

Replacement for Dkt. 157-1

1 GIBSON, DUNN & CRUTCHER LLP
JOSHUA A. JESSEN, SBN 222831
2 JJessen@gibsondunn.com
JEANA BISNAR MAUTE, SBN 290573
3 JBisnarMaute@gibsondunn.com
PRIYANKA RAJAGOPALAN, SBN 278504
4 PRajagopalan@gibsondunn.com
ASHLEY M. ROGERS, SBN 286252
5 ARogers@gibsondunn.com
1881 Page Mill Road
6 Palo Alto, California 94304
Telephone: (650) 849-5300
7 Facsimile: (650) 849-5333

8 GIBSON, DUNN & CRUTCHER LLP
CHRISTOPHER CHORBA, SBN 216692
9 CChorba@gibsondunn.com
333 South Grand Avenue
10 Los Angeles, California 90071
Telephone: (213) 229-7000
11 Facsimile: (213) 229-7520

12 Attorneys for Defendant
FACEBOOK, INC.
13

14 UNITED STATES DISTRICT COURT
15 NORTHERN DISTRICT OF CALIFORNIA
16 OAKLAND DIVISION

17 MATTHEW CAMPBELL and MICHAEL
18 HURLEY,

19 Plaintiffs,

20 v.

21 FACEBOOK, INC.,

22 Defendant.

Case No. C 13-05996 PJH

PUTATIVE CLASS ACTION

**APPENDIX OF EVIDENCE IN SUPPORT
OF DEFENDANT FACEBOOK, INC.'S
OPPOSITION TO PLAINTIFFS' MOTION
FOR CLASS CERTIFICATION**

HEARING:

Date: March 16, 2016

Time: 9:00 a.m.

Place: Courtroom 3, 3rd Floor
The Honorable Phyllis J. Hamilton

INDEX

<u>Document</u>	<u>Page Numbers</u>
Declaration of Christopher Chorba	1-14
Exhibit A – Chart: Variability Surrounding Named Plaintiffs and Some Putative Class Members	15-17
Exhibit B – Graphical Representation of Steps Required to Send and Receive a Facebook Message with a URL Preview Attachment ...	18-19
Exhibit C – Graphical Representations of Individualized Inquiries Related to Ascertainability	20-29
Exhibit D – Charts: Summary of Variability for Challenged Practices ...	30-37
Exhibit E – Chart: Evidence of Implied Consent.....	38-60
Exhibit F – Publications Corresponding to Implied Consent Chart (Part 1: FB000000066 - FB000000120)	61-101
Exhibit G – Publications Corresponding to Implied Consent Chart (Part 2: FB000000121 - FB000000208)	102-184
Exhibit H – Publications Corresponding to Implied Consent Chart (Part 3: FB000000209 - FB000000255)	185-229
Exhibit I – Publications Corresponding to Implied Consent Chart (Part 4: FB000000256 - FB000000329)	230-285
Exhibit J – Publications Corresponding to Implied Consent Chart (Part 5: FB000000330 - FB000000384)	286-341
Exhibit K – Publications Corresponding to Implied Consent Chart (Part 6: FB000000385 - FB000000424)	342-376
Exhibit L – Excerpts from May 9, 2015 Deposition of Matthew Campbell	377-445
Exhibit M– Excerpts from July 9, 2015 Deposition of Michael Hurley....	446-499
Exhibit N – Excerpts from October 1, 2015 Deposition of David Shadpour	500-556
Exhibit O – Plaintiff Matthew Campbell’s Corrected Objections and Responses to Defendant Facebook, Inc.’s First Set of Interrogatories	557-688
Exhibit P – Plaintiff Michael Hurley’s Objections and Responses to Defendant Facebook, Inc.’s First Set of Interrogatories	689-710
Exhibit Q – (Former) Plaintiff David Shadpour’s Corrected Objections and Responses to Defendant Facebook, Inc.’s First Set of Interrogatories	711-728
Exhibit R - April 10, 2015 Letter from David Rudolph to Joshua Jessen .	729-732
Exhibit S – Plaintiff Matthew Campbell’s Facebook Messages Produced by Plaintiffs (Part 1: CAMPBELL000001 - CAMPBELL000181)	733-914

	<u>Document</u>	<u>Page Numbers</u>
1		
2	Exhibit T – Plaintiff Matthew Campbell’s Facebook Messages Produced by Plaintiffs (Part 2: CAMPBELL000440 - CAMPBELL000494)	915-970
3	Exhibit U – Plaintiff Matthew Campbell’s Facebook Messages Produced by Plaintiffs (Part 3: CAMPBELL000495 - CAMPBELL000496)	971-973
4	Exhibit V – Plaintiff Michael Hurley’s Facebook Messages Produced by Plaintiffs (HURLEY000001 - HURLEY000003).....	974-977
5		
6	Exhibit W – July 24, 2015 Letter from David Rudolph to Joshua Jessen .	978-983
7	Exhibit X – Defendant Facebook, Inc.’s Responses and Objections to Plaintiffs’ First Set of Requests for Admission	984-989
8	Exhibit Y – April 7, 2015 Letter from Hank Bates to Joshua Jessen and Christopher Chorba	990-992
9	Exhibit Z – May 13, 2015 Letter from Joshua Jessen to Hank Bates	993-997
10	Exhibit AA – June 12, 2015 Letter from Joshua Jessen to David Rudolph	998-1000
11	Exhibit BB – Excerpts from June 30, 2015 Deposition of Jiakai Liu.....	1001-1010
12	Exhibit CC – Excerpts from September 25, 2015 Deposition of Ray He..	1011-1026
13	Exhibit DD – Excerpts from December 18, 2015 Deposition of Fernando Torres	1027-1088
14	Exhibit EE - Excerpts from December 16, 2015 Deposition of Jennifer Golbeck	1089-1350
15	Exhibit FF – Excerpts from August 7, 2015 Deposition of ██████████ ██████████	1351-1374
16	Exhibit GG – Excerpts from August 10, 2015 Deposition of ██████████	1375-1411
17	Exhibit HH – Excerpts from August 11, 2015 Deposition of ██████████ ██████████	1412-1458
18	Exhibit II – Excerpts from October 28, 2015 Deposition of Ray He.....	1459-1474
19	Exhibit JJ – Excerpts from October 28, 2015 Deposition of Michael Adkins	1475-1487
20	Exhibit KK– February to March 2011 Facebook Email Chain Produced by Facebook (FB000006429).....	1488-1494
21	Exhibits LL – Google Analytics Data Produced by Facebook (FB000009906 and FB000009914).....	1495-1507
22	Declaration of Alex Himel	1508-1533
23	Exhibit MM – Defendant Facebook, Inc.’s Second Supplemental Responses and Objections to Plaintiffs’ Narrowed Second Set of Interrogatories	1534-1555
24		
25		
26		
27		
28		

	<u>Document</u>	<u>Page Numbers</u>
1		
2	Exhibit NN – Defendant Facebook, Inc.’s Supplemental Responses and Objections to Plaintiffs’ First Set of Interrogatories	1556-1605
3	Exhibit OO – June 1, 2015 Declaration of Alex Himel on Behalf of Defendant Facebook, Inc.	1606-1692
4	Declaration of Dan Fehete	1693-1708
5	Exhibit PP – Summary of Relevant Variability in Recommendations Plugin Functionality	1709-1710
6		
7	Exhibit QQ – Source Code Differential D94144	1711-1749
8	Exhibit RR – Source Code Differential D100080.....	1750-1773
9	Exhibit SS– Source Code Differential D122427	1774-1792
10	Exhibit TT – Source Code Differential D121547	1793-1798
11		
12	Exhibit UU – Source Code Differential D155812	1799-1825
13	Exhibit VV – Source Code Differential D179234	1826-1835
14	Exhibit WW – Source Code Differential D186382	1836-1843
15	Exhibit XX – Source Code Differential D211615	1844-1853
16	Exhibit YY – Source Code Differential D236924	1854-1899
17		
18	Exhibit ZZ – Source Code Differential D172147	1900-1914
19	Exhibit AAA – Source Code Differential D404158	1915-1927
20	Declaration of Michael Adkins	1928-1938
21	Expert Report of Dr. Benjamin Goldberg	1939-1992
22		
23	Exhibit BBB – Curriculum Vitae.....	1993-2000
24	Exhibit CCC – Materials Considered.....	2001-2002
25	Expert Report of Dr. Catherine Tucker	2003-2058
26	Exhibit DDD – Curriculum Vitae	2059-2073
27		
28		

