th Cir. 2002).....	12
17	<i>Lewis-Burke Assocs. LLC v. Widder,</i> No. 09-302-JMF, 2010 U.S. Dist. LEXIS 76180 (D.D.C. July 28, 2010).....	18
18		
19	<i>Maxner Co. Ltd., v. Costco Wholesale Corp.,</i> No. 03-35865, 2004 U.S. App. LEXIS 14298 (9th Cir. July 12, 2004).....	20
20	<i>Mendiondo v. Centinela Hosp. Med. Ctr.,</i> 521 F.3d 1097 (9th Cir. 2008).....	5
21		
22	<i>Milkovich v. Lorain Journal Co.,</i> 497 U.S. 1 (1990).....	24
23	<i>Optinrealbig.com, LLC v. Ironport Systems, Inc.,</i> 323 F. Supp. 2d 1037 (N.D. Cal. 2004)	3, 7, 8
24		
25	<i>Price v. Stossel,</i> 620 F.3d 992 (9th Cir. 2010).....	23
26	<i>Secureinfo Corp. v. Telos Corporation,</i> 387 F. Supp. 2d 593 (E.D. Va. 2005).....	18
27		
28	<i>Solano v. Playgirl, Inc.,</i> 292 F.3d 1078 (9th Cir. 2002).....	23

TABLE OF AUTHORITIES
(Cont.)

FEDERAL CASES

		Page(s)
1		
2		
3		
4		
5	<i>Sprewell v. Golden State Warriors,</i>	
6	266 F.3d 979 (9th Cir. 2001).....	6
7	<i>Stac Elecs. Sec. Litig.,</i>	
8	89 F.3d 1399 (9th Cir. 1996).....	14
9	<i>State-Wide Photocopy Corp. v. Tokai Financial Services, Inc.,</i>	
10	909 F. Supp. 137 (S.D.N.Y. 1995).....	16
11	<i>In re Toys R Us, Inc., Privacy Litig.,</i>	
12	No. C00-2746-MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001).....	17
13	<i>Winter v. Bassett,</i>	
14	2003 U.S. Dist. LEXIS 26904 (M.D.N.C. Aug. 22, 2003).....	8
15	<i>Young v. Facebook, Inc.,</i>	
16	2010 U.S. Dist. LEXIS 116530 (N.D. Cal. Oct. 25, 2010).....	5
17	<i>Zango, Inc. v. Kaspersky,</i>	
18	2007 U.S. Dist. LEXIS 97332 (W.D. Wash. Aug. 28, 2007).....	9, 10
19	<i>Zango, Inc. v. Kaspersky,</i>	
20	568 F.3d 1169 (9th Cir. 2009).....	7, 8, 9, 10
21		
22		
23		
24		
25		
26		
27		
28		

STATE CASES

18	<i>Chavez v. Whirlpool Corp.,</i>	
19	93 Cal. App. 4th 363 (2001).....	22
20	<i>Della Penna v. Toyota Motor Sales, Co.,</i>	
21	11 Cal. 4th 376 (1995).....	19, 20
22	<i>Fellows v. Nat'l Enquirer, Inc.,</i>	
23	42 Cal. 3d 234 (1986).....	23
24	<i>Gilbert v. Sykes,</i>	
25	147 Cal. App. 4th 13 3d 752 (2007).....	23
26	<i>Korea Supply Co. v. Lockheed Martin Corp.,</i>	
27	29 Cal. 4th 1134 (2003).....	19
28	<i>Lazar v. Hertz Corp.,</i>	
	69 Cal. App. 4th 1494 (1999).....	22
	<i>Pacific Gas & Elec. Co. v. Bear Stearns & Co.,</i>	
	50 Cal. 3d 1118 (1990).....	19

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**TABLE OF AUTHORITIES
(Cont.)**

STATE CASES

Page(s)

Quelimane Co. v. Stewart Title Guar. Co.,
19 Cal. 4th 26 (1998) 19

Selleck v. Globe Int'l,
166 Cal. App. 3d 1123 (1985)..... 25

Westside Ctr. Assocs. v. Safeway Stores 23, Inc.,
42 Cal. App. 4th 507 (1996) 21

FEDERAL STATUTES

15 U.S.C. § 7701 3, 11

18 U.S.C. § 1030 1, 17, 18

18 U.S.C. § 2510 1, 11, 12

18 U.S.C. § 2511 12, 13, 14

18 U.S.C. § 2518 15

18 U.S.C. § 2701 1, 16

47 U.S.C. § 230 1, 5, 6, 7, 9, 11

Fed. R. Civ. P. 8(a)(2) 6

Fed. R. Civ. P. 12(b)(6) 1, 5, 6, 13, 6, 13

STATE STATUTES

Page(s)

California Bus. & Prof. Code § 17200 1, 22

California Civil Code § 43 1

California Penal Code § 630 1, 15

California Penal Code § 631 15

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**TABLE OF AUTHORITIES
(Cont.)**

MISCELLANEOUS

Page(s)

Restatement (Second) of Torts § 652E [1976]..... 23

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on February 25, 2011 at 9:00 a.m., or as soon thereafter as the matter may be heard, in the courtroom of the Honorable Jeremy Fogel, United States District Court, 280 S. First Street, San Jose, California 95113, Microsoft Corporation (“Microsoft”) will move the Court for an order dismissing the Complaint of Holomaxx Technologies Corporation pursuant to Federal Rule of Civil Procedure 12(b)(6).

Dated: December 17, 2010

GABRIEL M. RAMSEY
Orrick, Herrington & Sutcliffe LLP

/s/ Gabriel M. Ramsey
GABRIEL M. RAMSEY
Attorneys for Defendant
MICROSOFT CORPORATION

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

2 **I. INTRODUCTION**

3 This motion presents a straightforward issue. The efforts taken by an e-mail provider to
4 stop spam, as alleged here, are not actionable as a matter of law. Plaintiff Holomaxx
5 Technologies Corporation (“Holomaxx”) is a self-described “e-mail marketing service.”
6 Specifically, every day Holomaxx sends millions of bulk commercial solicitations and
7 advertisements to e-mail recipients. As a federal judge recently described a similar e-mail
8 marketing service, “[s]ome, perhaps even a majority in this country, would call it a spammer.”
9 *e360Insight, LLC v. Comcast Corporation*, 546 F. Supp. 2d 605, 606 (N.D. Ill. 2008).

10 Defendant Microsoft Corporation (“Microsoft”) provides e-mail services to Internet users,
11 such as the free Windows Live Hotmail service (“Hotmail”). Like virtually every other e-mail
12 provider (such as Yahoo!, Google, Comcast, Qwest and others), Microsoft filters e-mails that
13 arrive at its servers in order to manage network resources and prevent objectionable e-mails from
14 reaching its subscribers. According to Holomaxx’s Complaint, Microsoft blocked millions of
15 Holomaxx’s unwanted e-mails from reaching Microsoft e-mail subscribers and thereafter stated,
16 accurately, that Holomaxx had been blocked “for policy reasons” “or for spamming.”

17 Incredibly, Holomaxx argues that by protecting its customers and servers this way,
18 Microsoft has purportedly violated no fewer than nine federal and California laws, and has here
19 brought claims under: (1) 18 U.S.C. §§ 2510, *et seq.* (The Wiretap Act); (2) 18 U.S.C. §§ 2701, *et*
20 *seq.* (The Stored Communications Act); (3) 18 U.S.C. §§ 1030, *et seq.* (Computer Fraud); (4)
21 Intentional Interference with Contract; (5) Intentional Interference with Prospective Business
22 Advantage; (6) California Penal Code §§ 630, *et seq.* (Wiretapping/Eavesdropping); (7) Civil
23 Code §§ 43, *et seq.* (Defamation); (8) False Light; and (9) California Business & Professions Code
24 §§ 17200, *et seq.* (Unfair Competition).

25 Holomaxx’s claims against Microsoft are without merit. First, Claims 3-6 and 9—based
26 on Microsoft’s filtering of Holomaxx’s e-mails—are barred by the Communications Decency Act
27 of 1996 (“CDA”), 47 U.S.C. Section 230. The CDA explicitly exempts service providers such as
28 Microsoft from liability for filtering of objectionable content, including objectionable e-mail.

