

1 Paul R. Kiesel, Esq. (SBN 119854)
KIESEL BOUCHER LARSON LLP
2 *kiesel@kbla.com*
3 8648 Wilshire Boulevard
4 Beverly Hills, CA 90211
5 Telephone: (310) 854-4444
6 Facsimile: (310) 854-0812
7 **Interim Liaison Counsel**

8 Edward D. Robertson, Jr.
9 Stephen M. Gorny
10 James P. Frickleton
11 Mary D. Winter
12 Edward D. Robertson III
13 *chiprob@earthlink.net*
14 **BARTIMUS, FRICKLETON,**
15 **ROBERTSON & GORNY, P.C.**
16 11150 Overbrook Road, Suite 200
17 Leawood, KS 66211
18 Tel: 913-266-2300
19 Fax: 913-266-2366
20 **Interim Co-Lead Counsel**

David A. Straite (admitted *pro hac vice*)
Ralph N. Sianni
Michele S. Carino
Lydia E. York
dstraite@stewartslaw.com
STEWARTS LAW US LLP
1201 North Orange Street, Suite 740
Wilmington, DE 19801
Tel: 302-298-1200
Fax: 302-298-1222
Interim Co-Lead Counsel

13
14
15 UNITED STATES DISTRICT COURT
16 NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

17
18 IN RE: FACEBOOK, INC. INTERNET
19 TRACKING LITIGATION

Case No. 5:12-md-02314-EJD

20 **[CORRECTED] PLAINTIFFS’**
21 **OPPOSITION TO DEFENDANT’S**
22 **MOTION TO DISMISS PLAINTIFFS’**
23 **CORRECTED FIRST AMENDED**
24 **CONSOLIDATED CLASS ACTION**
25 **COMPLAINT**

Judge: Hon. Edward J. Davila
Date: October 5, 2012
Time: 9:00 a.m.
Crtrm.: 4

Trial Date: None

TABLE OF CONTENTS

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 iii-vii

I. INTRODUCTION..... 1

II. SUPPORTING FACTS..... 3

 A. Facebook violated its own policies and the law..... 3

 B. How Facebook Tracks Its Users..... 5

III. STANDARD OF REVIEW 8

IV. ARGUMENT 9

 A. Plaintiffs’ Allegations Confer Article III Standing 9

 1. Facebook’s Statutory Invasions Give Rise to an Injury in Fact..... 9

 2. Plaintiffs Have Alleged Injury In Fact with Sufficient Specificity..... 10

 3. Plaintiff Davis’ Litigation Cost’s Establish Standing. 11

 B. THE FAC STATES FRAUD WITH PARTICULARITY..... 11

 C. THE COMPLAINT STATES A CLAIM UNDER THE WIRETAP ACT..... 13

 1. Facebook “Intercepted” Plaintiffs’ Communications..... 13

 2. Facebook Intercepted the “Contents” of Communications..... 15

 3. Facebook Used a “Device” to Intercept Communications..... 17

 4. Facebook Was Not a Party to the Intercepted Communications..... 17

 5. Neither Plaintiffs Nor the Third-Party Websites They Visited
 “Consented” to the Interceptions..... 18

 D. THE COMPLAINT STATES A CLAIM UNDER CALIFORNIA’S
 INVASION OF PRIVACY ACT, PENAL CODE § 631..... 21

 1. The Statute Was Designed to Cover Advances in Technology, Which
 Include Electronic Communications..... 22

 2. Plaintiffs Did Not Know Facebook Was Tracking Them; Therefore
 Facebook was not a Participant to the Communication..... 23

 3. Plaintiffs’ Allegations Satisfy the Statutory Prerequisites..... 23

 4. Plaintiffs Aver that Facebook Knew The Contents Of The Data It
 Retrieved 24

 E. THE COMPLAINT STATES A CLAIM UNDER THE STORED
 COMMUNICATIONS ACT..... 24

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

F. THE COMPLAINT STATES A CLAIM UNDER PENAL CODE § 502 (COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT) 25

1. The Allegations Show Facebook Tracked Post-Logout Without Permission. 26

2. The FAC Alleges that Facebook Unlawfully Accessed Plaintiffs’ Computers and Data. 27

3. The FAC Alleges that Facebook’s Cookies are Contaminants. 27

4. Damages and Losses. 27

G. THE FAC STATES A CLAIM UNDER THE UCL. 28

1. Plaintiffs Pled Economic Injury. 28

2. Plaintiffs Have Alleged a Predicate Violation. 28

H. THE COMPLAINT STATES A CLAIM UNDER THE CONSUMER LEGAL REMEDIES ACT. 29

I. THE COMPLAINT STATES A CLAIM FOR CONVERSION. 31

J. THE COMPLAINT STATES A CLAIM FOR TRESPASS TO CHATTELS. 32

K. THE COMPLAINT STATES A CLAIM FOR INTRUSION UPON SECLUSION. 32

1. Plaintiffs Had Objectively Reasonable Expectation Of Seclusion Or Solitude. 33

2. Intrusion Was In A Manner Highly Offensive To A Reasonable Person. 33

L. PLAINTIFFS WITHDRAW THEIR CLAIM UNDER THE COMPUTER FRAUD AND ABUSE ACT. 34

V. CONCLUSION 35

1 **TABLE OF AUTHORITIES**

2 **Cases**

3 *Amati v. City of Woodstock, Ill.*, 829 F. Supp. 998 (N.D. Ill. 1993) 34

4 *Annis v. Tomberlin & Shelnutt Associates, Inc.*, 195 Ga. App. 27, 392 S.E.2d 717 (1990) 32

5 *Ashcroft v. Iqbal*, 556 U.S. 662 (2009) 8, 11

6 *Baugh v. CBS, Inc.*, 828 F. Supp. 745 (N.D. Cal. 1993) 33

7 *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007) 8, 11

8 *Bell v. Hood*, 327 U.S. 678 (9th Cir. 1946) 11

9 *Binkley v. Loughran*, 714 F. Supp. 776 (M.D.N.C. 1989) 34

10 *Bosse v. Crowell Collier and Macmillan*, 565 F.2d 602 (9th Cir. 1977) 12

11 *Brown v. Waddell* 50 F.3d 285 (4th Cir. 1995) 17

12 *Bunnell v. Motion Picture Ass’n of Am.*, 567 F. Supp. 2d 1148 (C.D. Cal. 2007) 16

13 *Burlesci v. Petersen*, 68 Cal.App.4th 1062, 80 Cal.Rptr.2d 704 (1998) 31

14 *Canessa v. J. I. Kislak, Inc.*, 97 N.J. Super. 327 (Law Div. 1967) 30

15 *Cavallaro v. Rosado*, 2006 Conn. Super. LEXIS 2919, 2006 WL 2949143 (Conn. Super. Ct.
16 Oct. 5, 2006) 34

17 *Chance v. Avenue A*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) 15, 22

18 *Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29 (2007) 27

19 *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855 (N.D. Cal. 2011) 23

20 *Comm. on Children’s Television, Inc. v. Gen. Foods Corp.*, 35 Cal.3d 197 (1983) 12

21 *Conant v. Karris*, 165 Ill. App. 3d 783, 117 Ill. Dec. 406, 520 N.E.2d 757 (1987) 32

22 *Conway v. Geithner*, 2012 WL 1657156 (N.D. Cal. 2012) 19

23 *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311
(D.D.C. 2011) 25

24 *Cozzolino v. Maricopa County*, 2006 U.S. Dist. LEXIS 44567, 2006 WL 1794761 (D. Ariz.
25 June 27, 2006) 34

26 *Crispin v. Christian Audiger, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal.) 25

27 *Datacomm Interface, Inc. v. Computerworld, Inc.*, 396 Mass. 760, 489 N.E.2d 185 (1986) 32

28 *Deteresa v. American Broadcasting Cos., Inc.*, 121 F.3d 460 (9th Cir. 1997) 33

1 *Dietemann v. Time, Inc.* 449 F.2d 245 (9th Cir. 1971) 33

2 *Doe I v. AOL LLC*, 719 F. Supp. 2d 1102 (N.D. Cal. 2010) 30

3 *Doe v. City and County of San Francisco*, 2012 WL 2132398, (N.D. Cal. Jun. 12, 2012) 25

4 *eBay, Inc., v. Bidder’s Edge*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000)..... 32

5 *Edwards v. First American Corp.*, 610 F.3d 514, 516-517 (9th Cir. 2010)..... 10, 11

6 *Erickson v. Pardus*, 551 U.S. 89 (2007)..... 9

7 *Facebook, Inc. v. ConnectU, LLC*, 489 F.Supp.2d 1087 (N.D. Cal. 2007) 27

8 *Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750 (N.D. Cal. 2010) 27

9 *Farmers Ins. Exch. v. Zerlin*, 61 Cal.Rptr.2d 707 (1997) 31

10 *Farmers Ins. Exchange v. Superior Court*, 2 Cal.4th 377 (1992) 13

11 *Ferrington v. McAfee, Inc.*, WL 3910169 (N.D. Cal. Oct. 5, 2010) 31

12 *FMC Corp. v. Capital Cities/ABC, Inc.*, 915 F.2d 300 (7th Cir. 1990) 32

13 *Fowler v. Southern Bell Tel. & Tel. Co.*, 343 F.2d 150 (5th Cir. 1965)..... 34

14 *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011) 29

15 *Gaos v. Google Inc.*, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) 10

16 *Gelbard v. United States*, 408 U.S. 41 (1972)..... 14

17 *In re Apple iPhone Application Litigation*, 2012 WL 2126351 (N.D. Cal. June 12, 2012)..... 18, 31

18 *In re Application of the United States for an Order Authorizing the use of a Pen Register and*
Trap, 396 F.Supp.2d 45 (D. Mass. 2005)..... 17

19 *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D. N.Y. 2001)..... 15, 22

20 *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705 (N.D. Cal. 2011)..... 10, 18

21 *In re Ins. Brokerage Antitrust Litig.*, 579 F.3d 241 (3d Cir. 2009)..... 11

22 *In re iPhone App. Litig.*, 2011 WL 4403963 (N.D. Cal. Sep. 20, 2011)..... 11

23 *In re JetBlue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y 2005) 11

24 *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003) 14, 15, 17, 19

25 *In re Toys ‘R’ Us, Inc., Privacy Litigation*, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001)..... 21

26 *Jewel v. Nat’l Sec. Agency*, 673 F.3d 902 (9th Cir. 2011) 11

27 *Konop v. Hawaiian Airlines, Inc.* 302 F.3d 868 (9th Cir. 2002)..... 14

28

1	<i>Kremen v. Cohen</i> , 337 F.3d 1024 (9th Cir. 2003).....	32
2	<i>Kwikset Corp. v. Superior Court</i> , 51 Cal.4th 310 (2011).....	28, 29
3	<i>LaCourt v. Specific Media, Inc.</i> , 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011)	11, 23
4	<i>Lopez v. Smith</i> , 203 F.3d 1122 (9 th Cir. 2000)	9
5	<i>Love v. United States</i> , 915 F.2d 1242 (9 th Cir. 1988).....	9
6	<i>Low v. LinkedIn Corp.</i> , 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011).....	11
7	<i>Lujan v. Nat’l. Wildlife Fed.</i> , 497 U.S. 871 (1990).....	11
8	<i>Luken v. Edwards</i> , 2011 U.S. Dist. LEXIS 47545 (N.D. Iowa May 3, 2011)	34
9	<i>Maya v. Centex</i> , 658 F.3d 1068 (9th Cir. 2011).....	11, 12
10	<i>Mortenson v. Bresnan Communications, LLC</i> , 2010 WL 5140454 (D. Mont. 2010).....	15
11	<i>Motschenbacher v. R. J. Reynolds Tobacco Co.</i> , 498 F.2d 821 (9 th Cir 1974).....	30
12	<i>Native Village of Kivalina v. ExxonMobil Corp.</i> , 663 F. Supp. 2d 863 (N.D. Cal. 2009).....	12
13	<i>People v. Lawton</i> , 48 Cal. App. 4th Supp. 11 (1996).....	27
14	<i>People v. Suite</i> , 101 Cal. App. 3d 680 (1980).....	23
15	<i>Ribas v. Clark</i> , 38 Cal. 3d 355 (Cal. 1985)	34
16	<i>Rogers v. Ulrich</i> , 52 Cal. App. 3d 894 (1975)	24
17	<i>Rubio v. Capital One Bank</i> , 613 F.3d 1195 (9th Cir. 2010).....	29
18	<i>Sanders v. American Broadcasting Companies</i> , 20 Cal. 4th 907 (Cal. 1999)	33
19	<i>Scott v. Kuhlmann</i> , 746 F.2d 1377 (9 th Cir. 1984)	19
20	<i>Skinner v. Switzer</i> , 562 U.S. ___, 131 S. Ct. 1289 (2011)	8
21	<i>Smith v. Capital One Fin. Corp.</i> , 2012 U.S. Dist. LEXIS 66445 (N.D. Cal. May 11, 2012)	33
22	<i>Southern California Housing Rights Center v. Los Feliz Towers Homeowners Ass’n.</i> , 426 F.Supp.2d 1061 (C.D.Cal. 2005).....	29
23		
24	<i>Starr v. Baca</i> , 652 F.3d 1202, 12 (9 th Cir. 2011).....	9
25	<i>Steel Co. v. Citizens for a Better Env’t</i> , 523 U.S. 83 (1998).....	12
26	<i>Taus v. Loftus</i> , 40 Cal. 4th 683 (Cal. 2007)	34
27	<i>Tavernetti v. Super. Ct.</i> , 22 Cal. 3d 187 (1978)	23
28	<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir. 2004).....	24