	<u>Document</u>	<u>Page Numbers</u>
1		
2	Exhibit EEE – Prior Testimony	2074-2075
3	Exhibit FFF – Materials Considered	2076-2085
4	Exhibit GGG– Facebook Quarterly Revenue and Expenses.....	2086-2087
5		
6	Exhibits HHH, III, JJJ – Torres Social Graph Valuation.....	2088-2093
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 GIBSON, DUNN & CRUTCHER LLP
JOSHUA A. JESSEN, SBN 222831
2 JJessen@gibsondunn.com
JEANA BISNAR MAUTE, SBN 290573
3 JBisnarMaute@gibsondunn.com
PRIYANKA RAJAGOPALAN, SBN 278504
4 PRajagopalan@gibsondunn.com
ASHLEY M. ROGERS, SBN 286252
5 ARogers@gibsondunn.com
1881 Page Mill Road
6 Palo Alto, California 94304
Telephone: (650) 849-5300
7 Facsimile: (650) 849-5333

8 GIBSON, DUNN & CRUTCHER LLP
CHRISTOPHER CHORBA, SBN 216692
9 CChorba@gibsondunn.com
333 South Grand Avenue
10 Los Angeles, California 90071
Telephone: (213) 229-7000
11 Facsimile: (213) 229-7520

12 Attorneys for Defendant
FACEBOOK, INC.

13
14 UNITED STATES DISTRICT COURT
15 NORTHERN DISTRICT OF CALIFORNIA
16 OAKLAND DIVISION

17 MATTHEW CAMPBELL and MICHAEL
HURLEY,

18 Plaintiffs,

19 v.

20 FACEBOOK, INC.,

21 Defendant.
22

Case No. C 13-05996 PJH

**DECLARATION OF CHRISTOPHER
CHORBA IN SUPPORT OF DEFENDANT
FACEBOOK, INC.'S OPPOSITION TO
PLAINTIFFS' MOTION FOR CLASS
CERTIFICATION**

1 I, Christopher Chorba, declare as follows:

2 1. I am an attorney admitted to practice law before this Court. I am a partner in the law
3 firm of Gibson, Dunn & Crutcher LLP, and I am one of the attorneys responsible for representing
4 Defendant Facebook, Inc. (“Facebook”) in the above-captioned action. I submit this declaration in
5 support of Facebook’s Opposition to Plaintiffs’ Motion for Class Certification (Dkt. 138). Unless
6 otherwise stated, the following facts are within my personal knowledge and, if called and sworn as a
7 witness, I could and would testify competently to these facts.

8 **I. Demonstratives**

9 2. Attached as **Exhibits A–D** are demonstrative graphics regarding the named plaintiffs
10 and challenged practices.*

11 a. Attached as **Exhibit A** is a chart summarizing a number of individualized issues
12 concerning the named Plaintiffs and some putative class members.

13 b. Attached as **Exhibit B** is a graphical representation of the steps required to send
14 and receive a Facebook message with a URL preview attachment.

15 c. Attached as **Exhibit C** are graphical representations of the individualized inquiries
16 related to ascertainability.

17 d. Attached as **Exhibit D** are charts summarizing the variability for the challenged
18 practices.

19 3. Facebook and its messaging service have often been the subject of public news
20 reports, blog posts, and other publications. Attached as **Exhibit E** is a chart summarizing seventy-
21 seven publicly available online publications, including, *inter alia*, news reports, articles, editorials,
22 and Facebook developer documentation, published between May 6, 2009 and August 7, 2013.
23 Attached as **Exhibits F, G, H, I, J, and K** are the corresponding seventy-seven publications, arranged
24 by Bates numbers FB000000066 to FB000000424 and produced by Facebook during this litigation.
25

26 * For the Court’s convenience, and to avoid duplication in the numbering of the exhibits submitted
27 by Plaintiffs, Facebook has used letters rather than numbers to designate its exhibits.

1 **II. Discovery Requests And Responses From Plaintiffs**

2 **A. Plaintiffs' Deposition Testimony**

3 4. Attached as **Exhibit L** is a true and correct copy of relevant excerpts of the deposition
4 transcript of Plaintiff Matthew Campbell on May 19, 2015.

5 5. Attached as **Exhibit M** is a true and correct copy of relevant excerpts of the deposition
6 transcript of Plaintiff Michael Hurley on July 9, 2015.

7 6. Attached as **Exhibit N** is a true and correct copy of relevant excerpts of the deposition
8 transcript of Mr. David Shadpour on October 1, 2015.

9 **B. Plaintiffs' Written Discovery Responses**

10 7. Attached as **Exhibit O** is a true and correct copy of Plaintiff Campbell's Corrected
11 Objections and Responses to Defendant Facebook, Inc.'s First Set of Interrogatories, dated April 2,
12 2015. As these responses reflect, Mr. Campbell has sent or received at least [REDACTED] Facebook messages
13 containing URLs between the time he filed this action (December 30, 2013), and the date of his
14 responses (April 2, 2015).

15 8. Attached as **Exhibit P** is a true and correct copy of Plaintiff Hurley's Objections and
16 Responses to Defendant Facebook, Inc.'s First Set of Interrogatories, dated April 1, 2015. As these
17 responses reflect, Mr. Hurley has sent or received at least [REDACTED] Facebook messages containing URLs
18 between the time he filed this action (December 30, 2013), and the date of his responses (April 1,
19 2015).

20 9. Attached as **Exhibit Q** is a true and correct copy of (Former) Plaintiff Shadpour's
21 Corrected Objections and Responses to Defendant Facebook, Inc.'s First Set of Interrogatories, dated
22 April 2, 2015. As these responses reflect, Mr. Shadpour has sent or received at least [REDACTED] Facebook
23 messages containing URLs between the time he filed this action (January 21, 2014), and the date of
24 his responses (April 2, 2015).

25 10. On April 10, 2015, Plaintiffs supplemented their responses to Facebook's
26 Interrogatories through a letter from counsel (David Rudolph). In particular, Plaintiffs supplemented
27 their responses to Facebook's Interrogatory No. 5 to describe the manner in which they learned of the
28

1 facts supporting their claims, as follows:

- 2 • [REDACTED]
- 3 [REDACTED]
- 4 [REDACTED]
- 5 [REDACTED]
- 6 • [REDACTED]
- 7 [REDACTED]
- 8 [REDACTED]
- 9 • [REDACTED]
- 10 [REDACTED]
- 11 [REDACTED]

12 Attached as **Exhibit R** is a true and correct copy of Mr. Rudolph’s letter dated April 10, 2015.

13 **C. Plaintiffs’ Document Productions**

14 11. During discovery, Facebook requested that Plaintiffs produce copies of the Facebook
15 messages that they sent or received, including but not limited to messages containing URLs.

16 12. Attached as **Exhibits S–U** are true and correct copies of the Facebook messages that
17 Mr. Campbell produced in this action, bearing Bates numbers CAMPBELL000001–181 ([REDACTED])
18 ([REDACTED]), CAMPBELL000440–494 ([REDACTED])
19 ([REDACTED]), and CAMPBELL000495–496
20 ([REDACTED])
21 ([REDACTED]). In the latter category, [REDACTED]
22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 [REDACTED]

1 [REDACTED]
2 (Ex. V, CAMPBELL000495–496 (emphases added).)

3 In response, [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]

8 (Ex. V, CAMPBELL000496.)

9 13. Attached as **Exhibit V** are true and correct copies of the Facebook messages that Mr.
10 Hurley produced in this action, bearing Bates numbers HURLEY000001–003.