1 Through the CDA, Congress immunized Microsoft from precisely the sort of liability that
2 Holomaxx seeks to impose here. Indeed, one federal court recently held that claims based on e-
3 mail filtering were barred by the CDA. *See e360Insight, LLC*, 546 F. Supp. 2d at 609-610. The
4 same analysis should be adopted here. Further, even accepting Holomaxx’s allegations as true,
5 every cause of action based on Microsoft’s filtering activities (Claims 1-6 and 9) independently
6 fails to state a claim upon which relief may be granted, as Holomaxx has failed to allege legally
7 sufficient facts and puts forth theories that are unsupported in the law.¹

8 Additionally, Claims 7-8 for defamation and “false light”—based on Microsoft’s alleged
9 statement that it blocked Holomaxx’s e-mail “for policy reasons” “or for spamming”—are
10 deficient as a matter of law. Holomaxx’s Complaint itself establishes that these statements are
11 accurate, reflect Microsoft’s opinion and are otherwise non-defamatory. Holomaxx fails to plead
12 any other legally sufficient facts. Given that Congress and the courts have recognized that
13 filtering objectionable e-mail is protected and a matter of public significance, to impose liability
14 for speaking about such activities would be flatly inconsistent with the CDA and would severely
15 chill valid speech. Accordingly, like the rest of the complaint, Claims 7-8 should be dismissed.

16 **II. FACTUAL BACKGROUND**

17 Microsoft is one of the world’s largest interactive computer service providers. Compl.
18 ¶ 20. Among its many services, Microsoft provides e-mail accounts to millions of Internet users
19 and businesses. *Id.* For example, Microsoft provides the free Windows Live Hotmail service
20 (“Hotmail”), which was one of the first web-based e-mail services on the Internet, and, since its
21 launch in 1996, one of the most popular. E-mails sent to Microsoft account holders reside on
22 Microsoft’s servers; users can then access Microsoft’s servers to view or download their e-mail
23 messages. The operation of Microsoft’s online e-mail servers is similar to those operated by
24 many other major e-mail service providers.

25
26
27 ¹ Many of Holomaxx’s allegations are false. For example, contrary to Holomaxx’s unsupported
28 assertion, Microsoft does not receive any income from Return Path < inc., former Co-Defendant
in this case. That said, as it must, Microsoft accepts Holomaxx’s allegations as true for purposes
of this motion.

1 A significant percentage of e-mails sent to e-mail accountholders, including Microsoft's
2 customers, are objectionable and burdensome commercial solicitations. Such bulk, commercial
3 electronic mail is generally and commonly referred to as "spam" e-mail. *See Gordon v.*
4 *Virtumundo, Inc.*, 575 F.3d 1040, 1045 n.1 (9th Cir. 2009) ("While 'spam' in this context does
5 not have a precise definition, it is typically understood to refer broadly to unsolicited e-mail
6 messages (or 'junk' e-mail), typically commercial in nature."); noting that the term "spam" has,
7 since the early days of the Internet, referred to repetitive online activity); *e360Insight*, 546 F.
8 Supp. 2d at 607 (Internet marketing company commonly referred to as "a spammer");
9 *Optinrealbig.com, LLC v. Ironport Systems, Inc.*, 323 F. Supp. 2d 1037, 1039 (N.D. Cal. 2004)
10 ("Spam is 'unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple
11 mailing lists, individuals, or newsgroups; junk e-mail.'").

12 In 2003, Congress found that "[u]nsolicited commercial electronic mail is currently
13 estimated to account for over half of all electronic mail traffic ... and the volume continues to
14 rise". 15 U.S.C. § 7701(a)(2). Congress recognized that "[t]he growth in unsolicited commercial
15 electronic mail imposes significant monetary costs on providers of Internet access services... that
16 carry and receive such e-mail." § 7701(a)(6). In response to these problems, and like all
17 participants in this industry, Microsoft uses proprietary software to identify, filter, and block
18 objectionable e-mail messages. To maintain the stability and reliability of its network, and to
19 limit the amount of objectionable spam e-mail that reaches its users' mailboxes, Microsoft uses its
20 software, feedback from abandoned user accounts, industry evaluation and reputation scores,
21 marking of e-mail by users as "spam," and other factors to filter out messages having
22 characteristics of inappropriate commercial e-mail. Compl. ¶¶ 20-22, 34, 41, 51.

23 Holomaxx, which describes itself as an "e-mail marketing service," sends bulk
24 commercial e-mails to millions of Internet users, including Microsoft e-mail accountholders.
25 Compl. ¶¶ 13-17. Holomaxx acknowledges that, on average, it sends 10 million e-mails *per day*,
26 including an estimated 3 million e-mails to Microsoft users. *Id.* ¶ 17. Holomaxx admits that it
27 sends thousands of *unwanted* e-mails everyday: by its own calculations, it sends over *100,000* e-
28 mails to Microsoft alone *every week* which are either returned as invalid or result in a user opting-

1 out—hallmarks of bulk “spam” e-mail. *Id.* ¶ 17 (3 million e-mails to Microsoft); ¶ 19 (.5% of e-
2 mails to Microsoft are to an invalid address or result in a user opt-out). Holomaxx alleges that
3 beginning in about November 2009, Microsoft’s filtering software began blocking e-mails
4 directed at Microsoft’s e-mail accountholders because the e-mails contained “spam-like
5 characteristics” or had “IP/domain reputation problems.” *Id.* ¶¶ 31-34. Holomaxx also alleges
6 that Microsoft, as part of its filtering process, accessed information from these e-mails. *Id.* ¶ 11.

7 Holomaxx puts forth three sets of purported facts, none of which is sufficient to support
8 its claims:

9 First, Holomaxx asserts that Microsoft has systems and processes in place to filter spam e-
10 mail (based on, among other things, proprietary software, industry evaluation and reputation
11 scores, marking of e-mail by users as “spam” and other factors), that those systems and processes
12 were applied to Holomaxx’s e-mail, but that Holomaxx believes some different criteria should be
13 used because their e-mails purportedly comply with the Controlling the Assault of Non-Solicited
14 Pornography and Marketing Act of 2003 (the “CAN-SPAM Act”), 15 U.S.C. section 7701, *et seq.*
15 *Id.* ¶¶ 9-10, 18, 20-22, 31-36.

16 Second, Holomaxx asserts that, as part of this process, Microsoft allegedly accessed
17 Microsoft’s *own* e-mail servers and systems, examined the e-mails stored therein that had been
18 aimed by Holomaxx at Microsoft’s accountholders and, based on the IP addresses and other
19 criteria, Microsoft filtered and blocked those e-mails. *Id.* ¶¶ 11, 41.

20 Third, Holomaxx alleges that Microsoft told Holomaxx’s Internet hosting company that
21 Holomaxx IP addresses had been blocked by Microsoft “for policy reasons” “or for spamming.”
22 *Id.* ¶¶ 11, 42, 44-47.

23 **III. ARGUMENT**

24 Holomaxx’s Claims 1-6 and Claim 9 arise from Microsoft’s alleged filtering of
25 Holomaxx’s e-mails. On this theory, Holomaxx asserts: The Wiretap Act (Claim 1), The Stored
26 Communications Act (Claim 2), Computer Fraud & Abuse Act (“CFAA”) (Claim 3), Intentional
27 Interference with Contract (Claim 4), Intentional Interference with Prospective Business
28 Advantage (Claim 5), Wiretapping/Eavesdropping (Claim 6) and Unfair Competition (Claim 9).

1 See Compl. ¶¶ 59, 66, 72, 81, 92, 100, 121. These claims should be dismissed for two
2 independent reasons. First, Claims 3-6, as well as Claim 9, are barred by the Communications
3 Decency Act of 1996 (“CDA”), 47 U.S.C. Section 230, which protects providers, such as
4 Microsoft, who take actions to filter objectionable content. Second, all of Claims 1-6 and Claim 9
5 should be dismissed for failure to state a claim, as Holomaxx fails to plead facts sufficient to
6 support those claims and it sets forth theories that are not recognized in the law.

7 Additionally, Holomaxx has brought two claims—Claims 7 and 8—based on Microsoft’s
8 alleged statements about this filtering activity. On this theory Holomaxx asserts: Defamation
9 (Claim 7) and False Light (Claim 8). Holomaxx fails to plead legally sufficient facts to support
10 these causes of action. Accordingly, like the rest of its claims, Holomaxx’s defamation and false
11 light allegations must be dismissed for failure to state a claim.