1 *Turnbull v. ABC*, 2004 U.S. Dist. LEXIS 24351 (C.D. Cal. Aug. 19, 2004)..... 33

2 *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) 16

3 *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008) 16

4 *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. Cal. 2007) 33

5 *United States v. Peden*, 2007 U.S. Dist. LEXIS 61354 (E.D. Cal. Aug. 9, 2007) 33

6 *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010)..... 16

7 *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011) 23

8 *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097 (9th Cir. 2003)..... 9, 12

9 *Warden v. Kahn*, 99 Cal. App. 3d 805 (1979)..... 24

10 *Warth v. Seldin*, 422 U.S. 490 (1975) 10, 11

11 *Weingand v. Harland Financial Solutions, Inc.*, 2012 WL 2327660 (N.D. Cal. 2012)..... 27

12 **Statutes**

13 18 U.S.C. §2701 25

14 18 U.S.C. §2510 14, 17

15 18 U.S.C. §2511 18

16 Cal. Civ. Code § 1760 30, 31

17 Cal. Penal Code §502 26, 27, 28

18 Cal. Penal Code §630 22

19 Cal. Bus. & Prof. Code §17200..... 28, 29

20 Hong Kong Personal Data (Privacy) Ordinance, Ord. No. 81 of 1995 (amended June 27,
21 2012)..... 2

22 Japan's Personal Information Protection Law, Law No. 57 of 2003..... 2

23 Directive 95/94/EC of the European Parliament and the Council of 24 October 1995 on the
24 Protection of Individuals with Regard to the Processing of Personal Data and on the
25 Free Movement of Such Data..... 2

26

27

28

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

Other Authorities

Lori Andrews, "I Know Who You Are and I Saw What You did: Social Networks and the Death of Privacy" (2012)..... 2

Rory Cellan-Jones, "Web Creator Rejects Net Tracking," BBC News (Mar 17, 2008) 2

William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (July 1, 1997)..... 2

Senator John Kerry, "We Need a Commercial Privacy Bill of Rights," *Think Progress Justice Blog* (Mar. 21, 2012) 2

Peter Maas "Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless," www.wired.com (June 28, 2012). 3

Kashmir Hill, "The FTC, 'Your Privacy Watchdog,' Does Have Some Teeth," *Forbes* (June 29, 2012)..... 3

Joseph Turow, *et al.*, "Contrary to What Marketers Say, Americans Reject Tailored Advertising" (Sept. 2009)..... 2

Douglas Wood, "The Importance of Self-Regulation in Improving Digital Privacy," *Corporate Counsel* (July 10, 2012) 2

C. Wright, A. Miller, *Federal Practice and Procedure*, § 1277 19

Nature of Property or Rights Other than Tangible Chattels Which May Be Subject of Conversion, 44 A.L.R.2d 927 (1955)..... 32

Prosser & Keeton on the Law of Torts § 117 (5th ed. 1984) 34

Restatement (Second) of Torts § 256 (1965) 33

Rules

Fed. R. Civ. P. 8 8

Fed. R. Civ. P. 9(b)..... 12

Fed. R. Civ. P. 12(b)(6)..... 9

1 **I. INTRODUCTION**

2 Online advertisers and social media companies now track our every move over the internet and
3 create remarkably detailed profiles that Professor Lori Andrews calls our alternative “digital selves.”
4 See Lori Andrews, “I know Who You Are and I Saw What You Did: Social Networks and the Death
5 of Privacy” (2012). Websites routinely place cookies on our computers when we surf the web,
6 ostensibly to assist with identifying the user upon re-visits. Recently, however, these “tracking”
7 cookies are being packaged with referrer headers and other information to track, in real time, our
8 cyberspace destinations and the search terms we use to find them. Then our computers – usually
9 without our knowledge – are programmed to transmit this data to aggregators for targeted
10 advertising. That business model – part of Mark Zuckerberg’s “Holy Grail” – becomes increasingly
11 profitable the more data these companies gather about us. As U.S. Senator John Kerry said, “[t]hat’s
12 not just invasive – it’s a little creepy.” Sen. John Kerry, “We Need a Commercial Privacy Bill of
13 Rights,” *Think Progress Justice Blog* (Mar. 21, 2012).

14 Cookies were not originally meant for web tracking. Even Sir Tim Berners-Lee, the MIT
15 researcher who helped to invent the web, expressed deep concern about the new practice. See Rory
16 Cellan-Jones, “Web Creator Rejects Net Tracking,” BBC News (Mar. 17, 2008). In 2009, researchers
17 at the University of Pennsylvania and the Berkeley Center for Law and Technology released the first
18 independent study on public reaction to being tracked online. They established that 66% of
19 Americans were uncomfortable with web tracking. The number rose to 86% “when Americans are
20 informed of three common ways that marketers gather data about people in order to tailor ads.” See
21 Joseph Turow, *et al.*, “Contrary to What Marketers Say, Americans Reject Tailored Advertising”
22 (Sept. 2009).

23 To offer citizens at least some fixed level of digital privacy and data protection, most of the
24 developed world relies on a system of national (or even regional) government rules, often modeled on
25 the European Union’s Data Protection Directive.¹ The United States, in contrast, has no general

26 _____
27 ¹ See Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the
28 (footnote continued)

1 national digital privacy or data protection law, and largely relies on a porous system of contract-based
2 self-regulation. *See, e.g.*, Douglas Wood, “The Importance of Self-Regulation in Improving Digital
3 Privacy,” *Corporate Counsel* (July 10, 2012). Indeed, the very first principle of President Clinton’s
4 landmark 1997 *Framework for Global Economic Commerce* clearly states that “governments should
5 encourage industry self-regulation and private-sector leadership.” President William J. Clinton &
6 Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (July 1, 1997).
7 Economic actors decide among themselves the extent to which privacy is to be protected. But the
8 agreements are meaningless without enforcement. As President Clinton said, “[i]t is essential,
9 therefore, to ensure personal privacy in the networked environment” and “consumers are entitled to
10 redress if they are harmed by improper use or disclosure of personal information.” *Id.* at Section II.5.

11 *Forbes* magazine recently noted that enforcement of our country’s digital privacy self-
12 regulation framework rests on a three-legged stool, consisting of federal enforcement by the Federal
13 Trade Commission, state enforcement by States Attorneys General, and private enforcement largely in
14 the form of privacy class actions. Kashmir Hill, “The FTC, ‘Your Privacy Watchdog,’ Does Have Some
15 Teeth,” *Forbes* (June 29, 2012). The FTC’s enforcement efforts in this area are routinely mocked in the
16 press² and in popular culture,³ and of course State Attorney General efforts are limited to state laws
17 that have largely not kept pace with the pace of technology. That leaves private enforcement as the

18 _____
19 Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement
20 of Such Data; *see also* Australia’s Privacy Act 1988 (amended in 2000 to cover the private sector
21 broadly consistent with the EU Data Directive); Hong Kong Personal Data (Privacy) Ordinance, Ord.
22 No. 81 of 1995 (amended June 27, 2012) (broadly consistent with the EU Directive); Japan’s Personal
Information Protection Law, Law No. 57 of 2003.

23 ² *See, e.g.*, Peter Maas, “Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless,”
24 www.wired.com (June 28, 2012).

25 ³ *See, e.g.*, commentary by comedian Jon Stewart, host of “The Daily Show,” noting on April 18,
26 2012 that a recent fine against Google, Inc. for stealing personal information leaking from home Wi-Fi
27 routers would be less than the NFL fines players for doing a touchdown dance. Stewart also quipped,
“Google, I am shocked. You stole people’s personal information without their permission? That’s
Facebook’s job.”

1 most important of these three legs.

2 On July 2, 2012, Defendant Facebook asked this Court to dismiss the entirety of Plaintiffs’
3 Complaint that demands Facebook be held accountable for its secret, unauthorized and purposeful
4 tracking of its members’ internet use. In the sections below, Plaintiffs respond to each of Facebook’s
5 early dismissal arguments. But Plaintiffs’ necessarily claim-by-claim opposition should not obscure
6 how extraordinary Facebook’s request, taken as a whole, really is. Facebook asks this Court to hold
7 as a matter of law that no legal remedy exists for the knowing, purposeful tracking of 150 million
8 internet users (800 million globally) without their knowledge or consent. The impact of such a finding
9 on the internet industry and society at large cannot be overstated. Why would any online or
10 telecommunications company ever honor their contracts, terms of use or privacy policies ever again?
11 Without enforcement, how can a system of regulation – let alone self-regulation - work? Facebook
12 asks this Court to remove the third leg from the three-legged stool of privacy enforcement. That
13 request should not be granted.

14 **II. SUPPORTING FACTS**

15 **A. Facebook violated its own policies and the law.**

16 Facebook’s terms of use set not only the users’ reasonable expectation of privacy, but also
17 definitively limit the extent to which Facebook could permissibly track its users’ internet activities.
18 Facebook promised its members that it would not track their personal internet browsing history after
19 they had logged-off of Facebook.⁴ As noted in Plaintiffs’ Corrected First Amended Consolidated
20 Class Action Complaint (“FAC”), ¶16:⁵

21

22

23

24 ⁴ Mischaracterizing plaintiffs’ pleading, which must be read as a whole, and overstating plaintiffs’
25 burden at this initial pleading stage, Facebook’s repeated claim that Plaintiffs rely exclusively on a
26 single entry in Facebook’s help center nonetheless underscores the centrality of that “single entry.” A
contractual promise is no less valid simply because it can be stated clearly on one sentence.

27 ⁵ References to specific paragraphs of the FAC hereinafter designated as “¶ ____.”

28

- 1 1. **Facebook’s online help center:** *Does Facebook use cookies if I don’t have an account*
2 *or have logged out of my account?*⁶ “When you log out of Facebook, we remove the
3 cookies that identify your particular account.”
- 4 2. **Facebook’s online help center:** “*How does Facebook use cookies?*” “We do not use
5 cookies to create a profile of your browsing behavior on third-party sites or to show you
6 ads...”
- 7 3. **Facebook’s data use policy:** “We receive data whenever you visit a game, application,
8 or website that uses Facebook Platform or visit a site with a Facebook feature (such as a
9 social plug-in). *This may include...if you are logged in to Facebook, your user ID.*”
10 (emphasis added).
- 11 4. **Facebook’s privacy policy (April, 22 2010) – Facebook Exhibit C:** “Pre-Approved
12 Third-Party Websites and Applications – In order to provide you useful social
13 experiences off of Facebook, we occasionally need to provide General Information about
14 you to pre-approved third-party websites and applications that use Platform at the time
15 you visit them (*if you are still logged in to Facebook*)...*In addition, if you log out of*
16 *Facebook before visiting a pre-approved application or website, it will not be able to*
17 *access your information.* (emphasis added).

18 Facebook’s own Engineering Director further assured the public that Facebook did not engage
19 in post-log-out tracking: “We’ve said that we don’t do it, and we couldn’t do it without some form of
20 consent and disclosure.”⁷

21 But Facebook secretly did exactly that. Facebook disingenuously responds that its members
22 “generally” authorize Facebook to set cookies. This case, however, is about much more than “the
23 mere use of cookies.” *See* Defendant’s Motion to Dismiss at 6 (hereinafter “MTD at ___”).
24 Facebook’s contention belies basic tenets of privacy expectation. Facebook’s logic is akin to saying
25 that a photographer who shoots a supermodel in a studio has “general” permission to secretly
26 photograph the model in private, without her knowledge and consent, and for the photographer’s
27 pecuniary gain. “General” permission to track while logged in does not permit Facebook to record a
28 user’s activity after log-out, then monetize that surreptitiously obtained data. This is the core of the

24 ⁶ Upon information and belief, Defendant’s Exhibit D to the *Declaration of Sandeep Solanki*, entitled
25 *Data Use Policy* from Sept. 23, 2011, provides a link to the exact help center page Plaintiffs cited in
26 their complaint. Upon information and belief, Defendant’s Exhibit C to the same Declaration, entitled
27 *Privacy Policy* from April 22, 2010, does the same.