11 **D. Plaintiffs’ Interrogatory No. 8 To Facebook**

12 14. On May 26, 2015, Plaintiffs propounded their Second Set of Interrogatories, which
13 consisted of Interrogatory No. 8, and which sought detailed information regarding the processing of
14 “each [Facebook] message sent or received by Plaintiffs containing a URL.” (Dkt. 130.)

15 15. After discussions between the parties regarding the scope of Interrogatory No. 8,
16 Plaintiffs’ counsel (Mr. Rudolph) wrote to Facebook’s counsel on July 24, 2015, to confirm
17 Plaintiffs’ agreement to limit their Interrogatory No. 8 “to a subset of the total messages at issue,” and
18 Mr. Rudolph provided a list of 19 messages (8 messages to/from Plaintiff Hurley, and 11 messages
19 to/from Plaintiff Campbell). Mr. Rudolph explained that for these 19 messages, “Plaintiffs seek
20 identification and data production of each of the Objects and Associations created when Facebook
21 processed Plaintiffs’ Private Messages containing a URL.” Attached as **Exhibit W** is a true and
22 correct copy of Mr. Rudolph’s letter dated July 24, 2015.

23 16. A true and correct copy of Facebook’s Second Supplemental Responses and
24 Objections to Plaintiffs’ Narrowed Second Set of Interrogatories (dated October 28, 2015) is attached
25 to the Declaration of Alex Himel as **Exhibit MM**. As discussed in these Responses, [REDACTED]
26 [REDACTED]
27 [REDACTED]

28 [REDACTED] (*Id.* at 17.) Facebook explained [REDACTED]

1 [REDACTED]
2 [REDACTED] (*Id.*) At the time of the Responses, Facebook determined that [REDACTED]
3 [REDACTED]
4 [REDACTED] (*Id.*) Facebook
5 produced documents related to its responses regarding the 19 messages. (*Id.* at 18 & Ex. A)

6 17. Facebook also analyzed these messages to determine which of the messages (if any)
7 had a possibility of incrementing a social plugin count on a third-party website. Although Facebook
8 does not possess records to determine whether a particular third-party webpage displayed a social
9 plugin count at the time Plaintiffs’ selected messages were either sent or received, the Internet
10 Wayback Machine (<https://archive.org/web/>) is a “reliable” resource that Plaintiffs’ technical expert,
11 Dr. Jennifer Golbeck, uses “pretty frequently” to view archived webpages. (**Ex. EE**, Golbeck Depo.
12 Tr., at 20:7-21:3.)

13 18. For each of the remaining twelve messages selected by Plaintiffs and for which a share
14 object was created, the Internet Wayback Machine revealed that for the 10 of 12 messages that did
15 have a share object, there was no corresponding social plugin on the websites referenced by the URLs
16 in Plaintiffs’ messages at or near the time the messages were sent. For example, on [REDACTED]

17 [REDACTED]
18 [REDACTED]
19 [REDACTED]

20 [REDACTED] Thus, 10 of the 19 messages identified by Plaintiffs had a share
21 object but did not have a corresponding social plugin on the third-party website.

22 19. For 1 of the 12 messages that did have a share object, the Internet Wayback Machine
23 did not have the webpage archived. That message was sent by [REDACTED]

24 [REDACTED]
25 [REDACTED]

26 20. The remaining message was sent from Plaintiff Hurley to Plaintiffs’ counsel Melissa
27 Gardner.

1 **III. Other Discovery Issues**

2 **A. Facebook’s “Public-Facing Statements” and “Dedicated Team of Privacy**
3 **Professionals”**

4 21. In their Motion, Plaintiffs assert as follows:

5 Discovery also demonstrates that Facebook’s public-facing statements about
6 “procedural safeguards” for ensuring user privacy in product development are
7 false. Facebook has represented, *inter alia*, in its filings with the Security and
8 Exchange Commission that it has “a dedicated team of privacy professionals who
9 are involved in new product and feature development from design through
10 launch” and who conduct “ongoing review and monitoring of the way data is
11 handled by existing features and applications.” However, when asked to produce
12 documents sufficient to identify the individuals comprising this “dedicated team,”
13 Facebook responded that *none* existed.

14 (Dkt. 138 at 20-21.)

15 22. In fact, Facebook’s counsel never told Plaintiffs’ counsel that Facebook did not have a
16 “dedicated team of privacy professionals.” On the contrary, Facebook specifically *denied* Plaintiffs’
17 request to admit that there was no such team, and indeed there is such a team. Attached as **Exhibit X**
18 is a true and correct copy of Defendant Facebook, Inc.’s Responses and Objections to Plaintiffs’ First
19 Set of Requests for Admission dated June 29, 2015.

20 23. Rather, Facebook’s counsel simply confirmed that, in response to a *document request*,
21 there was not a “specific list.” Plaintiffs’ request sought “*documents*” regarding “the ‘dedicated team
22 of privacy professionals’ identified on page 8 of Your Form 10-K for fiscal year ending
23 December 31, 2013.” (Dkt. 138-4, Ex. 31.) Facebook responded by explaining that it did not have a
24 *document* responsive to Request No. 29, listing members of its internal privacy team. Plaintiffs even
25 misstated the correspondence among counsel by *omitting* the bolded portion below in their brief:

26 With respect to Request No. 29, please be advised that there is no specific list of
27 the ‘dedicated team of privacy professionals’ referenced in the Request, **but we**
28 **have already agreed to conduct a reasonable search for non-privileged**
documents sufficient to identify Facebook’s current and former employees
who may possess knowledge relevant to the practice challenged in this action,
and we also have identified witnesses with relevant knowledge in Facebook’s
Initial Disclosures and responses to Plaintiffs’ Interrogatories.

29 Plaintiffs attached Facebook’s complete response to the request as Exhibit 32 (Dkt. 138-4, Ex.
30 32).

1 **B. Plaintiffs’ Expanded Proposed Class Definition Exceeds The “Relevant Time**
2 **Period” For Discovery**

3 24. Plaintiffs’ Consolidated Amended Complaint identified the following proposed class:
4 “All natural-person Facebook users located within the United States who have sent or received
5 private messages that included URLs in their content, from within two years before the filing of this
6 action up through and including the date when Facebook ceased its practice,” which Plaintiffs alleged
7 to be “at some point after it was exposed in October 2012.” (Dkt. 25 ¶ 59 & n.3.)

8 25. In their Motion for Class Certification, Plaintiffs now seek to certify a proposed class
9 of all “Facebook users located within the United States who have sent, or received from a Facebook
10 user, private messages that included URLs in their content (and from which Facebook generated a
11 URL attachment), within two years before the filing of this action *up through the date of*
12 *certification of the class.*” (Dkt. 138 at 10 (emphasis added).) In other words, Plaintiffs have now
13 expanded their proposed class by over three years.

14 26. Plaintiffs’ new proposed class definition extends well beyond the relevant time period
15 to which the parties expressly agreed for discovery. On April 7, 2015, Hank Bates, counsel for
16 Plaintiffs, proposed that the “Relevant Time Period” for “producing documents” should be April 1,
17 2010, to the date of filing the action, December 30, 2013. Attached as **Exhibit Y** is a true and correct
18 copy of Mr. Bates’ letter dated April 7, 2015.

19 27. After some further discussions between the parties, Facebook agreed to this time
20 period in letters dated May 13 and June 12, 2015. Attached as **Exhibits Z** and **AA** are true and
21 correct copies of these letters.

22 28. Regarding the production of source code, the parties agreed (and stipulated, *see*
23 Dkt. 90) to a slightly different time period—September 1, 2009 to December 31, 2012—reflecting the
24 fact that Plaintiffs had alleged that the challenged practice had ceased “at some point after it was
25 exposed in October 2012.” (Dkt. 25 ¶ 59 & n.3.)

26 29. Additionally, during depositions of Facebook’s witnesses, counsel for Plaintiffs
27 repeatedly limited questions to the time period of “2010 to 2012” or “2010 to 2013.” Attached as
28 **Exhibits BB** and **CC** are true and correct copies of excerpts of the deposition transcripts of Facebook

1 witnesses, Jiakai Liu and Ray He, dated June 30, 2015 and September 25, 2015, respectively,
2 reflecting, *inter alia*, a handful of those questions.