12 On these bases, the entire complaint should be dismissed.

13 **A. Motion to Dismiss Standard.**

14 A party may move to dismiss a claim under Federal Rule of Civil Procedure 12(b)(6) if,
15 from the face of the complaint, the plaintiff fails to state a claim upon which relief can be granted.
16 Fed. R. Civ. P. 12(b)(6). A plaintiff must “provide the grounds of his ‘entitle[ment] to relief’ ...
17 [which] requires more than labels and conclusions, and a formulaic recitation of a cause of action
18 will not do ... [f]actual allegations must be enough to raise a right to relief above the speculative
19 level” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citations omitted). Dismissal
20 for failure to state a claim under Rule 12(b)(6) is appropriate “where the complaint lacks a
21 cognizable legal theory or sufficient facts to support a cognizable legal theory.” *Mendondo v.*
22 *Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). For instance, this Court recently
23 granted a motion to dismiss where plaintiff’s allegations, taken as true, would give rise to conduct
24 immunized by the CDA. See *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193, 1202 (N.D. Cal.
25 2009) (Fogel, J.); *Black v. Google, Inc.*, 2010 U.S. Dist. LEXIS 82905 (N.D. Cal. Aug. 13, 2010)
26 (Wilken, J.); see also *Young v. Facebook, Inc.*, 2010 U.S. Dist. LEXIS 116530 (N.D. Cal. Oct.
27 25, 2010) (Fogel, J.) (allegations regarding termination of user account failed to state a claim).

28

1 Further, the Court need not credit conclusory allegations, unwarranted deductions of fact,
 2 or unreasonable inferences. *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949-50 (2009); *Sprewell v.*
 3 *Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001). Rule 12(b)(6) must be read in
 4 conjunction with the pleading requirements of Rule 8(a)(2). *Sprewell*, 266 F.3d at 988. Rule
 5 8(a)(2) requires “a short and plain statement of the claim showing that the pleader is entitled to
 6 relief.” Fed. R. Civ. P. 8(a)(2). Rule 8(a)(2) requires a “‘showing,’ rather than a blanket
 7 assertion, of entitlement to relief ... [w]ithout some factual allegation in the complaint, it is hard
 8 to see how a claimant could satisfy the requirement of providing not only ‘fair notice’ of the
 9 nature of the claim, but also ‘grounds’ on which the claim rests.” *Twombly*, 550 U.S. at 556 n.3.
 10 Though a pleading must contain “only enough facts to state a claim to relief that is plausible on
 11 its face,” *id.* at 570, if the “plaintiffs ... have not nudged their claims across the line from
 12 conceivable to plausible, their complaint must be dismissed.” *Id.*

13 **B. The Communications Decency Act Bars Holomaxx’s Third Through Sixth**
 14 **And Ninth Claims.**

15 The CDA bars Holomaxx’s Third through Sixth and Ninth claims. These claims are
 16 predicated on Microsoft’s filtering of e-mail aimed by Holomaxx at Microsoft’s customers. Such
 17 filtering cannot be the basis of liability pursuant to the CDA’s “Good Samaritan” provision:

18 (c) **Protection for “Good Samaritan” blocking and screening of offensive material**

19 ...

20 No provider or user of an interactive computer service shall be held liable on
 account of—

21 (A) any action taken voluntarily in good faith to restrict access to or availability
 22 of material that the provider or user considers to be obscene, lewd, lascivious,
filthy, excessively violent, harassing, or otherwise objectionable, whether or not
 such material is constitutionally protected; or

23 (B) any action taken to enable or make available to information content
 24 providers or others the technical means to restrict access to material described in
 [subparagraph (A)]

25 47 U.S.C. § 230(c)(2) (emphasis added). Congress has made clear that these safe harbor
 26 provisions were intended to be broad, directing: “[n]o cause of action may be brought and no
 27 liability may be imposed under any State or local law that is inconsistent with this Section.”
 28 *Id.* 230(e)(3).

1 Federal courts have recognized that e-mail filtering, such as Microsoft's activities in this
2 case, fall squarely within the CDA's safe harbor. The recent case *e360Insight, LLC v. Comcast*
3 *Corp.* is directly on point. 546 F. Supp. 2d at 609-610. There, the Northern District of Illinois
4 found that the CDA barred claims against a service provider who filtered objectionable e-mail.
5 The complaint, identical in all relevant respects to the complaint at issue here, was dismissed.
6 *e360Insight*, Dismissal is similarly mandated here. *Id.*

7 **1. Accepting Holomaxx's Allegations As True, Microsoft Satisfies All**
8 **Requirements Necessary For CDA Immunity.**

9 To qualify for immunity from liability under CDA Section 230, a defendant must (1) be a
10 "provider ... of an interactive computer service," (2) take action "to restrict access to or
11 availability of material that the provider ... considers to be ... harassing, or otherwise
12 objectionable," and (3) take that action "in good faith." 47 U.S.C. § 230(c)(2); *see also Zango v.*
13 *Kaspersky*, 568 F.3d 1169 (9th Cir. 2009) (setting forth requirements for CDA Section 230
14 immunity). Microsoft easily satisfies all of the CDA's requirements.

15 *First*, it is undisputed and clear from Holomaxx's own allegations that Microsoft is an
16 "interactive computer service" provider. The CDA defines this term as:

17 any information service, system, or access software provider that provides or
18 enables computer access to multiple users to a computer server, including
specifically a service or system that provides access to the Internet.

19 47 U.S.C. §§ 230 (b)(3), (f)(2); *see also Optinrealbig.com LLC, v. Ironport Systems, Inc.*, 323 F.
20 Supp. 2d 1037, 1044 (N.D. Cal. 2004) (courts "have recognized that the definition includes a
21 wide range of cyberspace services ..."); *Black*, 2010 U.S. Dist. LEXIS 82905, at *6 (courts have
22 adopted "a relatively expansive definition of 'interactive computer service'"). Holomaxx alleges
23 that Microsoft is a service provider that enables computer access. Compl. ¶ 20 (asserting that
24 Microsoft is "one of the world's largest internet service providers ('ISPs')" and "provides free
25 email accounts to millions of users and businesses"). Specifically, Microsoft operates computer
26 servers (i.e., its e-mail servers), which users access to view and download their e-mail.

27 Holomaxx also alleges that Microsoft utilizes its "automated spam filter." *Id.* ¶ 20. Thus,
28 Microsoft also falls within the above definition as an "access software provider." *See* 47 U.S.C. §

1 230(f)(4)(A) (defined as a provider of software tools that “filter, screen, allow or disallow
2 content...”). Thus, Microsoft qualifies as an “interactive computer service.” This conclusion
3 comports with that of courts holding that e-mail providers that filter objectionable e-mail qualify
4 as “interactive computer service” providers. *See e360Insight*, 546 F. Supp. 2d at 607; *Winter v.*
5 *Bassett*, 2003 U.S. Dist. LEXIS 26904, *7 n.4 (M.D.N.C. Aug. 22, 2003) (service providers that,
6 among other things, “provide email services,” are “interactive computer services under the
7 Communications and Decency Act.”). Microsoft thus meets the first element for CDA immunity.

8 *Second*, it is undisputed that Microsoft has taken action “to restrict access to or availability
9 of material” that it “considers to be ... harassing, or otherwise objectionable.” Holomaxx
10 repeatedly alleges that Microsoft is engaged in the filtering or blocking of e-mail that it considers
11 harassing and objectionable. *See, e.g.*, Compl. ¶¶ 20-24, 31-36, 49-51. Holomaxx itself alleges
12 that Microsoft made a determination (based on Microsoft’s proprietary analysis) that Holomaxx’s
13 e-mails constitute objectionable spam. *Id.* ¶¶ 34, 51(a). Case law confirms that CDA immunity
14 adheres to the blocking of objectionable, bulk e-mail. *See, e.g., e360Insight*, 546 F. Supp. 2d at
15 607 (bulk e-mails are the sort of communications a service provider could deem objectionable);
16 *see also Zango*, 568 F.3d at 1175 (Congress intended to “immunize the providers of blocking
17 software”); *Optinrealbig.com*, 323 F. Supp. 2d at 1040 (holding that defendant, which collected
18 and sent user complaints about spam e-mail to ISPs, was protected by Section 230 in an action by
19 bulk e-mail company). Thus, Microsoft meets this element for CDA immunity as well.

20 *Third*, Holomaxx does not claim that Microsoft carried out its filtering in bad faith. Nor
21 could it. Indeed, as alleged, Microsoft’s proprietary filtering software is of the same type used by
22 many other companies, including those that federal courts have held immunized by the CDA.
23 *e360Insight*, 546 F. Supp. 2d at 606-610 (plaintiff failed to sufficiently plead bad faith under
24 *Twombly*; finding CDA immunity where defendant, like the federal judiciary and other
25 enterprises, used software filters to control e-mail volume and to block e-mail deemed
26 objectionable); *Optinrealbig.com*, 323 F. Supp. 2d at 1040 (CDA immunity where defendant
27 collected and forwarded spam complaints to ISPs); *Zango, Inc.*, 568 F.3d at 1170-71 (CDA
28

1 immunity where defendant used software to filter and block other software it deemed malicious).
2 Thus, Microsoft meets this element for CDA immunity.