28 ⁷ Acohido, Byron, *How Facebook Tracks you across the Web*, USA TODAY, 11/16/11 available at
<http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1>.

1 causes of action alleged in the FAC.

2 **B. How Facebook Tracks Its Users**

3 **1. Cookies Generally**

4 A server is a computer that stores data and makes that data available on the World Wide Web.
5 A browser is a software application that allows a computer to access information on the World Wide
6 Web. A cookie is a small text file created by a server. Some servers send cookies to their users’
7 browsers when the user accesses the server. The browser stores the cookie in a directory on its
8 computer.

9 Cookies often contain a unique identifier. They are helpful to servers because they allow the
10 server to recognize the person or browser. When a user contacts a web server, the users’ browser
11 checks to see if that server has previously set any cookies on the users’ computer. (¶ 39). If there were
12 cookies set by that server, the users’ browser sends those cookies back to the server. The server can
13 then identify the exact person/browser accessing its server.

14 Cookies can be used to track and record specific information on the particular person/browser.
15 For example, some companies set up data logs to record exactly when a person/browser accessed their
16 server and exactly what they did on the server. Ordinarily, a server that has placed a cookie is only
17 able to access that cookie if the user comes back to that same server. It would be the only time that the
18 users’ browser would recognize the server as matching the cookie on its machine.

19 **2. Facebook’s use of the “Like Button” and other Social Plug-ins to track**
20 **users Internet browsing habits on websites other than Facebook.com**

21 Facebook has crafted a way to gain access to its cookies even when a user is on non-Facebook
22 websites. This information is invaluable to Facebook as it can then advertise that it knows what
23 websites its users have visited, when they have visited them, and what precisely the user did on that
24 particular web site. Facebook social plug-ins, including the Facebook “Like Button,” are small
25 symbols that appear on third-party web pages.⁸ Social plug-ins allow users to share the content on

26 _____
27 ⁸ The Like button has a thumbs-up symbol next to the word “Like,” and users may click it in order to
28 (footnote continued)

1 non-Facebook web pages with their Facebook friends. (¶60; MTD at 4, fn. 4).

2 Facebook uses social plug-ins to become aware of its users' internet browsing history on third-
3 party sites. Facebook is able to do this by withholding the code for its social plug-ins from the servers
4 that house them. Instead of giving the server the actual content, Facebook embeds a command in the
5 social plug-in code that forces the user to contact Facebook's server directly in order to obtain the
6 social plug-in code.⁹

7 The process works as follows. First, a user types in a web server's Uniform Resource Locator
8 ("URL") and the user's browser sends a "GET" request to the web server in order to obtain the
9 content of the web page they wish to view. This is shown as step 1 in the diagram below. The user's
10 browser then checks to see if that particular web server has previously set any cookies on its machine.
11 If it has, the user's browser sends the cookie from the user's machine along with the other information
12 from the request to the first web server. Second, the web server sends the content of the web page to
13 the user's browser, see step 2 in the diagram below, without the Facebook content because the web
14 server does not have that content. Next, along with the content of the web page (minus the Facebook
15 content), the web server sends an embedded command to the user's browser (which was created by
16 Facebook) that automatically causes the user's browser to contact Facebook's server in order to
17 receive the content for the Facebook social plug-in,¹⁰ as shown in step 3 below. The user's browser
18 sends that command to the Facebook server, the user's browser does the same browser check to see if
19 the Facebook server has ever placed any cookies on the user's machine, the user's browser finds out
20 that Facebook's server has placed cookies on the user's computer in the past and responds by sending
21 the Facebook server the user's cookie information (that has been sitting in storage on the user's
22 computer), along with all of the information from the electronic communication between the user and

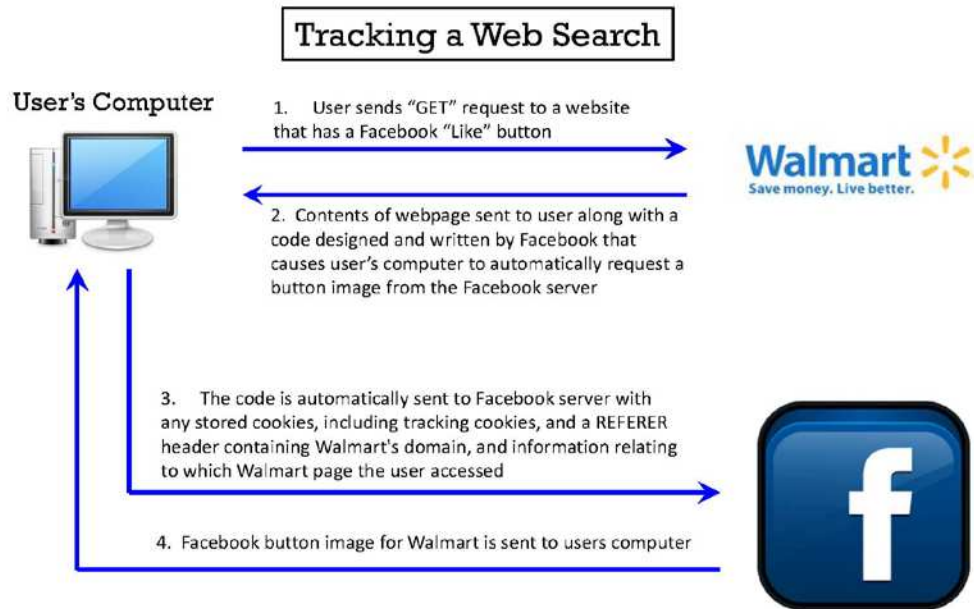
23 _____
24 share their affinity for particular content with their Facebook Friends. See MTD at 4.

25 ⁹ When this happens, the user is completely unaware that they are interacting with Facebook's web
26 server at any point. The command forces the users' computer to communicate with Facebook's server
behind the computer screen where no user can see.

27 ¹⁰ Again, the user is completely unaware they are even interacting with Facebook's server.

28

1 the non-Facebook server.¹¹ Finally, Facebook logs this information and then sends the content of the
2 Facebook social plug-in to the user's browser as shown in step 4 below, and the full web page shows
3 up on the user's screen.¹² This process is illustrated below:



17 The practical implication of this system is that any time a user visits any website with a
18 Facebook social plug-in, even though the user has no intention of sending information to or receiving

19 _____
20 ¹¹ In this scenario, because Facebook is actually a non-party to the communication between the user
21 and the web server, the users computer (because of the command given it by Facebook in the HTML
22 code) sends to the Facebook server the contents of the electronic communication between the user and
23 the web server. The contents of the communication include, but are not limited to: the details of the
24 communication (i.e. any purchases made, any comments posted, any links clicked on, etc.), the URL
25 request from the user to the third-party website, the date of the communication, the time of the
26 communication, the web address of the web pages clicked on, the identification of the content
27 accessed on each page, the characteristics of the user's PC, mobile computer, cell phone, and browser,
28 such as the IP address, universal device identifier ("UDID") on mobile devices, screen resolution,
operating system and browser version.

¹² Facebook actually knows the content of the users' request to the third-party web server before the
user even has a chance to see the full content of the page.

1 information from the Facebook server, the user is forced to interact with the Facebook server, without
2 their knowledge or consent. When the user’s browser interacts with the Facebook server, the browser
3 sends to Facebook’s server the cookies previously embedded by Facebook. These cookies contain
4 personally identifying information. *The browser also sends all of the content from the*
5 *communication the user had with the web site.*

6 **III. STANDARD OF REVIEW**

7 Federal Rule of Procedure 8(a) only requires a plaintiff to plead each claim with sufficient
8 specificity to “give the defendant fair notice of what the ... claim is and the grounds upon which it
9 rests.” *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal quotations omitted). *See*
10 *also Skinner v. Switzer*, 562 U.S. ___, 131 S. Ct. 1289 (2011). (Rule 8(a)(2) requires only short and
11 plain statement of plausible claim, not exposition of legal argument). “A complaint will survive a
12 motion to dismiss when it contains sufficient factual matter, that when accepted as true, states a claim
13 to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662 (2009). Factual content is
14 sufficient when it raises a right to relief above the speculative level. *Twombly*, 550 U.S. at 570; *see*
15 *also Erickson v. Pardus*, 551 U.S. 89 (2007) (decided two weeks after *Twombly*: “[s]pecific facts are
16 not necessary; the statement need only ‘give the defendant fair notice of what the...claim is and the
17 ground upon which it rests’”); *Starr v. Baca*, 652 F.3d 1202, 12 (9th Cir. 2011) (key pleadings tests
18 are (i) “fair notice” of claim and (ii) allegations “sufficiently plausible” to warrant discovery).
19 Facebook’s detailed arguments show Facebook has fair notice of, and knows how to defend against,
20 Plaintiffs’ claims. Facebook’s admission (MTD at 2-3, 5, 6, 11, 24, 26, 28, 34) that it promised *not* to
21 follow users post-logout, and ultimately factual arguments about, for example, what is and is not a
22 proscribed “intercept” under the Wiretap Act, demonstrates that putting Facebook “to the expense of
23 discovery” is not “unfair.” *Id.* A motion to dismiss a fraud claim under Rule 9(b) is the functional
24 equivalent of a motion to dismiss under Rule 12(b)(6) for failure to state a claim. *Vess v. Ciba-Geigy*
25 *Corp. USA*, 317 F.3d 1097, 1107 (9th Cir. 2003).

26 On a 12(b)(6) motion, the court accepts as true all of the complaint’s factual allegations.
27 *Twombly*, 550 U.S. at 555-56. The court must also construe those facts in the light most favorable to
28 the plaintiff. *Love v. United States*, 915 F.2d 1242, 1245 (9th Cir. 1988). If dismissal is appropriate

1 under either Rule 12(b)(6) or (9)(b), the Court should grant leave to amend should unless the
2 allegation of other facts could not possibly cure the defect. *Lopez v. Smith*, 203 F.3d 1122, 1130 (9th
3 Cir. 2000); *Vess*, 317 F.3d at 1108.

4 **IV. ARGUMENT**

5 **A. Plaintiffs’ Allegations Confer Article III Standing.**

6 **1. Facebook’s Statutory Invasions Give Rise to an Injury in Fact.**

7 “The actual or threatened injury¹³ required by Art. III may exist *solely* by virtue of statutes
8 creating legal rights, the invasion of which creates standing.” *Warth v. Seldin*, 422 U.S. 490, 500
9 (1975); *Edwards v. First American Corp.*, 610 F.3d 514, 516-517 (9th Cir. 2010), *cert. granted in*
10 *part*, 131 S. Ct. 3022, 180 L. Ed 2d 843 (2011), *and cert. dismissed as improvidently granted*, No. 10-
11 708, 2012 WL 2427807 (U.S. June 28, 2012); *In re Facebook Privacy Litigation*, 791 F. Supp. 2d
12 705, 711 (N.D. Ca. 2011); *see also Gaos v. Google Inc.*, 2012 WL 1094646 * 2 (N.D. Cal. Mar. 29,
13 2012) (Davila, J.). The standing question in such cases, like this one, is “whether the...statutory
14 provision on which the claim rests properly can be understood as granting persons in the plaintiff’s
15 position a right to judicial relief.” *Id.* The FAC alleges that Facebook intercepted and tracked the
16 electronic communications of each plaintiff in violation of various federal and state statutes.¹⁴ These
17 allegations establish “injury in fact” as a matter of law. *Id.*

18 Contrary to *Warth* and its progeny, Facebook asks the Court to engineer a “two-tiered injury-
19 in-fact” standing test that requires not only the invasion of a statutory right, but some additional harm,
20 presumably economic. But as *Gaos* properly recognized, *Warth* teaches that standing exists where, as
21 here, the alleged invasion is to the plaintiff’s own rights under the statute rather than to some
22 generalized right. *Gaos*, at * 3. *Warth* and *Gaos* did not, as Facebook presupposes, require some

23 _____
24 ¹³ Defendant concedes *sub silentio* that Plaintiffs have sufficiently pleaded Art. III causation and
redressability.

25 ¹⁴ Count I (Wiretap Act), Count II (Stored Communications Act), Count III (Computer Fraud and
26 Abuse Act), Count VIII (California Unfair Competition Law), IX (California Computer Crime Law),
27 Count X (California Penal Code Invasion of Privacy Act), and Count XI (California Consumer Legal
Remedies Act).