3 **C. Fernando Torres' Expert Report And The Information He Claims That He**
4 **Needs To Complete His Damages Analysis**

5 30. Plaintiffs' proposed damages expert, Mr. Fernando Torres, testified that, in order to
6 complete his damages analysis, he needed *additional* information that is distinct from Plaintiffs'
7 previous damages discovery requests— which they represented were “critical to establishing” their
8 damages theory. Attached as **Exhibit DD** is a true and correct copy of relevant excerpts of the
9 deposition transcript of Mr. Fernando Torres on December 18, 2015.

10 31. In support of prior discovery motions, Plaintiffs argued that they would be “unduly
11 prejudice[d]” without “discovery relevant to damages in this action.” (Dkt. 112 at 2; *see also*
12 Dkt. 109 at 2, 4 (arguing that “[w]ithout discovery into the revenue Facebook has generated . . .
13 Plaintiffs will be hampered in formulating a class-wide damages theory”).) Plaintiffs represented that
14 the discovery they sought was “critical to establishing” their damages theory and that “expert analysis
15 of the [] information sought” would allow them to “accurately model the profits attributable to the
16 challenged conduct.” (Dkt. 112 at 2-3.) And they also argued that the damages discovery sought was
17 “directly relevant to the issues of damages suffered by the class as well as the appropriate injunctive
18 relief . . . and [was] . . . necessary for Plaintiffs to fashion a theory of class-wide relief for their class
19 certification briefing.” (Dkt. 109 at 2, 4.)

20 32. In light of these and other arguments, Plaintiffs received a 30-day extension of the
21 briefing schedule (Dkt. 117) and successfully compelled Facebook to produce extremely broad
22 discovery (Dkt. 130, 136.).

23 33. In his expert report, however, Mr. Torres cited only 7 of the thousands of documents
24 produced by Facebook during the course of this litigation. (Dkt. 138-4, Ex. 33.) He also asserted in
25 his report that he needed *other information* from Facebook: “with additional information, including
26 production from Facebook, and inputs, these conclusions [in the Report] could be refined.”
27 (Dkt. 138-4, Ex. 33, ¶ 11 n.12.) In the final paragraph of his report, Mr. Torres explained, “With
28 quantitative data on the number of affected ‘Like’ counts, and identification of the affected URLs, it

1 will be feasible to narrow the ranges discussed here and calculate more precisely the potential
2 incremental benefit attributable to the accused practice.” (*Id.* ¶ 74.)

3 34. During his deposition, Mr. Torres discussed the additional information he needed or
4 was expecting from Facebook in order to complete his analysis. But as of the date of this
5 Declaration, Plaintiffs have not requested the vast majority of information that Mr. Torres identified
6 in his deposition. To the extent some of the information has been requested previously, Facebook has
7 already conducted a reasonable search and diligent inquiry and has produced responsive information
8 to the extent it exists.

9 35. The following chart summarizes the discovery information Mr. Torres claims he needs
10 to complete his analysis and whether the information has been previously requested by Plaintiffs:

Information Mr. Torres Needs	Requested by Plaintiffs?
“[T]he number of [Facebook] messages that were intercepted that contain URLs” (Ex. EE [Torres Depo. at 27:20-22].)	No.
“[T]he total number of [Facebook] messages” (Ex. EE [Torres Depo. at 27:22-23].)	No.
“[H]ow many messages each user sent, et cetera, how many fall into the definition of the class” (Ex. EE [Torres Depo. at 227:9-11].)	No.
“[H]ow many URLs were intercepted that . . . led to like counts being increased” (Ex. EE [Torres Depo. at 285:10-14].)	Yes, but no responsive documents existed. ¹

23
24 ¹ Facebook’s Response to Plaintiffs’ Request for Production No. 57: “Facebook [] conduct[ed] a
25 reasonable search for non-privileged documents sufficient to identify the number [of] Likes that were
26 generated as a result of the processes involved in the practice challenged in this action (the alleged
27 increase in the Facebook ‘Like’ count on a website when the URL for that website was contained in a
28 message transmitted through Facebook’s Messages product) between April 1, 2010 and December
30, 2013, to the extent such documents exist, are within Facebook’s custody and control, ha[d] not
already been produced to Plaintiffs, and c[ould] be located using a reasonable search.”

Information Mr. Torres Needs	Requested by Plaintiffs?
<p data-bbox="212 237 932 310">“[T]he ratio of those increases to the total like counters”</p> <p data-bbox="212 342 932 384">(Ex. EE [Torres Depo. at 285:10-14].)</p>	No.
<p data-bbox="212 415 932 489">“[T]he value of the advertising revenue perceived by Facebook”</p> <p data-bbox="212 520 932 562">(Ex. EE [Torres Depo. at 285:14-15].)</p>	Yes. ²
<p data-bbox="212 594 932 636">“The advertising revenue that reflects only the U.S.”</p> <p data-bbox="212 657 932 699">(Ex. EE [Torres Depo. at 205:16-22].)</p>	No.
<p data-bbox="212 730 932 804">“[T]he number of links captured that fall under the definition of the class.”</p> <p data-bbox="212 835 932 877">(Ex. EE [Torres Depo. at 208:19-20].)</p>	No.
<p data-bbox="212 909 932 951">“[T]he number of links on the social graph.”</p> <p data-bbox="212 972 932 1014">(Ex. EE [Torres Depo. at 218:2-3].)</p>	No.
<p data-bbox="212 1045 932 1150">Whether websites corresponding to URLs in Facebook messages had social plugins at the time the message was sent.</p> <p data-bbox="212 1182 932 1220">(Ex. EE [Torres Depo. at 266:17-22].)</p>	No.

D. Response To Rudolph Declaration And Plaintiffs’ Misstatements About Discovery

36. In support of the Motion, Plaintiffs’ counsel David Rudolph filed a supporting declaration (Dkt. 138-3) in which he raises several complaints about discovery in this case. Mr. Rudolph’s declaration contains a large number of misstatements about the discovery conducted in this case, and the following paragraphs respond to his points in sequence.

37. First, relying on his previously filed Declaration in support of Plaintiffs’ Motion to Enlarge Time and Extend Deadlines (Dkt. 109-2), Mr. Rudolph argues that Plaintiffs’ “ability to

² Facebook produced documents in compliance with the Court’s Orders, which, *inter alia*, compelled Facebook to produce documents responsive to Plaintiffs’ Requests for Production Nos. 53, 54, and 59. (Dkt. 130, 136; *see also supra* ¶¶ 31-32.)

1 prepare their motion for class certification” was “prejudice[ed]” by Facebook’s alleged “delay[s]
2 providing relevant discovery in this matter.” (Dkt. 138-3, ¶ 2.) More specifically, he claims that
3 Facebook “delayed production of its source code by over five months . . . and [] failed to produce a
4 significant number of documents responsive to Plaintiffs’ document requests” in a timely manner.
5 (*Id.*)

6 38. Mr. Rudolph does not explain that this Court already was presented with these
7 arguments on *two* separate occasions. After considering Facebook’s Opposition to Plaintiffs’ Motion
8 to Enlarge Time and Extend Deadlines (Dkt. 114) and the supporting Declaration of Joshua Jessen
9 (Dkt. 114-1), which rebutted similar assertions from Plaintiffs’ counsel, this Court ruled that the “90-
10 day extension sought by plaintiffs would unnecessarily delay the case,” and instead ordered a 30-day
11 extension. (Dkt. 117; *see also* Dkt. 113-1 at 13.)

12 39. Several weeks later, Plaintiffs filed a Renewed Motion to Continue, attempting to
13 revisit the issue and arguing that Facebook “delayed [] providing relevant discovery, including by
14 failing to produce a significant proportion of relevant and responsive documents until October 13,
15 and October 28.” (Dkt. 134-1.) Once again, Facebook responded to Plaintiffs’ false assertions and
16 corrected the record. (Dkt. 135, 135-1.) This Court denied Plaintiffs’ motion. (Dkt. 136.)