3 Because Microsoft operates an interactive computer service which is engaged in the good
4 faith blocking or filtering of objectionable content, it is entitled to immunity under the CDA as to
5 claims based on this activity under both federal and state law. *See* 47 U.S.C. §§ 230(c)(2)
6 (blanket immunity); (e)(3) (expressly barring state law claims inconsistent with CDA immunity).

7 **2. Because Microsoft Is Entitled To Immunity Under The CDA, The**
8 **Court Must Dismiss Holomaxx's Claims Three Through Six And Nine.**

9 Courts have repeatedly dismissed claims where a defendant's alleged conduct meets the
10 requirements of a CDA safe harbor. *See Zango, Inc.*, 568 F.3d at 1177-78; *Goddard*, 640 F.
11 Supp. 2d at 1202; *Black*, 2010 U.S. Dist. LEXIS 82905, at *9-10. Indeed, based on the CDA, one
12 court dismissed claims of an e-mail marketing company against an e-mail provider who filtered
13 out the marketing company's e-mail. *See e360Insight*, 546 F. Supp. 2d at 609-10 ("I grant
14 judgment on the pleadings with respect to the complaint as a whole on the grounds that § 230(c)
15 precludes proceeding on any of the claims."). Likewise, here, Microsoft satisfies all requirements
16 for CDA immunity. Accordingly, as was true of the ISP in *e360Insight*, Microsoft here
17 performed the exact function contemplated by the CDA: it used filtering technology to restrict
18 access to or availability of material it deemed to be objectionable. Therefore, Holomaxx's Claims
19 3-6 and 9, based on Microsoft's e-mail filtering activities, must be dismissed.

20 **3. Holomaxx's Disagreement With Microsoft's Filtering Methodology Is**
21 **Legally Irrelevant And Does Not Save Holomaxx's Claims.**

22 Holomaxx seeks to escape the clear applicability of the CDA safe harbor by asserting that
23 it disagrees with Microsoft's determination that Holomaxx's e-mails are objectionable. Compl.
24 ¶¶ 13-24, 31-41. This assertion is legally irrelevant and does not save Holomaxx's claims. In
25 order to qualify for CDA immunity, Section 230 requires only that Microsoft subjectively
26 determine that blocked material is "harassing" or "objectionable." *See e360Insight*, 546 F. Supp.
27 2d at 608 ("section 230 imposes a subjective element into the determination of whether a provider
28 or user is immune from liability"); *see also Zango, Inc. v. Kaspersky*, 2007 U.S. Dist. LEXIS

1 97332, *6-7 (W.D. Wash. Aug. 28, 2007), *affirmed by* 568 F.3d 1169 (9th Cir. 2009) (Section
2 230(c)(2) “does not require that the material actually be objectionable; rather it affords protection
3 for blocking material ‘that the provider or user considers to be’ objectionable”). As discussed
4 above, Holomaxx’s allegations themselves demonstrate that Microsoft subjectively determined
5 that the filtered e-mail were objectionable. Thus, Holomaxx’s argument fails.

6 Along the same lines, Holomaxx argues that its mass e-mail blasts complied with the
7 CAN-SPAM Act. *See, e.g.*, Compl. ¶ 18. Again, this is legally irrelevant. Nothing in the CDA
8 purports to carve back a service provider’s immunity merely because the plaintiff complies with
9 the CAN-SPAM Act. Nor can Holomaxx point to anything in the CAN-SPAM Act which
10 provides it a right to sue Microsoft despite the clear import of the CDA. Holomaxx’s suggestion
11 that CAN-SPAM compliance bears on the CDA ignores two federal statutes. Not surprisingly,
12 courts have rejected arguments identical to Holomaxx’s. For example, in *e360Insight*, as here,
13 the plaintiff pointed to its alleged CAN-SPAM compliance as evidence that its e-mails were not
14 properly the subject of CDA immunity. 568 F.3d at 608-09. The court rejected this theory,
15 noting, “compliance with CAN-SPAM, Congress decreed, does not evict the right of the provider
16 to make its own good faith judgment to block mailings.” *Id.* at 608 (“Section 7707 of the [CAN-
17 SPAM] Act says nothing in the Act shall ‘have any effect on the lawfulness ... under any other
18 provision of law, of the adoption, implementation, or enforcement by a provider of Internet access
19 service of a policy of declining to transmit, route, relay, handle or store certain types of electronic
20 mail messages.’”). The court further observed that “[u]nder the law, a mistaken choice to block,
21 if made in good faith, cannot be the basis for liability under federal or state law. To force a
22 provider like [defendant e-mail service provider] to litigate the question of whether what it
23 blocked was or was not spam would render § 230(c)(2) nearly meaningless.” *Id.*

24 More generally, Holomaxx asserts that Microsoft’s filtering is overly broad. Compl. ¶¶
25 13-24, 31-41. This assertion too is irrelevant. When Congress enacted the CDA Good Samaritan
26 provision, it understood that in order for content filtering technologies to function effectively,
27 such technologies might block too much or too little content:
28

1 Congress, and, I think, everyone else who studied the issue understood that
 2 blocking software would probably block too much. To insure that you or your
 3 child will not receive unwanted or inappropriate e-mails, your Internet service may
 4 wind up preventing you from receiving some e-mails that are neither unwanted nor
 inappropriate. Such Internet service providers feared they might be held liable for
 blocking too much, or even too little, and this was, as Congress recognized, “[a]
 disincentive[] for the ... utilization of blocking and filtering technologies.”

5 *e360Insight*, 546 F. Supp. 2d at 607. This observation is unsurprising, as it goes to the CDA’s
 6 core legal and policy justifications: to protect businesses and individuals from unwanted content
 7 by encouraging service providers such as Microsoft to develop and use filtering technologies
 8 without fear of legal retribution by e-mail marketers or other content providers.² 47 U.S.C. §
 9 230(c). In other words, even if Holomaxx could show that each of its millions of e-mails were
 10 the paragons of legitimate electronic communications, it would be totally irrelevant. When it
 11 enacted the CDA Congress anticipated that filtering technology would, at times, be overly broad
 12 and immunized service providers in order to encourage the development of filtering technologies.
 13 The CDA’s Good Samaritan provision was enacted precisely to bar the type of claim that
 14 Holomaxx brings against Microsoft in this case.

15 Accordingly, because Microsoft is immune from liability under the Good Samaritan
 16 provision of the CDA, the Third through Sixth and the Ninth Claims for Relief, arising out of
 17 Microsoft’s actions to block Holomaxx’s e-mails, should be dismissed.

18 **C. Each Of Holomaxx’s Claims Is Insufficiently Pled And Should Be Dismissed**
 19 **For Failure To State A Claim.**

20 **1. Holomaxx Fails To State A Claim For Violation Of The Wiretap Act.**

21 In its First Claim for Relief, Holomaxx alleges that Microsoft violated the Federal Wiretap
 22 Act. Compl. ¶ 59. The Wiretap Act prohibits the interception of electronic communications. 18
 23 U.S.C. §§ 2510 *et seq.* According to Holomaxx, Microsoft violated the statute by “intentionally
 24

25 _____
 26 ² Congress enacted the CDA “to encourage the development of technologies which maximize
 27 user control over what information is received by individuals, families, and schools who use the
 28 Internet and other interactive computer services.” 47 U.S.C. § 230(b)(3). Congress
 acknowledged that “[t]he problems associated with the rapid growth and abuse of unsolicited
 commercial electronic mail cannot be solved by Federal legislation alone. The development and
 adoption of technological approaches ... will be necessary as well.” 15 U.S.C. § 7701(a)(12).

1 intercept[ing] electronic communications sent by HOLOMAXX.” *Id.* This claim fails for four
2 independent reasons.

3 First, the Wiretap Act provides that the operator of an electronic communication service
4 cannot be liable for interceptions carried out to protect the operator’s rights or property:

5 It shall not be unlawful under this chapter for ... an officer, employee, or agent of
6 a provider of [an] ... electronic communication service, whose facilities are used
7 in the transmission of [an] ... electronic communication, to intercept, disclose, or
8 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...

9 18 U.S.C. § 2511(2)(a)(i); *see Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 U.S. Dist.
10 LEXIS 91644, *14-16 (W.D. Pa. Dec. 13, 2007) (dismissing Wiretap Act claims; defendant e-
11 mail provider had right to monitor e-mails sent to one of its e-mail addresses in order to protect its
12 rights and interests); *cf. Howard v. America Online, Inc.*, 208 F.3d 741, 751-53 (9th Cir. 2000)
13 (holding that AOL could properly exert control over the traffic it would accept). Here, Holomaxx
14 alleges that Microsoft accessed and filtered e-mails as part of an effort to protect itself and its
15 customers from spam. Clearly the alleged acts are a necessary incident to Microsoft’s protection
16 of its rights and property. Thus, Holomaxx fails to state a claim for violation of the Wiretap Act.