1 showing of additional harm, monetary or otherwise. *Gaos* held that the plaintiff had standing *solely*
2 by virtue of a violation of the Stored Communications Act. *Id. In re Facebook* reached the same
3 result. There, this Court found standing where plaintiffs had alleged a violation of the Wiretap Act.
4 *In re Facebook*, 791 F. Supp. 2d at 711-12.¹⁵

5 *Edwards*, in which the plaintiff alleged a violation of the Real Estate Settlement Practices Act
6 but did not allege any resulting monetary harm, makes the point. *Edwards*, 610 F. 3d at 516-17. The
7 Ninth Circuit held that “the damages provision in RESPA gives rise to a statutory cause of action
8 *whether or not* an overcharge occurred.” *Id.* (emphasis added). Thus, the invasion of plaintiffs’
9 statutorily protected rights establishes standing on its own, even absent additional allegations of harm.
10 *Id.*

11 Just as in *Gaos*, Facebook cites no authority¹⁶ holding that injury beyond a personal statutory
12 violation is required to establish standing for a statutory cause of action. *See Gaos*, at *3. The
13 allegations in the Complaint establish Article III standing.

14 **2. Plaintiffs Have Alleged Injury In Fact with Sufficient Specificity.**

15 Impliedly conceding that the invasion of statutory rights gives rise to injury in fact, Facebook
16 retreats to challenging standing with fact based “inspecificity” arguments. (Facebook’s MTD, 7-10).

17
18 ¹⁵ “If Plaintiffs’ here are able to show that Defendant transmitted the contents of users’
19 communications in the manner alleged, they will have effectively demonstrated that
20 all...users...suffered the same injury, which will necessarily mean that each individual Plaintiff will
21 have demonstrated that he was injured.” 791 F. Supp. 2d at 711-712.

22 ¹⁶Among many other distinctions: *In re JetBlue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 327
23 (E.D.N.Y 2005), was a Rule 12(b)(6), not a Rule 12(b)(1) case. A Rule 12(b)(1) motion must clear a
24 much higher hurdle. *See Jewel v. Nat’l Sec. Agency*, 673 F.3d 902, 907 (9th Cir.) (quoting *Lujan v.*
25 *Nat’l. Wildlife Fed.*, 497 U.S. 871, 889 (1990). In *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532
26 (C.D. Cal. Apr. 28, 2011), the plaintiffs did not allege they personally were affected by Defendant’s
27 practices violating specific statutes, and even so the court “probably would decline to say that it is
28 categorically impossible for Plaintiffs to allege some property interest that was compromised by
29 Defendant’s alleged practices,” but “at this point they have not done so.” *DoubleClick*, a Rule
30 12(b)(6) case, did not address standing at all. *In re iPhone App. Litig.*, 2011 WL 4403963 (N.D. Cal.
31 Sep. 20, 2011), recognized that “statutory standing under the Wiretap Act does not require a separate
32 showing of injury.” In *Low v. LinkedIn Corp.*, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011), the
33 plaintiff alleged only “embarrass[ment] and humiliat[i]on” from “disclosure of his personally
34 identifiable browsing history,” which was “valuable personal property.” *Id.* at *3. *Low* did not allege
35 standing from the Defendant’s invasion of his statutorily protected rights.

1 Facebook, however, ignores the longstanding rule that standing has nothing to do with the merits.
2 *See, e.g., Warth*, 422 U.S. at 500 (standing “in no way depends on the merits” of claim of illegal
3 conduct); *Bell v. Hood*, 327 U.S. 678, 682); *Maya v. Centex*, 658 F.3d 1068, 1068. General factual
4 allegations suffice because the Court presumes “that general allegations embrace those specific facts
5 that are necessary to support the claim. *Maya v. Centex*, 658 F.3d 1068, 1068 (citations omitted).¹⁷
6 Thus, plaintiffs need only allege harm at this stage, not, as Defendant argues, *prove* it. *See, e.g.,*
7 *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 89, 94 (1998) (criticizing the dissent for an
8 “attempt to convert the merits issue in this case into a jurisdictional one); *Maya*, 658 F.3d at 1068
9 (different degrees of evidence of standing required at different stages of litigation).

10 **3. Plaintiff Davis’ Litigation Cost’s Establish Standing.**

11 Defendant’s suppositions about plaintiff Davis’s consequential economic damages create at
12 most a factual dispute not susceptible to resolution on a motion to dismiss, while further corroborating
13 plaintiffs’ numerous other bases for standing.¹⁸

14 **B. THE FAC STATES FRAUD WITH PARTICULARITY.**

15 Facebook claims that Rule 9(b) requires the dismissal of plaintiffs’ § 502, UCL and CLRA
16 claims. (MTD at 11). Fraud, however, is not an essential element under either the UCL or the CLRA.
17 *See Comm. on Children’s Television, Inc. v. Gen. Foods Corp.*, 35 Cal. 3d 197, 197 Cal. Rptr. 783,
18 673 P.2d 660 (1983) and *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097 (2003). Additionally, 9(b)
19 requires only that in “all averments of fraud . . . , the circumstances constituting fraud . . . shall be

20 _____
21 ¹⁷ *Maya v. Centex*, 658 F.3d 1060, 1067-68 (9th Cir. 2011), also found that the pleading standards
22 enunciated in the 12(b)(6) cases of *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft*
23 *v. Iqbal*, 556 U.S. 662 (2009), “are ill-suited to application in the constitutional standing context”
24 because merits analysis is inapplicable for analyzing jurisdictional standing question. *See also In re*
Ins. Brokerage Antitrust Litig., 579 F.3d 241, 275 (3d Cir. 2009) “The named plaintiffs **only needed**
to allege that they suffered an injury in fact and were not required to prove the merits of their case
against the Gallagher Defendants to establish standing.” (emphasis added)).

25 ¹⁸ *Native Village of Kivalina v. ExxonMobil Corp.*, 663 F. Supp. 2d 863, 877-78 (N.D. Cal. 2009)
26 found plaintiffs had not alleged that any of the corporate defendants had caused the greenhouse gases
27 that perhaps one day would require villager relocation. Plaintiffs’ claims here are clearly more direct.
Nor need plaintiff allege Art. III causation with the precision required to demonstrate proximate
causation. *Id.*

1 stated with particularity.” Fed. R. Civ. P. 9(b) (emphasis added). Rule 9(b) imposes no heightened
2 pleading burden for non-fraud allegations. *Vess*, 317 F.3d at 1104. Where, as here, fraud is not the
3 sole element of the claim, only the allegations of fraudulent conduct must comport with Rule 9(b),
4 which plaintiffs’ allegations do. *Vess*, 317 F.3d at 1105.

5 “Rule 9(b)...only requires the identification of the circumstances constituting fraud so that the
6 defendant can prepare an adequate answer from the allegations.” *Bosse v. Crowell Collier and*
7 *Macmillan*, 565 F.2d 602, 611 (9th Cir. 1977). Asserting that the “who, what, when, where and how
8 of the misconduct charged,” is unpleaded (MTD at 11), Facebook ignores FAC ¶¶10-102, where
9 plaintiffs document the who,¹⁹ what,²⁰ when,²¹ where,²² and how²³ regarding Facebook’s fraudulent
10 conduct with great specificity. FAC ¶¶ 178 and 221 also specifically plead facts establishing
11 reasonable reliance on the multiple false statements Facebook made in public pronouncements,
12 policies, and in its privacy statements.

13 Facebook’s argument that plaintiffs failed to plead reliance also fails because plaintiffs’ allege
14 that Facebook does not properly declare its privacy policies (FAC ¶ 97) and used a made-up word
15 (“Honk”) to circumvent P3P software protections. When exposed, Facebook simply said it no longer
16 had a P3P privacy policy. *See* ¶ 100. It then re-engineered its privacy policy to a text statement that
17 would allow it to set its cookies, thereby continuing to deceive the browsers, and ultimately, users.
18 *See* ¶¶101-02. Users rely on their software to protect their privacy. Software relies on truthful
19 statements from manufacturers. Plaintiffs have pled, in detail, the element of reliance.

21 ¹⁹ See ¶¶ 19 (Gregg Stefancik); 29 (Kent Matthew Schoen, Gregory Luc Dingle and Timothy
22 Kendall); 33 (Kendall & Facebook).

23 ²⁰ See ¶¶ 14 (Facebook conditions of membership & tracking cookies), 38-84 (how the tracking
cookie methodology works).

24 ²¹ See ¶ 85, which alleges a long history of privacy abuses. Other dates abound in the complaint
25 describing when discrete acts were taken.

26 ²² See ¶9 denoting the location of Facebook’s company headquarters where it may be inferred the
majority, if not the totality of the conduct at issue, was planned and executed.

27 ²³ See ¶¶ 38-84. In this case the “what” and the “how” are almost synonymous.
28

1 An action based on the UCL “to redress an unlawful business practice ‘borrows’ violations of
2 other laws and treats these violations, when committed pursuant to business activity, as unlawful
3 practices independently actionable under section 17200 *et seq.* and subject to the distinct remedies
4 provided thereunder.” *Farmers Ins. Exchange v. Superior Court*, 2 Cal.4th 377, 383 (1992).
5 Therefore, any other claim in the FAC can serve as the predicate unlawful practice for Plaintiffs’ UCL
6 claim.

7 **C. THE COMPLAINT STATES A CLAIM UNDER THE WIRETAP ACT.**

8 The “paramount object” of the Wiretap Act “is to protect effectively the privacy of
9 communications.” *Gelbard v. United States*, 408 U.S. 41, 48 (1972). Plaintiffs’ FAC validly pleads a
10 valid Wiretap Act Claim because its alleges: (1) Facebook’s surreptitious tracking constituted an
11 “interception;” (2) Facebook intercepted the “contents” of communications; (3) Facebook used a
12 “device” to intercept; (4) Facebook was not a party to the intercepted communication; and (5) neither
13 Plaintiffs nor third-party websites consented to interceptions while Plaintiffs were logged-off of
14 Facebook.

15 **1. Facebook “Intercepted” Plaintiffs’ Communications.**

16 The Wiretap Act defines “intercept” as the “acquisition of the contents of any wire, electronic,
17 or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C.
18 §2510(4). Facebook, however, asks this Court to adopt an illogical definition of intercept supported by
19 neither statute nor case law, or, failing that, to engage in technical fact finding at this pleadings stage.
20 Facebook relies on *Konop v. Hawaiian Airlines, Inc.*, to define “intercept” to mean “to stop, seize, or
21 interrupt in progress or course before arrival.” MTD at 12, citing 302 F.3d 868, 874 (9th Cir. 2002).
22 In *Konop*, the 9th Circuit rejected a Wiretap Act claim where plaintiffs alleged that defendant acquired
23 information out of long term electronic storage on a secured website. The Ninth Circuit held that the
24 “intercept” be made “contemporaneously” with the electronic communication and not while it is in
25 electronic storage. The Court merely found that the dictionary definition of intercept, which Facebook
26 now cites, supported that interpretation. The Ninth Circuit did not, however, usurp legislative
27 authority and rewrite the statute to adopt the much more stringent non-statutory dictionary definition
28 Facebook suggests. *Id.* at 878. Requiring that a Wiretap Act defendant “stop, seize or interrupt” a

1 communication would lead to absurd results, frustrating the purpose of the Act. Under Facebook’s
2 interpretation, a traditional police phone tap would not be qualify because there would be no stopping,
3 seizing or interrupting and the telephone call would go through without delay.

4 The statute’s clear terms only require an “acquisition of contents” and Plaintiffs’ allegations
5 concerning Facebook’s use of persistent tracking cookies satisfy the intercept requirement. *See In re*
6 *Pharmatrak, Inc.*, 329 F.3d 9, 22 (1st Cir. 2003) (contemporaneity requirement may be inapplicable to
7 Wiretap Act cases concerning electronic communications); *Mortenson v. Bresnan Communications,*
8 *LLC*, 2010 WL 5140454 (D. Mont. 2010); *Chance v. Avenue A*, 165 F. Supp. 2d 1153 (W.D. Wash.
9 2001); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 513 (S.D. N.Y. 2001).²⁴ In
10 *Pharmatrak*, the defendant placed cookies on the plaintiffs’ computers to track their web usage on
11 certain pharmaceutical websites. *Pharmatrak* at 13. Upon a plaintiff’s first visit to one of the sites, a
12 persistent cookie was placed on his or her computer. *Id.* On subsequent visits, the defendant used the
13 cookie to relay the plaintiff’s URL strings back to the defendant “simultaneous” to the plaintiff’s
14 transmissions to third-party websites. *Id.* at 22. The *Pharmatrak* Court held that “[e]ven those courts
15 that narrowly read ‘interception’ would find that Pharmatrak’s acquisition was an interception.” *Id.*

16 Plaintiffs’ FAC alleges the same scenario. Facebook obtains the intercepted information in
17 real-time. ¶ 82. Facebook’s receipt is at least contemporaneous, if not simultaneous with the request--

18
19 ²⁴ This case is distinguishable from *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497
20 (S.D.N.Y. 2001) in two very important ways. First, the *DoubleClick* court found it “important to note”
21 that plaintiffs “can easily and at no cost prevent DoubleClick from collecting information from them.
22 They may do this in two ways: (1) visiting the DoubleClick Web site and requesting an ‘opt-out’
23 cookie; and (2) configuring their browsers to block any cookies from being deposited.” *Id.* at 504-05.
24 In the instant case, neither of those options is available to the Plaintiffs because Facebook required
25 tracking cookies to be deposited on users’ computers as a condition of accessing its network while
26 users were logged in; so, Plaintiffs could not block the Facebook cookies nor could the Plaintiffs op-
27 out. More importantly, Facebook assured its users that it would not track them post logout and made
28 affirmative representations that it would delete its tracking cookies when users logged out.