17 40. Mr. Rudolph’s most recent declaration (Dkt. 138-3) again argues that Facebook
18 “delayed” production of its source code, “delayed” producing a significant portion of documents until
19 October 13-28, 2015, and “delayed” producing additional documents until November 3-7, 2015.
20 (Dkt. 138-3, ¶¶ 2–5.) Facebook already refuted the first two assertions were before the Court. (*See*
21 Dkt. 114-1 ¶¶ 8–36; 135-1 ¶¶ 2–10.) On Mr. Rudolph’s last point, he fails to mention that
22 Facebook’s November productions were in response to Plaintiffs’ Motion to Compel (Dkt. 112),
23 Magistrate Judge James’ Order on October 14, 2015 (Dkt. 130), and this Court’s Order on
24 November 3, 2015. (Dkt. 136.) In other words, the productions were the result of *Plaintiffs’* motions
25 to compel. Facebook produced all responsive documents it could locate after a reasonable search in a
26 timely manner. Although Mr. Rudolph is correct to point out that the November 7 productions were
27 significant in volume, this was through no fault of Facebook—it had repeatedly warned Plaintiffs that
28

1 their requests were extremely overbroad and would yield many irrelevant documents, and Facebook
2 undertook extensive efforts to try to reach a reasonable compromise. (Dkt. 131-1.) For example,
3 Facebook offered to provide Plaintiffs with representative documents for certain of Plaintiffs'
4 requests, but Plaintiffs rejected all offers for compromise and continued to litigate these issues.
5 (Dkt. 131-1, Ex. 1.)

6 41. Contrary to Mr. Rudolph's declaration, Facebook's production was substantially
7 complete as of September 30, 2015, with respect to the documents Facebook had agreed to produce at
8 that point. Productions after this date were primarily in response to Plaintiffs' Motion to Compel
9 (Dkt. 112, 113, 122), which were not even decided until after September 30. (See Dkt. 130, 136.)

10 **IV. Authentication Of Remaining Exhibits**

11 42. Attached as **Exhibit EE** is a true and correct copy of excerpts of the deposition
12 transcript of Dr. Jennifer Golbeck (dated December 16, 2015).

13 43. Attached as **Exhibit FF** is a true and correct copy of excerpts of the deposition
14 transcript of [REDACTED] (dated August 7, 2015).

15 44. Attached as **Exhibit GG** is a true and correct copy of excerpts of the deposition
16 transcript of [REDACTED] (dated August 10, 2015).

17 45. Attached as **Exhibit HH** is a true and correct copy of excerpts of the deposition
18 transcript of [REDACTED] (dated August 11, 2015).

19 46. Attached as **Exhibit II** is a true and correct copy of excerpts of the deposition
20 transcript of Ray He (dated October 28, 2015).

21 47. Attached as **Exhibit JJ** is a true and correct copy of excerpts of the deposition
22 transcript of Michael Adkins (dated October 28, 2015).

23 48. Attached as **Exhibit KK** is a true and correct copy of a document that begins with
24 Bates number FB000006429, which Facebook produced during this litigation.