17 Second, Holomaxx has failed to adequately plead that Microsoft intercepted any
18 electronic communications. Holomaxx alleges, without any factual support, that Microsoft
19 “intercepted” electronic communications to Microsoft e-mail accountholders. Compl. ¶¶ 11, 59.
20 Such conclusory statements are not entitled to the assumption of truth. *Iqbal*, 129 S. Ct. at 1949
21 (citing *Twombly*, 550 U.S. at 555) (“Although for the purposes of a motion to dismiss we must
22 take all of the factual allegations in the complaint as true, we ‘are not bound to accept as true a
23 legal conclusion couched as a factual allegation’”). Holomaxx’s *own complaint* contradicts these
24 conclusory statements. Specifically, Paragraph 41 makes clear that Holomaxx alleges that
25 Microsoft “accessed computers on which HOLOMAXX’s confidential e-mail communications
26 were **stored**.” Compl. ¶ 41 (emphasis added). It is well-established that accessing e-mails while
27 they are in storage does not constitute an “interception” under the statute. *See Konop v. Hawaiian*
28 *Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (for an electronic communication to be

1 “‘intercepted’ in violation of the Wiretap Act, it must be acquired during transmission, not while
2 it is in electronic storage”); *see also Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967,
3 979 (M.D. Tenn. 2008) (“unless an e-mail is actually acquired in its split second transmission
4 over a computer network, it cannot be ‘intercepted’ as that term is reasonably understood.”).

5 In *Bradley v. Google*, No. C06-05289-WHA, 2006 U.S. Dist. LEXIS 94455, *14 (N.D.
6 Cal. Dec. 22, 2006), the plaintiff alleged that defendant, an e-mail service provider, violated the
7 Wiretap Act by removing or deleting messages stored on its servers. The court held that the
8 plaintiff failed to state a claim because the Wiretap Act only applies to communications that are
9 intercepted, or acquired during transition. *Id.* at *13-14. The Wiretap Act, Judge Alsup
10 recognized, simply does not apply to situations where the electronic communications are in
11 storage. *Id.* Here, just as in *Bradley*, Holomaxx itself has alleged that Microsoft accessed its e-
12 mail communications on computers where they were stored, not while they were in transmission.
13 Compl. ¶ 41. Therefore, Holomaxx fails to state a claim under the Wiretap Act.

14 Third, the statute is clear that no Wiretap Act violation can occur where, as here, one party
15 to the communication has given prior consent. *See* 18 U.S.C. § 2511(2)(d) (no Wiretap Act
16 violation “where one of the parties to the communication has given prior consent” to
17 interception). Here, the recipients of Holomaxx’s e-mails are users of Microsoft’s e-mail
18 services, such as Hotmail. Compl. ¶ 20. As such, they provide broad consent for Microsoft to
19 access or disclose e-mails sent to their accounts, so that Microsoft can effectively protect itself
20 and its customers. Specifically, through Paragraph 6 of the Hotmail Terms of Service,
21 accountholders agree that:

22 In particular, we [Microsoft] may access or disclose information about you,
23 including the content of your communications, in order to: (a) comply with the law
24 or respond to lawful requests or legal process; (b) protect the rights or property of
25 Microsoft or our customers, including the enforcement of our agreements or
policies governing your use of the service; or (c) act on a good faith belief that
such access or disclosure is necessary to protect the personal safety of Microsoft
employees, customers, or the public.³

26
27 ³ It is well-established that the Court may consider documents not attached or included in a
28 complaint when the pleading references or refers to them. *See Branch v. Tunnell*, 14 F.3d 449,
454 (9th Cir. 1994), *overruled by other grounds by Galbraith v. County of Santa Clara*, 307 F.3d
1119, 1127 (9th Cir. 2002) (“documents whose contents are alleged in a complaint and whose
authenticity no party questions, but which are not physically attached to the pleading, may be

1 See Declaration of Brooke Roundy in Support of Microsoft’s Motion to Dismiss, Ex. A
2 (submitted herewith). Because Microsoft’s alleged actions fall within its accountholders’ broad
3 consent, Holomaxx cannot state a claim for “interception” under the Wiretap Act. 18 U.S.C. §§
4 2511(1), (2)(d). Further, Holomaxx cannot state a claim for alleged “use” or “disclosure” of
5 electronic communications under the Wiretap Act (Compl. ¶ 60), because—as discussed—the
6 information was not obtained in violation of the Act. 18 U.S.C. §§ 2511(1)(c)-(d) (disclosure or
7 use prohibited where information was “obtained ... in violation of this subsection”).

8 Finally, Holomaxx’s Wiretap Act claim should also be dismissed as insufficiently pled.
9 Holomaxx does not even identify the Wiretap Act provisions that Microsoft allegedly violated,
10 nor does it plead sufficient facts. Instead, Holomaxx merely recites the language of the statute,
11 conclusorily claiming that Microsoft “intentionally intercepted” communications (Compl. ¶ 59),
12 and “intentionally used and disclosed the contents of such electronic communications” (*id.* ¶ 60).
13 Such bare legal conclusions are legally insufficient. *Iqbal*, 129 S. Ct. at 1949-50 (citing
14 *Twombly*, 550 U.S. at 555, 557) (“A pleading that offers ‘labels and conclusions’ or ‘a formulaic
15 recitation of the elements of a cause of action will not do.’”).

16 While Holomaxx cursorily asserts that Microsoft accessed computers on which
17 Holomaxx’s e-mail communications were stored and intercepted such e-mails, it fails entirely to
18 identify the computers or to allege any facts regarding how Microsoft accessed these computers,
19 to whom the computers belong, or how Microsoft obtained information in these e-mails. Compl. ¶
20 41. This is precisely the kind of “naked assertion” devoid of “further factual enhancement” that
21 the Supreme Court has found unacceptable. *See Twombly*, 550 U.S. at 557. Accordingly, the
22 Court should dismiss the First Claim for Relief.

23 ///

24
25 considered in a ruling on a Rule 12(b)(6) motion to dismiss”); *In re Stac Elecs. Sec. Litig.*, 89
26 F.3d 1399, 1405 n.4 (9th Cir. 1996) (documents whose contents are alleged in the complaint may
27 be considered in connection with a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6)). The
28 Court may thus properly consider the Hotmail terms of service, as Holomaxx’s Complaint
repeatedly references those terms and puts them at issue. *See, e.g.*, Compl. ¶ 41 (Microsoft
accessed electronic communications “without the consent of either HOLOMAXX or the intended
recipients”). A true and correct copy of the terms of service are attached hereto as Exhibit A to
the Declaration of Brooke Roundy.

1 2. **Independent Of The CDA, Holomaxx Fails To State A Claim For**
2 **Violation Of California Penal Code §§ 630 et seq.**

3 In its Sixth Cause of Action, Holomaxx brings a claim under California Penal Code
4 Section 631, analogous to the Federal Wiretap Act. This claim also fails. First, because
5 Holomaxx asserts precisely the same facts and legal theory under Section 631 and the Wiretap
6 Act, the state claim is preempted as a matter of law. The Federal Wiretap Act contains an express
7 preemption: “The remedies and sanctions described in this chapter with respect to the interception
8 of electronic communications are the only judicial remedies and sanctions for nonconstitutional
9 violations of this chapter involving such communications.” 18 U.S.C. § 2518(10)(c). Recently,
10 where plaintiff asserted Section 631 and the Wiretap Act under the same theory, the state law
11 claim was dismissed as preempted. *Bunnell v. Motion Picture Ass’n of Am.*, 567 F. Supp. 2d
12 1148 (C.D. Cal. 2007). Holomaxx’s Section 631 claim must be dismissed on this basis.

13 Moreover, like the Wiretap Act, Section 631 applies only to communications improperly
14 obtained while they are “in transit.” Cal. Penal Code § 631. Here, Holomaxx states, without any
15 factual support, that Microsoft accessed e-mails while they were in transit. As with the Wiretap
16 Act allegations, Holomaxx’s bare allegation is expressly contradicted by facts asserted elsewhere
17 in the Complaint that Holomaxx’s theories are based on alleged access to “**stored**”
18 communications. Compl. ¶¶ 41, 101. As discussed, accessing e-mails in storage cannot
19 constitute “interception” because such communications are not in transit. *See Bradley*, 2006 U.S.
20 Dist. LEXIS 94455, at *14-15 (granting defendant’s motion to dismiss: “Like its federal
21 counterpart, [Section 630 et seq.] ... requires the *interception* of an electronic communication”).