24 Second, the *DoubleClick* court also found it “important to note” that DoubleClick did not track
25 individual users; but rather, “DoubleClick collects information based upon the computer's Web
26 activity, regardless of whether one person or one hundred people happen to use that computer. In the
27 same vein, if one person uses multiple computers, DoubleClick would be unable to identify and
28 aggregate the person's activity on different computers.” *Id.* at n. 7. In the instant case, because
Facebook’s tracking cookies are linked to individual users’ accounts, Facebook did track individual
users (including the Plaintiffs) and identified and aggregated their personal activity.

1 "Facebook actually receives this information before the content of the user's request shows up on the
2 user's screen." ¶¶ 68, 80. As the Court stated in *Pharmatrak*, where the defendant "acquired the same
3 URL query string (sometimes containing personal information) exchanged as part of the
4 communication between the pharmaceutical client and the user", these "separate, but simultaneous
5 and identical, communications satisfy even the strictest real-time requirement." *Pharmatrak*, 329 F.3d
6 at 22.²⁵ *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010), explained that
7 "'contemporaneous' does not mean 'in flight' or 'in the middle' or any football metaphor." *Id.* at 706.
8 **[SENTENCE DELETED IN CORRECTED VERSION]**. Instead, it is "contemporaneous by any
9 standard" when the Wiretap defendant and the victims "receive[] each message with no more than an
10 eyeblink in between." *Id.* See also *Councilman*, 418 F.3d 67 (Wiretap Act's "broad definition of
11 electronic storage was to enlarge privacy protections for stored data . . . not to exclude email message
12 stored during transmission from these strong protections.") *Szymuszkiewicz* thus rejects a reading of
13 interception that imports "stop, seize, or interrupt in progress" requirement, and embraces a reading of
14 "interception" that means taken close in time to the communication. **[UNDERLINED LANGUAGE**
15 **ADDED IN CORRECTED VERSION]**.

16 The same analysis applies to this case. The FAC plead an interception.

17 **2. Facebook Intercepted the "Contents" of Communications.**

18 The Wiretap Act defines "contents" to mean "information concerning the substance, purport,
19 or meaning of the communication." 18 U.S.C. 2510(8). Plaintiffs' FAC (¶¶ 78, 79, 82, 84, 142)
20 alleges the interception of eleven items with each communication: (1) URL strings, including the date
21 and time of each page visited, (2) the identification of the contents accessed on each page, (3) the
22 user's name, (4) age, (5) gender, (6) email address, (7) IP address, (8) universal device identifier, (9)

23

24 ²⁵ *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1152-54 (C.D. Cal. 2007), does not
25 change the result. (Facebook MTD at 12). That Central District of California case did not address
26 persistent tracking cookies. Instead, it dealt with an e-mail re-routing and copying program. 567 F.
27 Supp. 2d. at 1154. Cf. *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005 (en banc) (finding
28 an interception under the Wiretap Act where electronic communication is acquired "during the
momentary intervals, intrinsic to the communication process, at which the message resides in transient
electronic storage.")

1 screen resolution, (10) operating system, and (11) browser. Ultimately, Facebook knows which
2 websites its members visited, when they visited them, and what the member did there.

3 The interception of URL strings alone is the interception of “content.” *United States v.*
4 *Forrester*, 512 F.3d 500, 510, fn. 6 (9th Cir. 2008) (URL constitutes “content” because URL
5 “identifies a particular document within a website that a person views and reveals much more
6 information about a person’s Internet activity”); *In re Application of the United States for an Order*
7 *Authorizing the use of a Pen Register and Trap*, 396 F. Supp. 2d 45 (D. Mass. 2005) (URL constitutes
8 “content” because the “substance” and ‘meaning’ of the communication is that the user is conducting
9 a search for information on a particular topic.”). Facebook cites no contrary authority.

10 URL strings for article pages reveal more content than URLs for search phrases. Consider the
11 URL in the footnote below.²⁶ As with the search phrase, the URL string reveals the information the
12 user is seeking. In addition, by simply following the link, one can see the full contents of the
13 communication back to the user.

14 *Brown v. Waddell* is also instructive. 50 F.3d 285 (4th Cir. 1995). In that case, police
15 investigators obtained permission to track telephone numbers of persons that were “paging” a criminal
16 suspect. The officers also obtained “pager clones” which intercepted additional number codes, one of
17 which indicated that the caller was “en route.” *Id.* at 287-88. The Fourth Circuit held that these
18 additional numbers were “contents” under the Wiretap Act. *Id.* at 294. If numbers on a pager
19 constitute “content,” so too must actual words and numbers contained within a URL string.

20 Plaintiffs’ FAC goes further than necessary, alleging Facebook intercepted more than just URL
21 strings. The FAC also alleges the interception of URL strings commensurate with the long list of
22 personally-identifiable information. *See, e.g.*, ¶ 82.

23
24
25
26
27
28

²⁶ http://www.washingtonpost.com/politics/fda-clears-first-over-the-counter-rapid-test-for-the-virus-that-causes-aids/2012/07/03/gJQAONTsKW_story.html.

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

3. Facebook Used a “Device” to Intercept Communications.

The Wiretap Act defines an “electronic ... device” broadly as “any device or apparatus which can be used to intercept a[n] ... electronic communication.” 18 U.S.C. §2510(5). The ordinary meaning of “device” is “a thing made for a particular purpose” or “a plan or scheme for effecting a purpose.” Random House Dictionary 2012.²⁷ As a matter of law, web servers and computers are “devices.” See *Szymusiewicz* at 707; see also *In re Pharmatrak* at 18-19. No court has ever found that servers, browsers, cookies, or any schemes using them to intercept communications are not “devices.” Plaintiffs’ FAC identifies at least seven devices Facebook uses to illegally track users post log-out: (1) cookies; (2) browsers; (3) computers; (4) Plaintiffs’ servers; (5) Facebook’s servers; (6) the plan or scheme Facebook put together to effect its purpose of tracking users while logged-off; or (7) a combination of all of the above. FAC ¶ 38-84. Plaintiffs have properly pled the “device” element.

4. Facebook Was Not a Party to the Intercepted Communications.

Facebook also argues its secret, post-logout tracking justified. Facebook says it was a party to the communications between its members and third-party websites since plaintiffs’ browsers transmitted communications to Facebook. MTD at 15. But Facebook’s reliance upon *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011) is misplaced. Here, plaintiffs have not alleged that Facebook intercepted communications while plaintiffs were *on* Facebook.com or even while they were surfing the web while *logged-in* to Facebook. Instead, the FAC alleges Facebook tracked plaintiffs when they were *logged-off*, at a time when Facebook promised it would not intercept its members’s communications with other websites and at a time when its members did not intend to send *any* messages to Facebook. It is illogical (and contrary to how courts have interpreted the law) for Facebook to secretly track its members and then claim it was a “party” to any communication. *In re Apple iPhone Application Litigation*, Case No. 11-MD-02250-LHK, *Order Granting in Part and Denying in Part Defendants’ MTD* at 22. (where plaintiffs had not intended any

²⁷ <http://www.dictionary.reference.com/browse/device>

1 communication, a Wiretap Act defendant like Apple “cannot manufacture a statutory exception
2 through its own accused conduct”); *see also Pharmatrak* at 22.

3 **5. Neither Plaintiffs Nor the Third-Party Websites They Visited**
4 **“Consented” to the Interceptions.**

5 *a. The question of consent is not appropriate for a motion to dismiss.*

6 Found separately in 18 U.S.C. §2511(2)(d), the consent exception is an affirmative defense
7 that Facebook bears the burden of establishing. *See Pharmatrak*, 329 F.3d at 19. Thus, it is not
8 appropriately the subject of this motion to dismiss.²⁸ *Scott v. Kuhlmann*, 746 F.2d 1377, 1378 (9th Cir.
9 1984) (citing Wright & Miller, *Federal Practice and Procedure*, § 1277 at 328-30) (affirmative
10 defenses may not be raised in a motion to dismiss unless there are no disputed issues of fact); *Conway*
11 *v. Geithner*, 2012 WL 1657156, at *2 (N.D. Cal. 2012) (citing *Kuhlman* for the same proposition).
12 Facebook’s argument boils down to the remarkable proposition that the FAC does not disprove
13 Facebook’s factually based affirmative defense. No Rule 12(b)(6) cases support such a distortion of
14 plaintiffs’ burden.

15 *b. Facebook’s Members Traded Limited Tracking Rights (while logged-*
16 *in) in Exchange for Facebook’s Service; Members Did not Consent to*
Post Log out Privacy Intrusions.

17 Consent “should not be casually inferred.” *Pharmatrak*, 329 F.3d at 20. A medical patient may
18 consent to one form of treatment and refuse another. A landowner may consent to one trespass but not
19 another. So too may a web user consent to one cookie function but not another. *Id.* at 19.
20 Emphasizing the factual nature of the inquiry, determining consent is, thus, a two-part inquiry. First a
21 court must determine the “dimensions of consent.” *Id.* Then it must “ascertain whether the
22 interception exceeded those boundaries.” *Id.* Facebook’s argument improperly infers consent for *all*
23 tracking based upon a narrow consent agreement it reached with its members for *limited* tracking

24
25
26 ²⁸ Even when a Defendant can prove consent, the Plaintiff may overcome such a showing by proving
27 an exception to the exception – that the interception was done for the “purpose of committing any
28 criminal or tortious act.” 18 U.S.C. §2511(2)(d).

1 during Facebook sessions. The FAC, however, details the boundaries of the plaintiffs’ consent. *See*
2 ¶¶ 16, 17, 21, 25, 86-102, 140, 141.

3 Even Facebook’s hand-selected documents permit the reasonable inference that plaintiffs did
4 not consent to tracking after log out, and that discovery will produce further evidence of lack of
5 consent. The privacy policies of both April 22, 2010 and December 22, 2010 promised users that
6 Facebook would not disclose information about them to “pre-approved” third-party websites after log-
7 out. See Facebook Exhibit C at 4 (“if you log out of Facebook before visiting a preapproved
8 application or website, it will not be able to access your information”). Facebook’s own Engineering
9 Director admitted, in regards to post log-out tracking, “*we couldn’t do it without some form of consent*
10 *and disclosure.*”²⁹ The FAC alleges the absence of that consent, justifying discovery on this highly
11 fact intensive inquiry.

12 c. *Facebook Improperly Asks the Court to Consider Incomplete Evidence*
13 *Outside the Pleadings.*

14 At this pleading stage, Facebook directs the Court to certain hand-selected, incomplete
15 evidence. Facebook, however, has failed to provide the Court with all documents describing its
16 relationship with the plaintiffs. For example, Facebook neglected to provide the Data Use Policy that
17 governed Facebook’s relationship with its members between December 22, 2010 and September 23,
18 2011 – a full nine months of the class period.³⁰ Moreover, Facebook also failed to provide its Help
19 pages—the very representations explicitly assuring its members that Facebook would not track them
20 post- logout.

21
22
23 ²⁹ See [http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-
24 data/51225112/1](http://www.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1). Plaintiffs regret the use of newspaper accounts in this response, but are given little
25 choice since Facebook has moved to dismiss on the issue of consent before Plaintiffs have had the
opportunity to conduct discovery.

26 ³⁰ This document was used as an Exhibit by Facebook in *Ung v. Facebook*, a privacy case in this
27 district in which Facebook was represented by the same counsel. 2011-CV-02829. Formal discovery
may reveal other undisclosed policies.

1 In a misguided effort, Facebook provides CNN.com’s publicly available Privacy Policy³¹. But
2 CNN is just one of thousands of third-party websites that Facebook members visit. To prevail at this
3 early juncture, Facebook must prove consent on the part of every website, not just a select one like
4 CNN.com. Importantly, at this threshold stage, Plaintiffs cannot ascertain how many other documents
5 exist between Facebook and CNN – or any of the other thousands of third-party sites –relevant to the
6 issue of third party consent. Plaintiffs should have the opportunity to conduct discovery on affirmative
7 defenses Facebook has raised to that the trier of fact can assess the matter. The issue of consent is not
8 ripe for consideration.