25
26
27
28

EXHIBIT A

App. 16-17
Filed Under Seal

EXHIBIT B

App. 19
Filed Under Seal

EXHIBIT C

App. 21-29
Filed Under Seal

EXHIBIT D

App. 31-37
Filed Under Seal

EXHIBIT E

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
1	FB000000079	Josh Constine, <u>Facebook Allows Users to Upgrade to the New Messages Product. Why You Should</u> , Inside Facebook (January 10, 2011), <i>available at</i> http://www.insidefacebook.com/2011/01/10/allows-upgrade-new-messages/ .	This article describes how a Facebook Messages product update “automatically filters non-essential communications into an Other folder, allowing the main inbox to show only important messages [and] also routes sent messages to whichever device or interface Facebook deems is the most convenient for the recipient, whether that’s Chat, Messages, SMS, or email.” The author praises the storage capacity and searchability of Facebook’s Messages product, but he writes that some “important Messages may be being filtered out.” The author concludes that “[o]verall, Messages will help most Facebook users [because] [i]t anticipates the shift to using multiple devices and interfaces to conduct a single conversation . . . declutters the inbox by removing spammy and low-value Page and Event updates . . . [and] improves one of the core uses of Facebook—instant communication with friends.”
2	FB000000156	Jiakai Liu, <u>Inside Facebook Messages’ Application Server</u> , Facebook (April 28, 2011), <i>available at</i> https://www.facebook.com/notes/facebook-engineering/inside-facebook-messages-application-server/10150162742108920/ .	In this Facebook Note, Facebook software engineer Jiakai Liu describes the technical details of the infrastructure behind Facebook’s Messages product, including the internals of the application server used to manage this infrastructure. He writes that the server will run “pre- and post-processing as needed, and determin[e] the folder and thread where the message should be routed based on a number of signals.” He also indicates that “[w]hen reading messages, the server gets various statistics about the user’s mailbox, like its capacity; number of messages, threads and replies; and the number of friends with whom the user has interacted. It also gets folder statistics and attributes, the list of threads by various search criteria (folder, attributes, authors, keywords, and so forth), and thread attributes and the individual messages in the thread.” He also discloses that Facebook’s Messages product supports “full text search” by maintaining a “reverse index from keywords to matched messages.” He describes how Facebook “parse[s]” and “convert[s]” a new messages when it arrives, and writes that “[a]ll messages, including chat history, email, and SMS, are indexed in real time.” He concludes by noting that Facebook did testing of the new application server software via a “dark launch,” but that Facebook would “continue to roll out the new Messages system to all our users.”
3	FB000000163	Facebook, <u>Facebook Developer Documentation: “Like” Button</u> , Facebook - Internet Archive Wayback Machine (March 7, 2011), <i>available at</i> http://web.archive.org/web/20110307213924/http://developers.facebook.com/docs/reference/plugins/like/ .	This Internet Archive capture is Facebook’s developer documentation describing how to implement the “Like” button and “FAQs” about that implementation. It discloses that the number shown on a “Like” button “is the sum of [items including] [t]he number of inbox messages containing this URL as an attachment.”
4	FB000000166	Facebook, <u>Facebook Developer Documentation: “Like” Button</u> , Facebook - Internet Archive Wayback Machine (October 19, 2012), <i>available at</i> http://web.archive.org/web/20121019095652/http://developers.facebook.com/docs/reference/plugins/like/ .	This Internet Archive capture is Facebook’s developer documentation describing how to implement the “Like” button and “FAQs” about that implementation. It discloses that the number shown on a “Like” button “is the sum of [items including] [t]he number of inbox messages containing this URL as an attachment.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
5	FB000000173	Elliot Schrage, <u>Proposed Updates to our Governing Documents</u> , Facebook (November 21, 2012), <i>available at</i> http://newsroom.fb.com/news/2012/11/proposed-updates-to-our-governing-documents/ .	In this News Post, a Facebook employee writes that Facebook is “proposing some updates to two documents which govern our site: our Data Use Policy, which explains how we collect and use data when people use Facebook, and our Statement of Rights and Responsibilities (SRR), which explains the terms governing the use of our services.” He notes that Facebook would continue to post “significant” changes to the documents for review and comment and provide “additional notification mechanisms” informing users of any changes to them. He also summarizes certain updates to the Data Use Policy, including 1) “[n]ew tools for managing your Facebook Messages - replacing the ‘Who can send you Facebook messages’ setting with new filters for managing incoming messages”; 2) changes to how Facebook refers to certain products; 3) reminders about what’s visible to others on Facebook; and 4) tips for managing timelines. He concludes by encouraging readers to read the proposed changes to the documents and leave comments.
10	FB000000240	Thomas McMahon, <u>Facebook’s Like Number is More than Just People Clicking Like</u> , Twister MC (September 8, 2011), <i>available at</i> http://www.twistermc.com/36579/facebook-like/ .	Here, the author asks, “[D]id you know that the number of Likes is made up of more than just people clicking Like?” Quoting Facebook’s developer site, he writes that “[t]he number shown on a Like button is the sum of: ‘[t]he number of likes for the URL; [t]he number of shares for the URL – This includes copy/pasting a link back to Facebook; [t]he number of likes and comments on stories on Facebook about the URL; [and] [t]he number of inbox messages containing the URL as an attachment.’” Providing an example, the author notes that if you have a blog post with a “Like” button social plug in, the “Like number showing would include: . . . The number of times someone has sent the blog post URL to a friend via Facebook’s messaging system.” He concludes that “[b]asically, anytime that blog post URL is active on Facebook, a Like is added to the count.”
6	FB000000204	Nicholas Carlson, <u>The Truth About The Latest Facebook Privacy Scare Everyone Is Talking About</u> , Business Insider (October 4, 2012), <i>available at</i> http://www.businessinsider.com/facebook-private-messages-likes-2012-10/ .	After reporting that “[w]hen a Facebook user sends a link to a Web page via a private Facebook message, that Web page will get an extra ‘Like,’ if it is a Facebook-‘Like’able Web page,” the author argues that the various publications (including The Wall Street Journal, Forbes, and Gizmodo) characterizing Facebook’s conduct as “a privacy invasion” are incorrect. He writes that there is “a simple reason why”: “That ‘Like’ is only added to the page’s counter. There is no way to tell who added the like . . . [and] [i]f you do not reveal something said or shared in private to others, you are not invading their privacy.” The author goes on to demonstrate the incrementation of the social plugin count, and he explains that “[t]here is no reason for anyone to be upset about Facebook doing this.” He notes that “email providers like Gmail scan user emails all the time. Gmail does it to show relevant ads, fight spam, and slow down viruses.” He also writes that “services across the Internet use whatever method they can to keep track of the popularity of Webpages Google has a list of trends. The New York Times keeps track of most emailed stories.” He concludes that “there is nothing to see here,” telling people to “[m]ove along.” In an update to the article, the author quotes a Facebook spokesperson’s statement on the issue, which noted that “[w]hat makes up the number shown on [a] Like button [includes] [t]he number of inbox messages containing this URL as an attachment.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
7	FB000000213	Facebook, <u>Update to Messaging and a Test</u> , Facebook (December 20, 2012), <i>available at</i> http://newsroom.fb.com/news/2012/12/update-to-messaging-and-a-test/ .	In this News Post, Facebook announces updates to Facebook Messenger on mobile and Facebook Messages on the web. The article notes that “[i]n 2010 we introduced the Other folder, where less relevant messages go,” and it continues, “We’ve heard that messages people care about may not always be delivered or may go unseen in the Other folder. As we announced last month, we’re replacing the ‘Who can send me Facebook Messages’ setting with up-front filters that help to address this feedback.” The article then describes the two types of filtering that will be made available (Basic and Strict), noting that “Facebook Messages is designed to get the most relevant messages into your Inbox and put less relevant messages into your Other folder. [Facebook] [relies] on signals about the message to achieve this goal. Some of these signals are social—we use social signals such as friend connections to determine whether a message is likely to be one you want to see in your inbox. Some of these signals are algorithmic—we use algorithms to identify spam and use broader signals from the social graph, such as friend of friend connections or people you may know, to help determine relevance.” The article concludes that Facebook will “continue to iterate and evolve Facebook Messages over the coming months.”
8	FB000000221	Samantha Murphy Kelly, <u>Facebook: We’re Not Liking Brand Pages For You</u> , Mashable (October 4, 2012), <i>available at</i> http://mashable.com/2012/10/04/facebook-brand-like/ .	In this article, the author notes that “[i]t’s been widely reported on Thursday that Facebook is scanning messages sent to others with attached links to better gauge their interests and add to a brand’s Link count,” writing the information is “used only on the back-end for publishers to see the analytics of articles and shared URLs.” She quotes a Facebook spokesperson’s statement on the issue, and she writes that “[e]mail services such as Gmail have long taken this approach to target its users with ads or fight against viruses based on content written.” She concludes that “Facebook’s developer page related to the Like button states that the number of Likes is derived by the number of likes in the URL and the number of shares. This includes copying and pasting a link back to Facebook. It also includes the number of inbox messages containing the URL as an attachment.”
9	FB000000234	Ryan Singel, <u>Facebook’s E-mail Censorship is Legally Dubious, Experts Say</u> , Wired (May 6, 2009), <i>available at</i> http://www.wired.com/2009/05/facebook-e-mail-censorship-is-legally-dubious-experts-say/ .	Here, the author reports that “legal experts say Facebook may have gone too far [in] blocking not only links to torrents published publicly on member profile pages, but also examining private messages that might contain them, and blocking those as well.” The author writes that Facebook messages are “governed by the Electronic Communications Privacy Act, which forbids communications providers from intercepting user messages, barring limited exceptions for security and valid legal orders,” opining that “[w]hile the sniffing of e-mails is not unknown—it’s how Google serves up targeted ads in Gmail and how Yahoo filters out viruses, for example—the notion that a legitimate e-mail would be not be delivered based on its content is extraordinary.” The author notes that then-Facebook Chief Privacy Officer Chris Kelly “acknowledged that the site censors user messages based on links [b]ut [] insisted that Facebook has the legal right to do so, because it tells users they cannot ‘disseminate spammy, illegal, threatening or harassing content.’” The author quotes Mr. Kelly: “‘Just as many e-mail services do scanning to divert or block spam, prevent fraudulent, unlawful or abusive use of the service—or in the case of some services, to deliver targeted advertising—Facebook has automated systems that have the capability to block links. ECPA expressly allows Facebook to operate these systems. The same automated system that blocks these links may also be deployed where there is a demonstrated disregard for intellectual property rights.’”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