22 3. **Holomaxx Fails To State A Claim For Violation Of The Stored**
23 **Communications Act.**

24 In its Second Claim for Relief, Holomaxx alleges that Microsoft violated the Stored
25 Communications Act (“SCA”), which prohibits a party from “intentionally access[ing] without
26 authorization a facility through which an electronic communication service is provided; ... or
27 intentionally exceed[ing] an authorization to access that facility; ... thereby obtain[ing] ... or
28

1 prevent[ing] authorized access to ... a wire or electronic communication while it is in electronic
2 storage...” 18 U.S.C. § 2701(a).

3 This claim fails for several reasons. In particular, the SCA does not apply to conduct
4 authorized by “entit[ies] providing a wire or electronic communications service” and conduct
5 authorized “by a user of that service with respect to a communication of or intended for that
6 user.” § 2701(c)(1)-(2). Microsoft’s alleged conduct is exempt under both subsections. First, the
7 SCA exempts searches of stored electronic communications by the party providing the
8 communications service. *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2003)
9 (“[W]e hold that, because [plaintiff’s] e-mail was stored on [defendant’s] system (which
10 [defendant] administered), its search of that e-mail falls within §2701(c)’s exception to [the
11 SCA]”); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (defendant could not
12 violate SCA when it retrieved pager text messages stored on its computer system because
13 defendant “is the provider of the ‘service’” and “service providers [may] do as they wish when it
14 comes to accessing communications in electronic storage.”). As another Northern District of
15 California judge summarized in dismissing a virtually identical ECPA/SCA claim:

16 Crowley’s second argument in support of his unauthorized access claim, which is
17 that Amazon had limited access to its own systems, strains credulity. First,
18 Crowley cites no authority in support of this argument. Second, a very similar
19 argument was rejected by the court in *State-Wide Photocopy Corp. v. Tokai*
20 *Financial Services, Inc.*, 909 F. Supp. 137 (S.D.N.Y. 1995). In that case, the court
21 said that, even assuming that a company’s computers, through which it sent and
22 received electronic communications, were “facilities through which an electronic
23 communication service is provided,” the computer could not have limited access to
24 its own facilities.” *See id. at 145*. Amazon’s access to its own systems is not
25 limited under the ECPA.

22 *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1272 (N.D. Cal. 2001) (citations omitted).
23 As the provider of the alleged recipients’ e-mail accounts, the SCA does not apply to Microsoft’s
24 alleged access of e-mails.

25 Second, as detailed above, Holomaxx’s SCA claim should be dismissed because the
26 alleged e-mail recipients, as Microsoft accountholders, authorized Microsoft to access e-mails
27 sent by Holomaxx, pursuant to the broad consent agreed to in Microsoft’s terms of use. “[T]he
28 statutory exemption set forth in § 2701(c)(2) is applicable as long as one party to a

1 communication provides consent.” *In re Toys R Us, Inc., Privacy Litig.*, No. C00-2746-MMC,
 2 2001 U.S. Dist. LEXIS 16947, at *18 (N.D. Cal. Oct. 9, 2001) (dismissing SCA claim without
 3 leave to amend where one party to the communication provided consent).

4 Third, Holomaxx’s SCA claim again merely recites the statutory language and is devoid
 5 of facts required to establish a plausible cause of action. Compl. ¶ 66 (restating bare language of
 6 the statute). As discussed, Holomaxx alleges that Microsoft accessed computers on which e-mail
 7 communications were stored (*see id.* ¶ 41), but fails entirely to allege any plausible facts regarding
 8 how this occurred in violation of the SCA. Accordingly, the Court should dismiss Holomaxx’s
 9 Second Claim. *See Iqbal*, 129 S. Ct. at 1949-50; *Twombly*, 550 U.S. at 557.

10 **4. Independent Of The CDA, Holomaxx Fails To State A Claim for**
 11 **Violation Of The Computer Fraud And Abuse Act.**

12 Holomaxx’s Third Claim for Relief for violation of the Computer Fraud and Abuse Act
 13 (“CFAA”), 18 U.S.C. Section 1030, *et seq.*, is deficient for a variety of reasons. First and
 14 foremost, Holomaxx’s assertions are predicated on facially impossible theory that Microsoft is
 15 liable for accessing without authorization *its own servers* in the process of filtering objectionable
 16 e-mail. Compl. ¶ 41 (Holomaxx alleges that Microsoft improperly “accessed computers on which
 17 HOLOMAXX’s confidential email communications were stored”). Nowhere in the Complaint
 18 does Holomaxx allege that Microsoft accessed any computer or system belonging to Holomaxx or
 19 any other party. Accessing a company’s own computers is not an unauthorized access to a
 20 “protected computer” in violation of the CFAA. *Cont’l Grp., Inc. v. Kw Prop. Mgmt, LLC*, 622
 21 F. Supp. 2d 1357, 1372 (S.D. Fla. 2009) (an entity “clearly has a right to control and define
 22 authorization to access its own computer systems”); *Ebay, Inc. v. Bidder’s Edge*, 100 F. Supp. 2d
 23 1058, 1070 (N.D. Cal. 2002) (holding that an internet company’s servers are its own “private
 24 property, conditional access to which [the company] grants the public.”).

25 The touchstone of CFAA—a statute directed at hackers or similar intruders into the
 26 computer systems of others—is that the proscribed access is without authorization or exceeds
 27 authorization.⁴ Plainly Microsoft’s access to its *own* servers is fully authorized and thus the

28 ⁴ In fact, in this case, the CFAA is much more appropriately applied to the emailing activities of

1 CFAA claim fails. *Lewis-Burke Assocs. LLC v. Widder*, No. 09-302-JMF, 2010 U.S. Dist.
2 LEXIS 76180 (D.D.C. July 28, 2010) (granting motion to dismiss CFAA claim where defendant
3 was authorized to access the computer); *Secureinfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593
4 (E.D. Va. 2005) (dismissing CFAA claim where plaintiff did not properly allege that defendants
5 had “unauthorized access” to the server or accessed the server in “excess of authority”).

6 More generally, to the extent that Holomaxx is attempting to allege that some other
7 “protected computer” has allegedly been accessed in violation of the CFAA, it has failed to plead
8 this theory at all, let alone with sufficient particularity. Holomaxx states no facts identifying such
9 computer or how alleged access was without or in excess of authorization, all of which is
10 necessary to state a claim under the CFAA. Again, Holomaxx merely recites partial statutory
11 language of the CFAA, without even specifying which CFAA section was allegedly violated and
12 without any further factual enhancement. *See* Compl. ¶ 73 (alleging that Microsoft “intentionally
13 exceeded [its] authorization to access computers used for interstate and foreign communications
14 and commerce, and obtained information from such computers, in violation of 18 U.S.C. §§ 1030
15 *et seq.*”). Such cursory legal conclusions and bare assertions devoid of requisite facts fail to state
16 a claim. *Iqbal*, 129 S. Ct. at 1949-50; *Twombly*, 550 U.S. at 557. For these reasons, Holomaxx’s
17 Third Claim for Relief should be dismissed.

18 **5. Independent Of The CDA, Holomaxx Fails To State A Claim For**
19 **Intentional Interference With Contract And Intentional Interference**
20 **With Prospective Business Advantage.**

21 In its Fourth and Fifth Claims for Relief, Holomaxx alleges that Microsoft interfered with
22 Holomaxx’s contractual and prospective business relationships by intercepting and blocking
23 Holomaxx’s e-mail communications and providing purportedly false and misleading information
24 about Holomaxx to Dragon Networks. Compl. ¶ 81. These claims are meritless.

25 To state a claim for Intentional Interference with Contract, Holomaxx must allege: (1) a
26 valid contract between Holomaxx and a third party; (2) Microsoft’s knowledge of this specific
27 contract; (3) that Microsoft’s intentional acts were designed to induce a breach or disruption of

28 Holomaxx, which intrudes upon Microsoft’s servers. *See Hotmail Corp. v. Van\$ Money Pie Inc.*,
47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (granting preliminary injunction under CFAA
where defendant sent spam email to Hotmail subscribers without their authorization).