9 *d. Third Party Web Sites, including CNN.com, Did Not Consent.*

10 Even if it were proper to treat Facebook’s motion as one for summary judgment, Facebook has
11 provided no evidence that *any* third-party web site consented to Facebook’s tracking of logged-out
12 members, let alone that *all* of them consented. In fact, the lone third-party privacy policy Facebook
13 provides disproves its own argument. Facebook’s Exhibit A to the *Declaration of Kyle C. Wong*,
14 CNN.com’s online Privacy Policy, states that “the use of these technologies by these third parties is
15 subject to their own privacy policies and is not covered by this privacy statement.” CNN.com’s
16 privacy policy thus defers to Facebook’s privacy policy for all issues regarding the use of cookies.
17 Because Facebook’s privacy policies prohibit the use of cookies to track personal browsing history
18 after logout, CNN.com’s privacy policy gives Facebook no greater freedom to do so. Indeed other
19 third-party web sites have privacy policies similar to CNN.com which preclude post log-out
20 tracking.³²

21
22 ³¹ This policy was only applicable to a limited part of the class period.

23 ³² Washington Post’s online Privacy Policy: “If personally identifiable information is being provided
24 to and/or maintained by any company other than these, our policy is that we will not transfer that
25 personally identifiable information unless notice is given prior to transfer.” Available at
26 http://www.washingtonpost.com/privacypolicy/2011/11/18/gIQASiiaiN_story_1.html. The New
27 York Times online Privacy Policy states, “if you have registered to use the NYT Services, we will not
28 sell, rent, swap or authorize any third party to use your e-mail address or any information that
personally identifies you without your permission.” Available at
<http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html#e>.

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

e. Consent Cannot be Inferred from Product Use.

Facebook also argues that third-party web site operators consented to post log-out user tracking because they chose to implement Facebook’s social plug-ins and this supposed consent was amorphously “part of the regular process by which third-party websites obtain Facebook content to display on their page.” MTD at 15. However, consent cannot be inferred (particularly at this stage) from the mere use of a product or the creation of a business relationship. *See Pharmatrak*, 329 F.3d at 20. Facebook cites three cases for its argument. All are distinguishable and none establish such a rule.³³

As in *Pharmatrak*, there is before this Court no evidence that third-party websites were aware that Facebook was using social plugins to facilitate tracking in direct contravention of its privacy policy. Further, Facebook’s Statement of Rights and Responsibilities includes a provision “applicable to developers/operators of applications and websites” requiring third-party websites to promise that they will “not give (Facebook) information that (they) independently collect from a user or a user’s content without that user’s consent.”(Facebook Exhibit A, at 3). Accordingly, if third-party websites agreed to Facebook’s post log out tracking, those websites breached their contract with Facebook and have subjected them to liability from their own visitors and users. Just as in *Pharmatrak*, there is no basis to find that third-party web sites consented to Facebook’s interceptions. That is a factual determination that must await discovery.

D. THE COMPLAINT STATES A CLAIM UNDER CALIFORNIA’S INVASION OF PRIVACY ACT, PENAL CODE § 631.

The California legislature wrote California’s Invasion of Privacy Act (CIPA) broadly to “protect the right of privacy” from “advances in science and technology... and the development of

³³ Unlike *In re Toys ‘R’ Us, Inc., Privacy Litigation*, 2001 WL 34517252, at * 7 (N.D. Cal. Oct. 9, 2001) the FAC includes no allegations that suggest such collaboration between third-party websites and Facebook. Further, Facebook’s reliance on *In re Doubleclick, Inc., Privacy Litigation*, 154 F. Supp. 2d 497 (S.D. N.Y. 2001) and *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wa. 2001) is equally misplaced. As the *Pharmatrak* Court stated “*Doubleclick* and *Avenue A* do not set up a rule contrary to the district court’s reading of them, that a consent to interception can be inferred from the mere purchase of a service, regardless of circumstances.” *Pharmatrak*, 329 F.3d at 20.

1 new devices and techniques....” Cal. Penal Code § 630. The Act must be interpreted with this
2 purpose in mind. To further this objective, the Act prohibits “any unauthorized connection” or any
3 attempt to read or learn the contents of any communication by means of “any machine, instrument or
4 convenience, or in any other manner.” Plaintiffs have averred that Facebook used technology to
5 “access, intercept and collect Plaintiffs’ and Class Members’ personally identifiable information and .
6 . . . interactions with certain websites after log-out . . .” See ¶200. Intentionally, see ¶130, Facebook
7 “directly participated in the interception, reading, and/or learning of the contents of the
8 communications between Plaintiffs, Class Members and California-based web entities” without
9 consent. See ¶¶ 103-106, 203, 204 and 208. These allegations provide fair notice of the nature of
10 Plaintiffs § 631 claim.

11 **1. The Statute Was Designed to Cover Advances in Technology, Which**
12 **Include Electronic Communications.**

13 Facebook asks this Court to be the first to hold that the Act excludes electronic
14 communications. Not only is this request contrary to the statute’s purpose and terms, but it is contrary
15 to established law as well. For instance, in *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D.
16 Cal. 2011), customers of an internet service provider alleged that the defendants monitored their
17 online activities in violation of § 631. The Court overruled a motion to dismiss, explaining that the
18 case arose “out of a practice of tracking individuals’ internet habits and harnessing that data to sell and
19 deliver targeted advertisements based on their web browsing history.” *Id.* at 1024. The data retrieved
20 “was used to sell advertising tailored to subscribers’ interests....” These allegations are virtually
21 identical to Plaintiffs’ allegations against Facebook. See ¶¶ 12-14, 31, 200.

22 The authority Facebook cites for this unprecedented concept is inapposite. For example, *People*
23 *v. Suite*, 101 Cal. App. 3d 680 (1980) and *Tavernetti v. Super. Ct.*, 22 Cal. 3d 187 (1978) involve the
24 suppression of telephone evidence in a criminal matter and pre-date the entire issue of internet
25 communications by several decades. *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855 (N.D. Cal.
26
27
28

1 2011), did not even involve the CIPA.³⁴

2 **2. Plaintiffs Did Not Know Facebook Was Tracking Them; Therefore**
3 **Facebook was not a Participant to the Communication.**

4 Facebook claims it is a party to the electronic communication such that § 631 does not apply.
5 The authority Facebook cites, however, shows otherwise. *Rogers v. Ulrich*, 52 Cal. App. 3d 894
6 (1975) and *Warden v. Kahn*, 99 Cal. App. 3d 805 (1979) simply hold that eavesdropping cannot occur
7 when the aggrieved party knows that someone is listening: “only a third party can listen secretly to a
8 private conversation.” *Rogers*, 52 Cal. App. 3d at 899. Here, Plaintiffs allege that Facebook (a third-
9 party) tracked Plaintiffs’ internet browsing activity — communications with other websites — after
10 they were logged out of Facebook without plaintiffs’ knowledge and consent. *See* ¶¶ 15-37, 71-84.
11 This factual scenario states a claim pursuant to § 631.

12 **3. Plaintiffs’ Allegations Satisfy the Statutory Prerequisites.**

13 Facebook asserts that Plaintiffs fail to allege (1) the use of a “machine, instrument or
14 contrivance”; (2) that Facebook made an “unauthorized connection with any telegraph or telephone
15 wire, line, cable or instrument”; and (3) that Facebook obtained the “contents” of any communication.
16 MTD at 18. First, a computer is a machine. A cookie is a “contrivance,” which is defined as “a
17 device, especially a mechanical one” and separately as “a plan or scheme.” Plaintiffs’ FAC ¶ 42
18 alleges that Facebook “implants a number of cookies onto the internet user’s computer.” The cookie
19 is software that carries an electronic plan that allows Facebook to participate in communications
20 between users and others. These allegations are sufficient.

21 The words “connection” and “contents” are similarly broad. Plaintiffs’ FAC ¶¶ 103-106, 203,
22 204 allege an unauthorized connection. “[P]ersonally identifiable information and other data,
23 including information concerning their interaction with certain websites” is “content.” *See* ¶ 200.

24 _____
25 ³⁴ Facebook also cites *Lacourt v. Specific Media*, No. SACV 10-1256-GW, 2011 WL 1661532 C.D.
26 Cal. Apr. 28, 2011), in which the Court comments that application of the Invasion of Privacy Act to
27 the conduct alleged was not “obvious.” (Facebook’s MTD at 17). Since the Court granted leave to
28 amend and did not comment on why it believed the allegations failed to state a claim, this remark is
not particularly instructive.

1 4. **Plaintiffs Aver that Facebook Knew The Contents Of The Data It**
2 **Retrieved**

3 Facebook tracked users’ browsing history and used what it learned to increase advertising
4 revenue. See ¶¶ 12-14, 200. Use of the data requires knowledge of its content. Otherwise, it would
5 have no value.

6 **E. THE COMPLAINT STATES A CLAIM UNDER THE STORED**
7 **COMMUNICATIONS ACT.**

8 “[T]he Stored Communications Act protects individuals’ privacy and proprietary interests.”
9 *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004). It provides a cause of action against:

10 a person who intentionally accesses without authorization a facility
11 through which an electronic communication service is provided, or
12 who 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 storage in such a system.

13 18 U.S.C. § 2701(a)(1). The statute “was enacted because the advent of the Internet presented a host
14 of potential privacy breaches that the Fourth Amendment does not address.” *See Crispin v. Christian*
15 *Audiger, Inc.*, 717 F. Supp. 2d 965, 971 (C.D. Cal.) (citations omitted). The SCA is best interpreted
16 “by considering its operation and purpose in light of the technology that existed in 1986.” *Id.* at 972
17 n.15.

18 Facebook argues that the Complaint fails to allege that it accessed a “facility” and took
19 communications from “electronic storage” and that it nevertheless had authority to do so. When
20 Facebook tracks a member’s internet browsing history, the user’s browser conversation is captured
21 and ultimately transmitted to Facebook, wherein Facebook stores the information permanently. Such
22 electronic storage as the SCA contemplates includes retaining an email on a server after delivery to
23 the recipient. *Doe v. City and County of San Francisco*, No. C10-04700 TEH, 2012 WL 2132398, *2
24 (N.D. Cal. Jun. 12, 2012). Thus, turning temporary information into a permanent record on a third
25 party’s facility is exactly the type of privacy invasion the SCA seeks to prohibit.

26 The SCA does not define “facility.” However, “Congress intended the term to include the
27 physical equipment used to facilitate electronic communications.” *Council on Am.-Islamic Relations*
28

1 *Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 334 (D.D.C. 2011). Here, Plaintiffs allege a
2 detailed system of communications between and among numerous physical means of communication,
3 including the user’s hardware, browser and the Facebook server, which result in Facebook obtaining
4 information the SCA prohibits. *See* ¶¶ 38-84. Regardless, discovery is appropriate to further allow
5 plaintiffs to further demonstrate how these physical means of communication constitute a
6 “facility.” *Gaubatz*, 793 F. Supp. 2d at 336 (denying a motion to dismiss because defendants’
7 argument that plaintiffs’ own office computers are not a facility “may or may not turn out to have
8 merit upon further development of the factual record”).

9 Impliedly conceding that the Act covers its conduct, Facebook retreats to the position that it
10 had permission to violate the Act. This argument is belied by the very assurance Facebook gave to its
11 customers. *See* ¶ 15. Consent to place cookies and track members during log-in in exchange for
12 Facebook access is not tantamount to consent to secretly use those cookies in a manner in which the
13 terms of use prohibited.

14 **F. THE COMPLAINT STATES A CLAIM UNDER PENAL CODE § 502**
15 **(COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT)**

16 By enacting § 502, the California legislature expanded the protection afforded to individuals
17 from unauthorized access to both their personal computers and individual data. Cal. Penal Code §
18 502(a). Pursuant to Section 502 (e)(1), any person who suffers “damage or loss by reason of a
19 violation of any of the provisions of subdivision (c)...” may bring a civil action against the violator.
20 Plaintiffs have asserted claims pursuant to Sections 502(c)(1), (6), and (7) which require allegations
21 that Facebook accessed their computers or data “without permission.” Plaintiffs also assert a claim
22 pursuant to Section 502(c)(8), which requires allegations that Facebook introduced a “contaminant”
23 into their computers. Facebook argues that Plaintiffs have not alleged (1) the absence of permission,
24 (2) unlawful access, (3) that Facebook tracking cookies are contaminants, and (4) cognizable
25 damages.

26
27
28

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. **The Allegations Show Facebook Tracked Post-Logout Without Permission.**

Plaintiffs allege that Facebook lacked permission to keep tracking cookies on Plaintiffs’ computers after logout, see ¶¶ 16, 19, and to access those cookies when Plaintiffs visited third party web sites after logout. *See* ¶¶ 17, 20-25, 103-106.

Facebook contends Plaintiffs consented to post-log out tracking because they generally consented to the use of use of cookies while logged in and “the Privacy Policy does not limit Facebook’s use of cookies based on whether a User is logged in or not.” *See* MTD at 15. Facebook’s argument fails due to its admitted contrary assurances in its online help center. *See* section C.2, *supra*. To the extent Facebook argues that its privacy assurances should be interpreted differently, that is for the trier of fact to decide.