11	FB000000248	Julian Evans, <u>Facebook Launches Anti-Malware URL Scanning Service</u> , Julian Evans Blog.com (October 3, 2011), <i>available at</i> https://www.julianevansblog.com/2011/10/facebook-launches-anti-malware-url-scanning-service.html/ .	Here, the author reports that “Facebook is introducing URL (link scanning) protection for its users as from today (Oct 3rd, 2011).” The author notes that Facebook will “analyze each URL in real-time for potential malicious content.” He acknowledges that “Facebook already scans URLs for malicious links,” noting that “by adding Websenses cloud-based malware technology . . . , they further enhance the security offering to Facebook users.” He concludes that “[o]ne can only applaud Facebook for continuing to build user privacy and protection, even if it is becoming rather more complex for end users to understand.”
12	FB000000146	Jennifer Valentino-DeVries and Ashkan Soltani, <u>How Private Are Your Private Facebook Messages?</u> , Wall Street Journal (October 3, 2012), <i>available at</i> http://blogs.wsj.com/digits/2012/10/03/how-private-are-your-private-messages/ .	In this article, the authors report that an online video shows that Facebook “scans the links you’re sending—registering them as though you ‘Like’ the page you sent,” which the authors characterize as “one example of how online messages that seem private are often actually examined by computers for data.” They note that “[e]mail providers such as Gmail have long reviewed messages in order to spot spam and place ads,” and that Facebook has previously disclosed that the company “analyze[s] messages to filter spam and to detect conversations that could be related to criminal behavior.” The authors also indicate that Facebook’s Developer Guidance discloses that “the number of inbox messages containing a link to a page will count as ‘Likes’—indicating that the recording of these links isn’t some sort of new bug.” They opine that it is “not clear from Facebook’s data use policy that regular users would expect links in their messages to be scanned this way,” because “the policy simply says generally that Facebook gets ‘data about you whenever you interact with Facebook,’ including when you ‘send or receive a message.’” The authors update their article with a Facebook spokesperson’s statement about the social plugin bug. Additionally, reader comments on the article include a statement by someone who writes that he or she is “[n]ot surprised at all”; another who suggests that “Facebook should update their data use policy to reflect what they already disclose in their guidelines to developers”; and another who states that he is “fine with Google/FB scanning messages as long as private information isn’t released” but does not like “the ability for scammers to inflate the like score with this method.”
13	FB000000281	Joey Tyson, <u>Relevant Ads That Protect Your Privacy</u> , Facebook (September 30, 2012), <i>available at</i> https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125/ .	In this Facebook Note, the author describes several features that “give advertisers new ways of reaching people who use Facebook.” The author writes that “[m]any sites across the web provide free services by including advertisements. Facebook is no exception, and as we pursue our goal of making the world more open and connected, we have designed our service to show ads that help people discover products that are interesting to them. We also recognize that our users trust us to protect the information they share on Facebook.” The author also writes, “Advertising helps keep Facebook free. We believe we can create value for the people who use our services every day by offering relevant ads that also incorporate industry-leading privacy protections. In our view, this is a win-win situation for marketers and for you.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
14	FB000000331	KS Sandhya Iyer, <u>Likes Shared Privately on Facebook Increase Page's Like Count</u> , NDTV Gadgets (October 5, 2012), available at http://gadgets.ndtv.com/social-networking/news/links-shared-privately-on-facebook-increase-pages-like-count-275993/ .	Here, the author writes that “Facebook is keeping an eye on your private messages for URLs that have Like buttons and should be increased,” noting that “The Next Web further pointed out that the Like button entry on the Facebook Developers page states that the number shown on Like buttons on other websites is a total of likes of that URL, shares of that URL, likes and comments on Facebook stories about that URL and inbox messages containing that URL as an attachment.” The author asks, “[H]ow big a deal is it and does it invade Facebook user privacy?” She answers, “Probably not,” because the “‘Like’ is only added to the page’s counter [and] It does not reveal who added the Like.” The article concludes that “[i]f you do not reveal something said or shared in private to others, you are not invading their privacy.” She quotes a Facebook spokesperson’s statement on the issue, and she writes that “Facebook isn’t going to be axed for this move for the simple reason that email providers like Gmail scan user emails all the time” in order to “show relevant ads, fight spam, and slow down viruses.” The author further writes that “[w]hat Facebook is doing is just adopting one of the many services of tracking the popularity of Webpages.” She quotes Facebook’s statement that its “systems parse the URL being shared in order to render the appropriate preview, and to also ensure that the message is not spam.”
15	FB000000372	Doug Mataconis, <u>Your Facebook Chats are Being Monitored, By Facebook</u> , Outside the Beltway (July 13, 2012), available at http://www.outsidethebeltway.com/your-facebook-chats-are-being-monitored-by-facebook/ .	The author of this article writes that “Mashable is out with a report that Facebook routinely monitors user chats for suspicious or criminal activity,” quoting several paragraphs of the Mashable article. He notes that the “news was first broken” in a Reuters article from July 2012, which “describes one incident in which [Facebook’s] software did in fact catch a child predator.” The author continues, “As it turns out, this is all covered in the company’s Privacy Policies,” quoting two paragraphs of Facebook’s Privacy Policy. He concludes that “[i]t’s hard to argue with what Facebook is doing here,” stating that “there are some privacy concerns here, but Facebook is a private company and free to set its own policies on these issues” and that “it has a corporate brand to protect, not to mention the potential of liability, from being known as a place where parents can’t be sure that their teenager children can be safe.”
16	FB000000170	Britney Fitzgerald, <u>New Facebook Bug Scans Messages, Increases ‘Likes’: What You Need To Know</u> , Huffington Post Tech (October 4, 2012), available at http://www.huffingtonpost.com/2012/10/04/new-facebook-bug_n_1940339.html/ .	In this article, the author opens by noting that “Facebook is experiencing a bug—but it’s not quite the privacy breach [sic] that’s been previously reported by multiple news sources.” She reports that Facebook “has been scanning private messages for links to third-party websites that use Facebook’s ‘Like’ button, a social plug-in that lets users interact with a brand’s products, news articles and other types of content on webpages (without directly visiting the Facebook Page for that brand).” She writes that “Likes also increase when a Facebook user sends another user a message containing a URL to a page featuring the ‘Like’ button; this should only up the ‘Like’ count by one, but it’s actually inflating the count by two.” The author writes that Facebook “insists that this is nothing new,” quoting a Facebook representative, who noted that the issue where “counts are jumping by two . . . is a bug [but . . . the actual shares going up when things are sent in messages—that is standard behavior and you can find that in our documentation.” The author further indicates, “All information posted on the social networking site is accessible for company use. Thus, if you were to share the URL for this article through a Facebook message, Facebook can check out what you’re sending and adjust the ‘Likes’ at the top of this page—whether you clicked ‘Like’ on it or not.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
17	FB000000177	Michelle Fitzsimmons, <u>Report: Facebook scanning private messages, Liking on users' behalf</u> , Tech Radar (October 4, 2012), <i>available at</i> http://www.techradar.com/us/news/internet/report-facebook-scanning-private-messages-liking-on-users-behalf-1101999/ .	In this article, the author writes that various news sources have indicated that “Facebook is scanning users’ private messages and automatically issuing Likes on their behalf.” The author notes that a Facebook spokesperson directed him to the the “Like Button” section of Facebook’s developer site, and “specifically to information titled ‘What makes up the number shown on my Like button?’.” The author quotes the site, which she writes “explained that ‘the number shown is the sum of’ [items including] [t]he number of inbox messages containing this URL as an attachment.” She concludes that “[m]essage scanning isn’t anything new” and notes that “Gmail scans user emails to create targeted ads and Facebook also reportedly scans user messages to look for sexual predators and child pornography.”
18	FB000000183	Matt Hicks, <u>See the Messages that Matter</u> , Facebook (February 11, 2011), <i>available at</i> https://www.facebook.com/notes/facebook/see-the-messages-that-matter/452288242130/ .	In this Facebook Note, the author “announce[s] the next evolution of Messages,” providing detail about the new functionality of the Messages product. He indicates that users may now use SMS, chat, email or Messages; Facebook is providing an “@facebook.com” email address to every person on Facebook who wants one; Facebook messages will take the form of a “single conversation”; and that “your Inbox will only contain messages from your friends and their friends,” and “[a]ll other messages will go into an Other folder where you can look at them separately.” He concludes by inviting readers to take a tour of Messages and asking for thoughts and feedback.
19	FB000000187	Jessica Lee, <u>The Facebook Like Button, Dissected</u> , Bruce Clay (May 25, 2011), <i>available at</i> http://www.bruceclay.com/blog/facebook-like-button/ .	Here, the author examines the “Like button phenomenon, its various uses and why you need to be liked to survive in the age of online marketing.” She provides an overview of the “two variations” of the “Like” button, writing with respect to the “Like” button social plugin that “Facebook notes that the number of likes shown on any given Web page or object is the sum of [items including] [t]he number of inbox messages containing this URL as an attachment.”