1 the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5)
2 resulting damage. *See Pacific Gas & Elec. Co. v. Bear Stearns & Co.*, 50 Cal. 3d 1118 (1990).
3 Although related to this first claim, the California Supreme Court has cautioned that intentional
4 interference with prospective business advantage is distinct and carries a “more rigorous pleading
5 burden since it must show that the defendant’s conduct was independently wrongful.” *Korea*
6 *Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1158 (2003). Accordingly, to state a
7 claim for interference with business advantage, Holomaxx must allege: (1) an existing economic
8 relationship between Holomaxx and a third party, containing a profitable future economic benefit
9 or advantage to plaintiff; (2) that Microsoft knew of the existence of this specific relationship; (3)
10 that Microsoft intentionally engaged in wrongful conduct designed to interfere with or disrupt this
11 relationship; (4) that the economic relationship was actually interfered with or disrupted; and (5)
12 resulting damage. *See Della Penna v. Toyota Motor Sales, Co.*, 11 Cal. 4th 376 (1995).

13 Holomaxx fails to meet its burden for either claim.

14 Here, Holomaxx first alleges that Microsoft interfered with its relationships and contracts
15 with unidentified clients, who allegedly contracted with Holomaxx to send bulk commercial e-
16 mails on their behalf. Compl. ¶ 81. Holomaxx next alleges that Microsoft interfered with its
17 relationship and contract with Dragon Networks, the company that allegedly hosted Holomaxx’s
18 IP datacenter. *Id.* ¶ 93.

19 First, to state a claim, Holomaxx would need to plead, at a minimum, that Microsoft had
20 knowledge of these specific contracts or relationships and that it engaged in conduct intentionally
21 aimed at disrupting them. *Korea Supply Co.*, 29 Cal. 4th at 1156-57 (to establish intentional
22 interference with business advantage, plaintiff must plead that defendant “kn[ew] that the
23 interference was certain or substantially certain to occur as a result of his action”); *Quelimane Co.*
24 *v. Stewart Title Guar. Co.*, 19 Cal. 4th 26, 56 (1998) (to establish intentional interference with
25 contract, plaintiff must plead that defendant knew that interference was a necessary consequence
26 of its actions). As to the alleged disruption, Holomaxx would need to additionally plead that
27 Microsoft’s actions were “wrongful.” Holomaxx does not do so. There is nothing in Holomaxx’s
28 Complaint alleging that Microsoft knew of these specific contracts or relationships when it

1 allegedly blocked Holomaxx's IP Addresses. *See Maxner Co. Ltd, v. Costco Wholesale Corp.*,
2 No. 03-35865, 2004 U.S. App. LEXIS 14298, at *18 (9th Cir. July 12, 2004) (finding that
3 plaintiff failed to establish intentional interference where, "[a]s to the knowledge element,
4 Maxner did not present sufficient evidence of Costco's awareness of Maxner *at the time of its*
5 *decision* to reject the bunnies") (emphasis added).

6 Holomaxx alleges that "Microsoft knows full well that Holomaxx sends emails on behalf
7 of commercial clients because, *inter alia*, Holomaxx has informed Microsoft of this fact in
8 numerous communications with Microsoft." Compl. ¶ 37. But Holomaxx fails to allege that
9 Microsoft knew of the alleged relationships or contracts at the time that it blocked Holomaxx's IP
10 addresses. To the contrary, Holomaxx only refers to an April 30, 2010 e-mail to Microsoft in
11 which Holomaxx wrote a vague assertion that if its e-mail "does not get through, we lose money
12 because they don't pay us for undelivered mail." *Id.* According to the Complaint, this alleged e-
13 mail communication came well after the November 20, 2009 date on which Holomaxx alleges
14 that "Microsoft began intermittently" blocking Holomaxx's objectionable e-mails. *Id.* ¶ 31.
15 Thus, the Complaint itself negates any possibility that Microsoft blocked Holomaxx's IP
16 addresses with knowledge of Holomaxx's specific contracts or relationships. Indeed, the
17 Complaint makes clear that Microsoft allegedly blocked the IP addresses because Microsoft had
18 determined that Holomaxx was sending spam; Holomaxx's prospective business relationships and
19 contracts never entered into the equation and Holomaxx alleges nothing to the contrary.

20 Nor was Microsoft's alleged blocking of the IP addresses wrongful. As discussed above,
21 Microsoft's e-mail filtering is fully protected by the CDA's Good Samaritan provision. *See*
22 Section III.B., *supra*. Therefore, since Microsoft's actions were expressly authorized and
23 encouraged by Congress, Holomaxx cannot establish that Microsoft's actions were independently
24 wrongful. The allegations thus necessarily also fail to meet the more rigorous pleading standard
25 required for Plaintiff's Intentional Interference with Prospective Business Advantage claim.
26 *Della Penna*, 11 Cal. 4th at 393 ("...a plaintiff seeking to recover for an alleged interference with
27 prospective contractual or economic relations must plead and prove as part of its case-in-chief
28 that the defendant not only knowingly interfered with the plaintiff's expectancy, but engaged in

1 conduct that was wrongful by some legal measure other than the fact of interference itself.”).
2 Plaintiff’s theory would render the CDA’s Good Samaritan provision meaningless. In effect,
3 Holomaxx argues that after the onset of CDA-compliant blocking, a complaint by the blocked
4 party is sufficient to retroactively impute wrongful knowledge for that blocking. This theory is
5 clearly wrong, would expose ISPs to unreasonable amounts of unknown risk and would
6 contravene Congressional intent in passing the CDA.

7 Once again, the recent *e360Insight* opinion is instructive. The plaintiff there also tried to
8 argue that by blocking its e-mail messages, defendant was intentionally interfering with plaintiff’s
9 contracts and relationships. *e360Insight*, 546 F. Supp. 2d at 609. The court rejected these
10 arguments, holding that such theories were barred by the Good Samaritan provision of the CDA.
11 *Id.* The court further noted that while it may be illegal to interfere with business prospects,
12 “usually they are a class of easily identified individuals and usually the interference is that of the
13 defendant interacting directly with the prospective buyers.” *Id.* at 609 n.3 (finding no cases in
14 which a “refusal to allow a plaintiff to run an advertisement in a medium with wide circulation ...
15 constitutes such tortious interference.”). This uncontroversial holding comports with long-
16 standing California law, which similarly requires an intentional interference claim specifically
17 identify contracts or relationships at issue, establish defendant’s knowledge of that specific
18 contract or relationship, and allege that defendant then interfered. *Accuimage Diagnostics Corp.*
19 *v. Terarecon, Inc.*, 260 F. Supp. 2d 941, 956-57 (N.D. Cal. 2003) (generic allegations that there
20 was an interference with unspecified third parties are insufficient as a matter of law); *Westside*
21 *Ctr. Assocs. v. Safeway Stores 23, Inc.*, 42 Cal. App. 4th 507, 523 (1996) (plaintiff’s claim for
22 interference as to unidentified prospective buyers was insufficient as a matter of law). Holomaxx
23 has alleged none of that here.

24 Holomaxx’s claims arising from its alleged relationship or contract with Dragon Networks
25 fare no better. For instance, Holomaxx has not pled facts sufficient to establish that its
26 relationship with Dragon Networks was actually disrupted. While Holomaxx claims that it did
27 not receive the benefits of its contract with Dragon Networks (Compl. ¶¶ 46, 82, 93), it does not
28 convert these allegations into “plausible” facts that show Holomaxx is entitled to relief.

1 *Twombly*, 550 U.S. at 555 (the Complaint must contain factual allegations sufficient to “raise a
2 right to relief above the speculative level.”). Holomaxx has not pled any facts to establish that
3 Holomaxx or Dragon Networks breached an existing contract or that Dragon Networks is no
4 longer serving as Holomaxx’s datacenter. Indeed, Holomaxx fails to allege *any* facts to show
5 how its relationship with Dragon Networks was disrupted. Therefore, Holomaxx cannot establish
6 intentional interference in its relationship with Dragon Networks.

7 For these reasons, and because Holomaxx’s claims are barred by the CDA, Holomaxx’s
8 Fourth and Fifth Claims for intentional interference should be dismissed.