Facebook, like the burglar that found that door unlocked, further argues it cannot have acted “without permission” because it did not overcome any “technical or code-based barriers” to track users after log-out. MTD at 24. That argument is based upon the inapposite *Facebook, Inc. v. Power Ventures, Inc.*, No. C08-05780 JW, 2010 WL 3291750 (N.D. Cal. 2010). *Power Ventures* addressed the concern that web site operators such as Facebook could unilaterally change terms of service anytime, subjecting users to criminal penalties under § 502. *Power Ventures* instituted the “overcoming of technical barriers” requirement to limit criminal liability to users who knowingly gained unauthorized access.

However, *Power Ventures* does not apply where, as here, the web site operator Facebook violates its own published terms of service. As Facebook has argued elsewhere,³⁵ no notice is required to tell Facebook what Facebook itself has done.

³⁵ In *Facebook, Inc. v. ConnectU, LLC*, 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007), Facebook successfully argued during the motion to dismiss stage that ConnectU exceeded the terms and conditions of use and accessed Facebook “without permission.” Facebook is judicially estopped from arguing a contrary position now.

1 **2. The FAC Alleges that Facebook Unlawfully Accessed Plaintiffs’**
2 **Computers and Data.**

3 Section 502 defines access as “to gain entry to, instruct or communicate with the logical,
4 arithmetical, or memory function resources of a computer...” § 502 (b)(1). This is exactly what
5 Facebook did when it tracked its members post logout. Facebook’s reliance upon *Chrisman v. City of*
6 *Los Angeles*, 155 Cal. App. 4th 29 (2007) is misplaced because in *Chrisman* an on duty police officer
7 used a police computer he had permission to use, to obtain information he was authorized to obtain.
8 The Court found that the officer’s actions were legal for these reasons. *Id.* at 35.

9 Unlike *Chrisman*, as soon as the Plaintiffs logged out, Facebook was on notice that its help
10 center promise was operative and that Facebook ***no longer had permission*** to access Plaintiffs’
11 computers. *See People v. Lawton*, 48 Cal. App. 4th Supp. 11, 14 (1996) (“permissible use of
12 hardware to access impermissible levels of software is a violation of that section.”); *see also*
13 *Weingand v. Harland Financial Solutions, Inc.*, 2012 WL 2327660, 2 (N.D. Cal. 2012) (denying
14 motion to dismiss § 502 claim where terminated employee “received permission to access
15 [employer’s] computer system based on his representations that he sought to get his ‘personal files’
16 after his termination, but that he had no authority with respect to the additional files he accessed.”).

17 **3. The FAC Alleges that Facebook’s Cookies are Contaminants.**

18 Facebook argues that its cookies are not contaminants because they are “standard web browser
19 functions.” MTD at 26. However, a “computer contaminant” is “any set of computer instructions that
20 are designed to ... transmit information within a computer, computer system, or computer network
21 without the intent or permission of the owner of the information.” § 502(b)(10). The tracking cookies
22 Facebook implanted on Plaintiffs’ computers were designed and intended to transmit Plaintiffs’
23 information back to Facebook without the owner’s intent or permission. Facebook’s tracking cookies
24 are, therefore, “contaminants” within § 502(b)(10).

25 **4. Damages and Losses.**

26 Plaintiffs have pleaded damages and losses. *See* ¶¶ 109-129. Section 502(e)(1) also allows
27 “compensatory damages,” defined as “any expenditure reasonably and necessary incurred by the
28 owner or lessee to verify that a computer system ... or data was or was not altered, damages, or

1 deleted by the access.” Plaintiffs have pleaded the aforementioned damages and loss which includes
2 retaining a computer expert to investigate Facebook’s unauthorized access to their computer systems
3 and data, see ¶¶ 109-110, and paying for proactive measures designed to prevent Facebook from
4 gaining unauthorized access to Plaintiffs’ computers again. See ¶¶ 128-120.

5 **G. THE FAC STATES A CLAIM UNDER THE UCL.**

6 Facebook argues that Plaintiffs have not (1) suffered an economic injury, (2) pleaded with Rule
7 9(b) specificity,³⁶ (3) alleged a predicate violation, nor (4) satisfied the UCL’s “unfair” prong. MTD at
8 27-29. Like the CLRA, the UCL’s reach is broad and remedial. See, e.g., *Kwikset Corp. v. Superior*
9 *Court*, 51 Cal. 4th 310, 320 (2011) (citing Cal. Bus. & Prof. Code § 17200) (“The UCL prohibits, and
10 provides civil remedies for, unfair competition, which it defines as ‘any unlawful, unfair or fraudulent
11 business act or practice.’ Its purpose is to protect both consumers and competitors by promoting fair
12 competition in commercial markets for goods and services.”). The UCL covers “anything that can
13 properly be called a business practice and that at the same time is forbidden by law.” *Id.* “[U]nder the
14 UCL, standing extends to “a person who has suffered injury in fact and has lost money or property as a
15 result of the unfair competition.” *Id.* at 321-22.

16 **1. Plaintiffs Pled Economic Injury.**

17 Under the UCL, a plaintiff pleads an economic injury by alleging that he “enter[ed] into a
18 transaction, costing money or property, that would otherwise have been unnecessary.” *Kwikset Corp.*,
19 51 Cal.4th at 323; *Southern California Housing Rights Center v. Los Feliz Towers Homeowners Ass’n.*,
20 426 F. Supp. 2d 1061, 1069 (C.D. Cal. 2005) (plaintiff had standing under UCL “based on loss of
21 financial resources in investigating this claim”). Plaintiffs pled economic injury, see ¶¶ 109-129, as well
22 as out-of-pocket economic loss as a result of Facebook’s conduct. See ¶¶ 109-110, 128-120.

23 **2. Plaintiffs Have Alleged a Predicate Violation.**

24 “The UCL also creates a cause of action for a business practice that is “unfair” even if not
25 specifically proscribed by some other law.” *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 812 (N.D.

26 _____
27 ³⁶ See discussion at IV B.

1 Cal. 2011). The Ninth Circuit approved two tests to determine whether a practice is unfair. *Id.* Under
2 the balancing test, a court examines the impact of the unfair practice on the victim, balanced against the
3 reasons, justifications and motives of the alleged wrongdoer. *See Rubio v. Capital One Bank*, 613 F.3d
4 1195, 1205 (9th Cir. 2010). Under the public policy test, Plaintiffs must show that Facebook’s policy of
5 tracking its users after logout “violates public policy as declared by specific constitutional, statutory or
6 regulatory provisions.” *Id.*

7 Under the balancing test, Facebook’s practice is unfair because Facebook has no legitimate
8 purpose (e.g. public safety, privacy preservation) to track Plaintiffs beyond their consent. Under the
9 public policy test, it is a violation of both public policy and “Section 5 of the FTC Act” for Facebook
10 to misrepresent its data collection as it did when it represented that tracking cookies would be deleted
11 upon logout. *See* Notice of Federal Trade Commission, File No. 102 3185, ScanScout Inc., 76 FR
12 71564-01, 2011 WL 5592938 (November 18, 2011) (consent agreement settling alleged violations of
13 federal law prohibiting the unfair deceptive practice of misrepresenting that consumers could prevent
14 the company from collecting data about their online activities by changing their browser settings to
15 prevent the implantation of cookies.).

16 **H. THE COMPLAINT STATES A CLAIM UNDER THE CONSUMER LEGAL**
17 **REMEDIES ACT.**

18 Facebook argues that Plaintiffs are unable to assert a claim under the CLRA because: (1)
19 Plaintiffs have not suffered damages; (2) Plaintiffs are not consumers; (3) the CLRA does not apply to
20 software; and (4) Plaintiffs failed to plead with Rule 9(b) specificity. None of Facebook’s arguments
21 has merit.

22 Plaintiffs pled damages, including statutory damages. *See* ¶¶109-129. “California courts have
23 recognized that ‘damage’ in CLRA parlance is not synonymous with ‘actual damages,’ and may
24 encompass ‘harms other than pecuniary damages.’” *Doe I v. AOL LLC*, 719 F. Supp. 2d 1102, 1111
25 (N.D. Cal. 2010) (disclosure of plaintiffs’ personal information encompassed as damages under
26 CLRA); *see also Motschenbacher v. R. J. Reynolds Tobacco Co.*, 498 F.2d 821, 825 n. 10 & 11 (9th
27 Cir 1974) (citing *Canessa v. J. I. Kislak, Inc.*, 97 N.J. Super. 327, 351 (Law Div. 1967)) (“If there is
28 value in it, sufficient to excite the cupidity of another, why is it not the property of him who gives it

1 the value and from whom the value springs?”).

2 Plaintiffs are consumers because the CLRA defines a consumer as “an individual who seeks or
3 acquires, by purchase or lease, any goods or services for personal, family, or household purposes.”
4 Cal. Civ. Code § 1761(d). The consideration for Facebook membership is the payment of personal
5 information to Facebook. See ¶¶ 111-125. This personal information has value to Facebook;³⁷ it
6 allows Facebook “to deliver ads” that are “valuable to advertisers” because it allows advertisers to
7 “target [their] specific audience.” Def. Decl. of Solanki, Ex. A, §§ 10-11. Because the CLRA is to be
8 “liberally construed and applied” to protect consumers from “unfair and deceptive business practices,”
9 Cal. Civ. Code § 1760, the bartered for exchange of Plaintiffs’ personal information in exchange for
10 the use of Facebook’s social networking service, falls within domain of the CLRA.

11 Facebook argues that the CLRA does not apply to software, but this position cannot be
12 stretched to include any product or service that includes software as only one component of the
13 product or service, otherwise the vast majority of goods and services whose use relates to software (
14 i.e. automobiles, telephones, appliances, and all consumer electronics) would be exempt from the
15 CLRA. Indeed, Facebook’s cases cited in support of this proposition deal *exclusively* with the
16 purchase of software. In *Ferrington v. McAfee, Inc.*, No. 10-cv-01455-LHK, 2010 WL 3910169 (N.D.
17 Cal. Oct. 5, 2010), for example, the court held that virus protection software was not a “good” or
18 “service” covered by the CLRA. *Id.* at 19; *see also In re Apple iPhone Application Litig.*, No. 11-md-
19 02250-LHK, 2011 WL 4403963 at 10 (N.D. Cal. Sept. 20, 2011) (“to the extent Plaintiffs’ allegations
20 are based *solely* on software, Plaintiffs do not have a claim under the CLRA” (emphasis added)), *rev’d*
21 *on other grounds, In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2012 WL 2126351 at 10
22 (N.D. Cal. June 12, 2012).

23 Facebook sells a social networking *service*, not software, see ¶ 9, even if software is
24 tangentially involved in the service. The CLRA covers Facebook’s social networking service. Cal.

25

26 ³⁷ Plaintiffs need not allege or prove their personal information had economic value they could trade
27 on some market in order to sufficiently allege that they agreed to provide that information to Facebook
28 during Facebook sessions in order to gain system access.

1 Civ. Code § 1761(b) (“‘Services’ means work, labor, and services for other than a commercial or
2 business use, including services furnished in connection with the same or repair of goods.”).
3 Facebook has cited no cases to the contrary.

4 Finally, Plaintiffs have pled their claims with the requisite specificity, as set forth in section IV
5 B, *supra*.

6 **I. THE COMPLAINT STATES A CLAIM FOR CONVERSION.**

7 Historically, “[c]onversion is the wrongful exercise of dominion over the property of another.”
8 *Farmers Ins. Exch. v. Zerin*, 61 Cal. Rptr. 2d 707, 709 (1997). A claim for conversion requires the
9 plaintiff’s ownership or right of possession at the time of the conversion, the defendant’s conversion
10 by a wrongful act of disposition of property rights and damages. *Burlesci v. Petersen*, 68 Cal. App. 4th
11 1062, 80 Cal. Rptr. 2d 704, 706 (1998).

12 Personal information is among the most important intangible property a person has in the
13 digital age – the bits and bytes of digital data that identify us. Possession of personal information has
14 value – to each of us as we exercise our interest in being known only to those we choose, and to
15 others, who would utilize personal digital information to turn us into sources of profit.

16 Unsurprisingly, there is a trend to expand the reach of conversion beyond its hide-bound
17 history:

18 [The] conception that an action for conversion lies only for tangible property capable
19 of being identified and taken into actual possession is based on a fiction on which the
20 action of trover was founded—namely, that the defendant had found the property of
another which was lost—and that such conception has become, in the progress of law,
an unmeaning thing which has been discarded by most courts....