9 **6. Independent Of The CDA, Holomaxx Fails To State A Claim For**
10 **Unfair Competition.**

11 Holomaxx’s Ninth Claim asserts Unfair Competition under California Business and
12 Professions Code Section 17200, *et seq.* (“UCL”). The claim is meritless and should be
13 dismissed. Holomaxx predicates this theory on the same factual allegations discussed above
14 regarding Microsoft’s e-mail filtering. Compl. ¶¶ 120-121 (“By engaging in the conduct
15 described herein, Defendants have engaged in unlawful, unfair, or fraudulent business acts or
16 practices in violation of [the UCL]”). Holomaxx asserts no independent acts to support this
17 claim; it merely references its other allegations concerning e-mail filtering and concludes that
18 “Defendants’ conduct, as described herein, was performed with malice and oppression, fraud, and
19 reckless indifference.” *Id.* ¶ 122. Under well-established California law, “[i]f the same conduct
20 is alleged to be both [a violation of one law] and an ‘unfair’ business act or practice for the same
21 reason ... the determination that the conduct is not [otherwise unlawful] necessarily implies that
22 the conduct is not ‘unfair’ toward consumers.” *Chavez v. Whirlpool Corp.*, 93 Cal. App. 4th 363,
23 375 (2001). As another court succinctly summarized it: “[t]he UCL does not apply if the
24 Legislature has expressly declared the challenged business practice to be lawful in other statutes.”
25 *Lazar v. Hertz Corp.*, 69 Cal. App. 4th 1494, 1505-06 (1999). Here the CDA expressly declares
26 the challenged practice to be lawful. Accordingly, the UCL does not apply, Holomaxx’s claim
27 fails and it should be dismissed.
28

1 7. **Holomaxx Fails To State A Claim For Defamation And False Light.**

2 In addition to claims arising from Microsoft’s alleged blocking of Holomaxx’s e-mails to
3 Microsoft e-mail users, in its Seventh and Eighth Claims Holomaxx asserts claims for defamation
4 and false light. Holomaxx seeks to ground these claims entirely on a single statement that
5 Microsoft allegedly made to Dragon Networks, the company operating the datacenter hosting
6 Holomaxx’s services. According to Holomaxx, after blocking Holomaxx’s IP addresses,
7 Microsoft allegedly informed Dragon Networks that the IP addresses had been rejected “for
8 policy reasons” “or for spamming.” Compl. ¶ 45. These allegations are insufficient to support
9 claims for defamation or false light and must be dismissed. *See Knievel v. ESPN*, 393 F.3d 1068,
10 1073-74 (9th Cir. 2005) (granting motion to dismiss; “It is for the court to decide [whether a
11 statement is actionable defamation] in the first instance as a matter of law.”) (citation omitted).

12 “[D]efamation ‘involves the intentional publication of a statement of fact which is false,
13 unprivileged, and has a natural tendency to injure or which causes special damage.’” *Price v.*
14 *Stossel*, 620 F.3d 992, 998-99 (9th Cir. 2010) (quoting *Gilbert v. Sykes*, 147 Cal. App. 4th 13
15 (2007)). Relatedly, to establish a claim for false light, Holomaxx must show that (i) Microsoft
16 disclosed to one or more persons information about or concerning Holomaxx that was presented
17 as factual but that was actually false or created a false impression about Holomaxx; (ii) the
18 information was understood by one or more persons to whom it was disclosed as stating or
19 implying something highly offensive that would have a tendency to injure Holomaxx’s
20 reputation; (iii) establish that Microsoft acted with constitutional malice; and that (iv) Holomaxx
21 was injured by the disclosure. *See Solano v. Playgirl, Inc.*, 292 F.3d 1078, 1082 (9th Cir. 2002)
22 (citing *Fellows v. Nat’l Enquirer, Inc.*, 42 Cal. 3d 234 (1986); Restatement (Second) of Torts §
23 652E [1976]).

24 Plaintiff falls far short of establishing these necessary elements. Holomaxx claims that
25 after allegedly blocking IP addresses hosted at Dragon Networks, Microsoft allegedly informed it
26 that it had done so because the IP addresses “had been rejected ‘for policy reasons,’ and were
27 blocked manually ‘or for spamming.’” Compl. ¶ 45. In order to be defamatory, Holomaxx, at a
28

1 minimum, would have to provide factual allegations that the statement that its IP addresses had
2 been rejected for “policy reasons” “or for spamming” was false. Holomaxx does not do so.

3 To the contrary, the Complaint establishes that the allegedly defamatory statements were
4 not false. In Paragraph 34, for instance, Holomaxx alleges that Microsoft blocked e-mails “based
5 on the recommendations of [its] SmartScreen filter.” *Id.* ¶ 34. Thus, Holomaxx itself recognizes
6 that the e-mails were blocked for “policy reasons” implemented through the SmartScreen filter.
7 Similarly, Holomaxx admits that Microsoft blocked e-mails on the basis that Microsoft believed
8 the e-mails contained “spam-like characteristics.” *Id.* ¶¶ 31, 33-34. Again, Holomaxx alleges
9 that the reason for Microsoft’s blocking was for spamming.

10 Holomaxx goes to great lengths to say that it is not a spammer. As the *e360Insight* court
11 noted, “[s]ome, perhaps even a majority in this country” would disagree, as that term refers
12 generally to the business in which Holomaxx engages. 546 F. Supp. 2d at 605, 607 (discussing
13 bulk e-mails “whether you call them spam or mass marketing mailings”); *see also Gordon v.*
14 *Virtumundo, Inc.*, 575 F.3d 1040, 1045 n.1 (9th Cir. 2009) (the term “spam ... does not have a
15 precise definition” and may “refer broadly” to forms of “junk e-mail”). Thus, at best, the alleged
16 statement that e-mail was filtered “for spamming” reflects a subjective opinion about the
17 objectionable nature of the e-mail, not statements of fact that are provably false. Indeed, given
18 that the alleged statement describes CDA-protected e-mail filtering, the conclusion that it reflects
19 a subjective opinion is inescapable. *See Knievel*, 393 F.3d at 1075 (“The context in which the
20 statement appears is paramount in our analysis, and in some cases it can be dispositive.”). Thus,
21 dismissal is warranted.⁵ *See Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 20 (1990) (no
22 defamation where a statement “cannot reasonably be interpreted as stating actual facts” that are
23 provably false); *Dodds v. Am. Broadcasting Co.*, 145 F.3d 1053, 1065 (9th Cir. 1998) (dismissing
24 defamation claim; statement that plaintiff engaged in “wrongful” conduct and implication that he

25
26 ⁵ Holomaxx vaguely attempts to suggest that Microsoft accused it of a crime, yet fails
27 completely to allege any criminal accusation much less any statement that Holomaxx violated any
28 law. Compl. ¶ 47. The statement that emails were filtered for “policy reasons” “or for spamming”
could not be reasonably interpreted as a criminal accusation. *Knievel*, 393 F.3d at 1074 (claim
dismissed where, in context, a term was not “reasonably susceptible” to interpretation as a
criminal accusation).

1 was unfit for his job “are not assertions of fact and thus cannot be proved to be false”; defendant
2 “was expressing an opinion” protected by the First Amendment)

3 But the Court need not reach that determination in order to dismiss Plaintiff’s defamation
4 claim. The Complaint alleges that Microsoft *did* allegedly block Holomaxx’s IP Addresses “for
5 spamming.” Holomaxx says nothing to the contrary. The statement complained of is true, based
6 on Holomaxx’s own allegations. And in any event, Holomaxx alleges that its IP addresses were
7 filtered “for policy reasons” “or for spamming.” Compl. ¶ 45 (emphasis added). The disjunctive
8 “or” plainly means that the allegedly defamatory statement was not false if Microsoft *either*
9 blocked Holomaxx’s IP addresses for policy reasons *or* blocked them for spamming. Holomaxx
10 repeatedly alleges that Microsoft blocked Holomaxx’s IP addresses as sending e-mail that was
11 inconsistent with the SmartScreen filter and the policies it implements. Compl. ¶¶ 31, 33, 34, 72,
12 81, and 92. Thus, on the face of the Complaint, the statement at issue is true. Plaintiff’s
13 defamation and false light claims fall accordingly.⁶

14 **IV. CONCLUSION**

15 For the foregoing reasons, Microsoft respectfully requests that Plaintiff Holomaxx’s
16 Complaint be dismissed in its entirety. Microsoft further requests that the Complaint be
17 dismissed with prejudice due to the futility of Holomaxx’s claims.

18 Dated: December 17, 2010

GABRIEL M. RAMSEY
Orrick, Herrington & Sutcliffe LLP

20 _____
/s/ Gabriel M. Ramsey

GABRIEL M. RAMSEY
Attorneys for Defendant
MICROSOFT CORPORATION

25 _____
26 ⁶ Further, because Holomaxx’s false light claim is premised on allegedly defamatory statements,
27 it is subsumed within the defamation claim and dismissed as a separate claim. *Selleck v. Globe*
28 *Int’l*, 166 Cal. App. 3d 1123, 1136 (1985) (“plaintiff’s libel claim provides him with a complete
remedy for any damages he has suffered...the second cause of action is, in effect, a duplication of
the first and hence must be dismissed as surplusage”); *Dworkin v. Hustler Magazine*, 867 F.2d
1188, 1193 n.3 (9th Cir. 1989) (“to survive as a separate cause of action, a false light claim must
allege a nondefamatory statement”).