21 Annotation, *Nature of Property or Rights Other than Tangible Chattels Which May Be Subject of*
22 *Conversion*, 44 A.L.R.2d 927, 929 (1955), quoted in *FMC Corp. v. Capital Cities/ABC, Inc.*, 915 F.2d
23 300, 304-05 (7th Cir. 1990) (recognizing the “modern trend of state law in protecting against the
24 misuse of confidential business information through conversion actions” (citing *Annis v. Tomberlin &*
25 *Shelnutt Associates, Inc.*, 195 Ga. App. 27, 392 S.E.2d 717 (1990) (affirming jury verdict for
26 conversion of confidential information); *Conant v. Karris*, 165 Ill. App. 3d 783, 117 Ill. Dec. 406, 520
27 N.E.2d 757 (1987) (upholding a claim for the conversion of confidential information); *Datacomm*
28 *Interface, Inc. v. Computerworld, Inc.*, 396 Mass. 760, 489 N.E.2d 185 (1986) (upholding damages

1 award for conversion of circulation list copy); *Kremen v. Cohen*, 337 F.3d 1024, 1033 (9th Cir. 2003)
2 (recognizing conversion of intangible property). Thus, the modern trend recognizes that misuse of the
3 confidential information becomes the gravamen of conversion, not the deprivation of property that had
4 previously been the tort’s hallmark.

5 Plaintiffs have alleged ownership or right to this specific personal information, its wrongful
6 disposition and damages. *See Kremen* 337 F.3d at 1029.³⁸ This states a cause of action. *See id.*

7 **J. THE COMPLAINT STATES A CLAIM FOR TRESPASS TO CHATTELS.**

8 A claim for trespass to chattels based on accessing a computer system involves: (1) an
9 intentional and unauthorized interference with the owner’s possessory interest in the computer system;
10 and (2) unauthorized use proximately resulted in damage to the owner. *eBay, Inc., v. Bidder’s Edge*,
11 100 F. Supp. 2d 1058, 1070,1071 (N.D. Cal. 2000). California generally recognizes a trespass claim
12 where the defendant exceeds the scope of the consent. *Id.* at 1071; *Baugh v. CBS, Inc.*, 828 F. Supp.
13 745, 756 (N.D. Cal. 1993) (even conduct that does not amount to a substantial interference with
14 possession, but which consists of intermeddling with or use of another’s personal property, is
15 sufficient to state a claim). In *Bidder’s Edge*, the Court found that an unauthorized and intentional
16 search of eBay’s electronic database constituted a trespass to eBay’s property. Similarly, Plaintiffs
17 here allege an unauthorized and intentional use of their private information (names, account
18 information, browsing history, purchasing habits) by Facebook and that they were damaged as a
19 result, giving rise to liability. *See* ¶103-129; *see also* Restatement (Second) of Torts § 256 (1965).

20 **K. THE COMPLAINT STATES A CLAIM FOR INTRUSION UPON**
21 **SECLUSION.**

22 An action for invasion of privacy by intrusion upon seclusion has three elements – (1) an
23 intrusion into a private place, conversation, or matter, (2) in a manner highly offensive to a reasonable
24 person, who (3) has a objectively reasonable expectation of seclusion or solitude in the place,
25 conversation or data source. *Smith v. Capital One Fin. Corp.*, 2012 U.S. Dist. LEXIS 66445, 8-9

26
27 ³⁸ Facebook’s argument that Plaintiffs consented to its post-logout tracking is addressed at section
28 C.V., *supra*

1 (N.D. Cal. May 11, 2012). The intrusion need not be physical, *Deteresa v. American Broadcasting*
2 *Cos., Inc.*, 121 F.3d 460, 465 (9th Cir. 1997), but includes “unwarranted sensory intrusions such as
3 eavesdropping, wiretapping, and visual or photographic spying.” *Turnbull v. ABC*, 2004 U.S. Dist.
4 LEXIS 24351, 35-36 (C.D. Cal. Aug. 19, 2004).

5 **1. Plaintiffs Had Objectively Reasonable Expectation Of Seclusion Or**
6 **Solitude.**

7 As a matter of law, one has reasonable expectation of privacy in one’s home computer. *See*
8 *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. Cal. 2007); *see also United States v.*
9 *Peden*, 2007 U.S. Dist. LEXIS 61354 (E.D. Cal. Aug. 9, 2007); *Dietemann v. Time, Inc.* 449 F.2d 245
10 (9th Cir. 1971). Under certain circumstances, the expectation of privacy includes a workplace
11 computer. *Sanders v. American Broadcasting Companies*, 20 Cal. 4th 907, 918 (Cal. 1999). Plaintiffs
12 have sufficiently alleged that they had a reasonable expectation of privacy from electronic intrusion
13 whether that activity took place at home or at work.

14 **2. Intrusion Was In A Manner Highly Offensive To A Reasonable Person.**

15 Facebook argues that “Plaintiffs fail to allege that Facebook used this [surreptitiously collected]
16 information at all, let alone that it was used for an “offensive or improper purpose.” Facebook
17 conflates *what* was done with the information with *how* the information was obtained. Rather than
18 engaging in “target advertising” or “routine commercial behavior,” Plaintiffs have alleged that
19 Facebook engaged in surreptitiously taking information it promised not to take. *See Taus v. Loftus*, 40
20 Cal. 4th 683, 751 (Cal. 2007) (“Wiretapping or surreptitious recording of conversations violates the
21 rights of those wiretapped or recorded, because such intrusions violate well-defined expectations of
22 privacy”); *Ribas v. Clark*, 38 Cal. 3d 355, 361 (Cal. 1985) (“[S]ecret monitoring denies the speaker an
23 important aspect of privacy of communication -- the right to control the nature and extent of the
24 firsthand dissemination of his statements”). Plaintiffs claim that Facebook surreptitiously obtained
25 information reasonably thought by its members to be secure states a claim for intrusion upon
26
27
28

1 seclusion.³⁹

2 **L. PLAINTIFFS WITHDRAW THEIR CLAIM UNDER THE COMPUTER**
3 **FRAUD AND ABUSE ACT.**

4 Plaintiffs withdraw their CFAA claim.

5 ///

6 ///

7 ///

8 ///

9 ///

10 ///

11 ///

12 ///

13 ///

14 ///

15 ///

16 ///

17 ///

18 ///

19 ///

20 ///

21 ///

22 _____

23 ³⁹ See also *Luken v. Edwards*, 2011 U.S. Dist. LEXIS 47545, 22-23 (N.D. Iowa May 3, 2011);
24 *Cozzolino v. Maricopa County*, No. CV-04-2229-PHX-FJM, 2006 U.S. Dist. LEXIS 44567, 2006 WL
25 1794761, at *2 (D. Ariz. June 27, 2006); *Amati v. City of Woodstock, Ill.*, 829 F. Supp. 998, 1010-11
26 (N.D. Ill. 1993); *Fowler v. Southern Bell Tel. & Tel. Co.*, 343 F.2d 150, 156 (5th Cir. 1965); *Binkley v.*
27 *Loughran*, 714 F. Supp. 776, 780 (M.D.N.C. 1989); *Cavallaro v. Rosado*, No. CV054009939, 2006
28 Conn. Super. LEXIS 2919, 2006 WL 2949143, at *4 (Conn. Super. Ct. Oct. 5, 2006); and W. Page
Keeton et al., *Prosser & Keeton on the Law of Torts* § 117, at 884-85 (5th ed. 1984) (citing
eavesdropping on telephone calls by wiretapping as an example for the tort of intrusion into the
seclusion of another).

1 **V. CONCLUSION**

2 Privacy is a cherished right in this country. The law defines the parameters of privacy,
3 recognizes its importance and provides remedies for its violation. Plaintiffs' FAC accuses Facebook
4 of engaging in tortious, illegal conduct deliberately designed to violate those rights for the basest of
5 reasons – profit. At this stage of the proceedings, plaintiff's factual allegations are held to be true.
6 The FAC invokes the remedies provided for in the law, and plaintiffs have done all that is
7 procedurally necessary to grant them the right to fully explore and prove the wrongs perpetrated by
8 this defendant. As such, the Motion to dismiss must be denied.

9 DATED this 2nd Day of August, 2012.

Respectfully submitted,

10 **BARTIMUS, FRICKLETON,**
11 **ROBERTSON & GORNY, P.C.**

STEWARTS LAW US LLP

12 /s/ Edward D. Robertson Jr.

/s/ David A. Straite

13 Edward D. Robertson, Jr.
14 James P. Frickleton
15 Mary D. Winter
16 Edward D. Robertson III
17 11150 Overbrook Road, Suite 200
18 Leawood, KS 66211
19 *chiprob@earthlink.net*
20 Telephone: (913) 266-2300
21 Facsimile: (913) 266-2366
22 ***Interim Co-Lead Counsel***

David A. Straite (admitted *pro hac vice*)
Ralph N. Sianni
Michele S. Carino
Lydia E. York
1201 North Orange Street, Suite 740
Wilmington, DE 19801
dstraite@stewartslaw.com
Telephone: (302) 298-1200
Facsimile: (302) 298-1222
Interim Co-Lead Counsel

18 **KIESEL BOUCHER LARSON LLP**

19 Paul R. Kiesel, Esq. (SBN 119854)
20 8648 Wilshire Boulevard
21 Beverly Hills, CA 90211
22 *kiesel@kbla.com*
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
Interim Liaison Counsel

23
24
25
26
27
28

1 Stephen G. Grygiel
John E. Keefe, Jr.
2 Jennifer Harwood
3 **KEEFE BARTELS LLC**
170 Monmouth Street
4 Red Bank, NJ 07701
Telephone: (732) 224-9400
5 Facsimile: (732) 224-9494
sgrygiel@keefebartels.com
6 ***Plaintiffs' Steering Committee Member***

7 Barry R. Eichen
8 Daryl L. Zaslow
Tom Paciorkowski
9 **EICHEN CRUTCHLOW ZASLOW &
MCELROY LLP**
10 40 Ethel Road
Edison, New Jersey 08817
11 Telephone: (732) 777-0100
12 Facsimile: (732) 248-8273
beichen@njadvocates.com
13 ***Plaintiffs' Steering Committee Member***

14 Andrew J. Lyskowski
15 Erik A. Bergmanis
BERGMANIS LAW FIRM, L.L.C.
16 380 W. Hwy. 54, Suite 201
P.O. Box 229
17 Camdenton, MO 65020
alyskowski@ozarklawcenter.com
18 Telephone: (573) 346-2111
19 Facsimile: (573) 346-5885
Plaintiffs' Steering Committee Member

20 William H. Murphy, Jr.
21 Tonya Osborne Baña
MURPHY, FALCON & MURPHY, P.A.
22 One South Street, 23rd Floor
Baltimore, MD 21202
23 *billy.murphy@murphypa.com*
Telephone: (410) 539-6500
24 Facsimile: (410) 539-6599
Plaintiffs' Steering Committee Member

Michael S. Schwartz
Mark S. Mandell
Zachary Mandell
**MANDELL, SCHWARTZ & BOISCLAIR,
LTD.**
1 Park Row
Providence, RI 02903
msmandell@msb-atty.com
Telephone: (401) 273-8330
Facsimile: (401) 751-7830
Plaintiffs' Steering Committee Member

Stephen M. Gorny
**BARTIMUS, FRICKLETON,
ROBERTSON & GORNY, P.C.**
11150 Overbrook Road, Suite 200
Leawood, KS 66211
steve@bflawfirm.com
Telephone: (913) 266-2300
Facsimile: (913) 266-2366
Plaintiffs' Steering Committee Member

William M. Cunningham, Jr.
Peter S. Mackey
Peter F. Burns
BURNS CUNNINGHAM & MACKEY PC
P.O. Box 1583
Mobile, AL 36633
wmcunningham@bcmlawyers.com
Telephone: (251) 432-0612
Facsimile: (251) 432-0625
Plaintiffs' Steering Committee Member

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

Margery S. Bronster
Robert Hatch
BRONSTER HOSHIBATA
1003 Bishop Street, Suite 2300
Honolulu, Hawaii 96813
mbronster@bhhawaii.net
Telephone: (808) 524-5644
Facsimile: (808) 599-1881
Special State AG Advisory Committee Member

Richard P. Ieyoub
Michael Reese Davis
L. J. Hymel
Tim P. Hartdegen
HYMEL, DAVIS & PETERSEN, LLC
10602 Coursey Blvd.
Baton Rouge, LA 70816
rieyoub@hymeldavis.com
Telephone: (225) 298-8188
Facsimile: (225) 298-8119
Special State AG Advisory Committee Member

Grant Woods
GRANT WOODS PC
Two Renaissance Square
40 N. Central Ave., Suite 2250
Phoenix, AZ 85004
gw@grantwoodspc.net
Telephone: (602) 258-2599
Facsimile: (602) 258-5070
Special State AG Advisory Committee Member

Mike Moore
MIKE MOORE LAW FIRM, LLC
10 Canebrake Blvd.
Suite 150 Flowood, MS 39232
mm@mikemoorelawfirm.com
Telephone: (601) 933-0070
Facsimile: (601) 933-0071
Special State AG Advisory Committee Member