20	FB000000251	Tekla S. Perry, <u>The Reengineering of Facebook Messages</u> , IEEE Spectrum (November 2, 2011), <i>available at</i> http://spectrum.ieee.org/computing/software/the-reengineering-of-facebook-messages/ .	In this article, the author discusses in detail how and why Facebook “completely redesign[ed] its messaging system” in 2009. The author discusses the rationale behind the “informal formatting” of the Messages product and the decisions to remove subject lines and store live chats in the same thread as messages. After explaining how Facebook engineers determined how to store messages, the author writes that “the engineers turned to the problem of spam, a bane of e-mail services.” She writes, “While traditional spam filters look mostly at message content, the spam filters built into Facebook messages also pay a lot of attention to who the message senders are. Messages from your friends and friends of friends bypass the spam filters and go directly into your in-box, unless you’ve changed the default or previously moved messages from that person out of your in-box; messages from people you aren’t connected to through a friend, along with announcements from organizations or businesses, go into a folder called ‘other.’ Messages with spamlike content and no friend-of-friend connection go into a separate spam file, the link to which is tucked away at the bottom of the ‘other’ mailbox and requires scrolling past every message in that mailbox to be seen.” The author concludes by opining that “the future of everyday communications will look a lot more like Facebook Messages.”
21	FB000000278	Donna Tam, <u>Facebook Processes More Than 500 TB of Data Daily</u> , Cnet (August 22, 2012), <i>available at</i> http://www.cnet.com/news/facebook-processes-more-than-500-tb-of-data-daily/ .	Here, the author writes that “[s]ince Facebook uses [its] data to build its user experience, it wants teams from across the company—whether they sell ads or build functions—to be able to access any of the data as needed.” The author notes that the Facebook employee who “runs Facebook infrastructure” indicated that “this keeps the creation and improvement of Facebook features as fast as possible . . . [and [t]hese nearly real-time efforts apply to most functions throughout the site because people won’t use the site if the personalized experience is poor, or slow.” The author also writes that Facebook keeps all of its data in one place for “easy access,” but that Facebook “has a zero-tolerance policy when it comes to any abuse from this broad access.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
22	FB000000285	Sam Biddle, <u>Facebook is Reading Your Messages and Liking Things For You (Updated: Not as Bad as We Thought)</u> , Gizmodo (October 4, 2012), <i>available at</i> http://gizmodo.com/5948948/facebook-is-reading-your-messages-and-liking-things-for-you/ .	Here, the author writes that Facebook’s “scanning increases the Like count for a given page Like-able link just by you talking about it” in a Facebook message. He indicates that “[a]uto-scanning is nothing new: Gmail has done it since day one to serve us ads,” and he opines that “there are serious potential personal consequences here.” The author continues by noting that “[i]t turns out this was just a very unlikely coincidence that played out in more than one place—the auto-liking only applies to external links with embedded Facebook liking.” He illustrates how a message increments the social plugin count, writing that “your name isn’t being associated publicly with something you’re talking about privately—but if even a mention is enough to kick up a Like, it seems like that’s pretty heavily diluting (even further) what ‘like’ even means—from preference to mere reference.” The author updates the article by quoting a Facebook spokesperson’s statement on the issues raised in the article.
23	FB000000301	Paul Shea, <u>Facebook Confirms Peeking at Private Messages</u> , Value Walk (October 4, 2012), <i>available at</i> http://www.valuewalk.com/2012/10/facebook-inc-fb-peeking-at-private-messages/ .	Here, the author reports that Facebook “confirmed that it scans private messages between users,” and that “these scans [] caused the likes of linked content to increase.” He writes that “a series of bots [] scan private messages for links to content that contains ‘Like’ buttons [and] [i]f a Like button is detected, however, a bug is activated, whereby the linked content has its likes increased by two.” The author further writes that it “may be news to some long time Facebook users” that the “‘Like’ counter measures not just clicks on a Like button, but takes into account sharing of the content, as well as comments on the content, and now private messages.” He continues, “Emil Protalinski, the writer at thenextweb.com who originally picked up on this story, rightly points out that the scanning of private messages for data on content is not the same as scanning for the same data on comments, or public declarations of ‘Like,’” and he notes that “[t]his is not the first time a company has been indicted for scanning the content of users’ private messages,” writing that “Google Inc and other web mail providers have been scanning users’ emails for years, in order to pick the advertisements best suited to them.” He quotes a Facebook spokesperson’s statement on the issue, and he concludes that “Facebook Inc [sic] has certainly not crossed a line with this latest news, any more than they have on hundreds of other occasions,” and that “[b]ecause of the nature of the business, the company will be dodging privacy issues for as long as it operates.”
24	FB000000305	Brittany Darwell, <u>Facebook Clarifies How Like Plugin Works, Addresses Privacy Concerns</u> , Social Times (October 4, 2012), <i>available at</i> http://www.adweek.com/socialtimes/facebook-clarifies-how-like-plugin-works-addresses-privacy-concerns/285167/ .	In this article, the author reports that Facebook “responded to reports today that alleged the social network was scanning private messages and Liking pages on users’ behalf” by stating that “the Like count of an article or webpage will increase when users share the link via direct messages [but] that no private information is shared . . . URLs sent through private messages are not shown publicly on user profiles and users will not see a friend’s name or photo next to a Like button if the person shared the article privately.” The author opines that is it not “completely clear to outsiders that the total includes actions that were made by clicking the button directly, as well as the number of times the link was copy-pasted into a Facebook post or message, which is why some users thought the social network had a security flaw.” She acknowledges that “Facebook explains this in the FAQ about the Like button plugin,” quoting the relevant FAQ. The author writes that “we see this as similar to site visitor widgets, which increase whenever a user visits a webpage but do not reveal who visited” and that accordingly, “privacy implications are minimal.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
25	FB000000328	Rick Burgess, <u>Facebook Bug Silently Tallies Up Extra 'Likes'</u> , TechSpot (October 5, 2012), available at http://www.techspot.com/news/50416-facebook-bug-silently-tallies-up-extra-likes.html/ .	This article reports that Facebook is facing “scrutiny” after a “security researcher uncovered a flaw in [Facebook’s] ‘like’ system which appears to be responsible for liking sites an unintended number of times.” The author writes that “Facebook reiterated though that some behaviors will generate likes without explicitly liking something, such as messaging a URL to a friend,” though “some find the sincerity of such a practice nebulous.” He writes that “[on Facebook for Developers . . . there are actually four ways to generate likes [and] . . . only one of those methods actually requires users to click a like button.” He concludes by citing Facebook’s recent “initiative which intends to fortify the integrity of Facebook’s likes and shares,” including deploying “automated tools . . . with the intent of deleting disingenuous likes that were determined to be purchased or originate from malware or compromised accounts.”
26	FB000000376	Lisa Vaas, <u>How Facebook Catches Would-Be Child Molesters by Analyzing Relationships and Chat Content</u> , Naked Security (July 16, 2012), available at https://nakedsecurity.sophos.com/2012/07/16/facebook-child-molester/ .	In this article, the author reports that “[l]aw enforcement is hailing Facebook for using its little-known data monitoring technology to spot a suspicious conversation about sex between a man in his early thirties and a 13-year-old girl from Florida,” and that “Facebook doesn’t talk much about this technology, which scans postings and chats for criminal activity.” She notes that Facebook’s then-Chief Security Officer Joe Sullivan said that Facebook’s “monitoring software analyzes relationships to find suspicious conversations between unlikely pairings” and “relies on archives of real-life chats that preceded sexual assaults.” She notes that Mr. Sullivan said that “the last thing the company wants is for its users to feel like they’re being eavesdropped on.” The author ends by quoting Mr. Sullivan, who says, “We’ve never wanted to set up an environment where we have employees looking at private communications, so it’s really important that we use technology that has a very low false-positive rate.”
27	FB000000391	Adam Estes, <u>Facebook’s Spying on You For a Good Cause</u> , Motherboard (July 13, 2012), available at http://motherboard.vice.com/blog/facebook-s-reading-your-messages-but-it-s-for-a-good-cause/ .	Here, the author writes that “[w]hether you realize it or not, a bundle of sophisticated technology is constantly scanning through Facebook interactions—wall posts, messages, chats—looking for sexual predators.” The author reports that Facebook’s program is “part of an aggressive effort the social network has made over the past few years to protect the safety of its 13- to 18-year-old users, and few would argue that the stated goals of the program aren’t sound.” He writes that “there’s something unnerving about Facebook reading your messages,” because “[p]reventing crime is one thing, but surveilling the most intimate user behavior is something completely different.” The author also notes that “Facebook is obviously aware of the privacy concerns and insist that their technology only spots the bad guys,” quoting Facebook’s then-Chief Security Officer Joe Sullivan, who says, “We’ve never wanted to set up an environment where we have employees looking at private communications, so it’s really important that we use technology that has a very low false-positive rate.” He concludes that “it’s easy to think of Facebook’s anti-pedophile software as just another form of moderation” because “[t]he vast majority of the scanning is also algorithmic, so it’s not like you have a bunch of Facebook employees poring over your every word,” writing that “[i]n truth, it’s a machine that’s trying to spot patterns and red flags” for “a good cause.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
28	FB000000393	Cale Guthrie Weissman, <u>Facebook Uses Scanning Technologies, Alters Authorities About Content</u> , OpenNet Initiative (July 16, 2012), <i>available at</i> https://opennet.net/blog/2012/07/facebook-uses-scanning-technologies-alerts-authorities-about-content/ .	Here, the author writes that “Facebook regularly scans user content for criminal activity, but the monitoring program is something the social media giant has generally kept quiet about. “ Quoting a report from Reuters, the author acknowledges that “this sort of scanning is commonplace for platforms like Facebook—most large social media companies scan chats for inappropriate language and exchange of personal information,” but he opines that many social media platforms “walk a tightrope between utilizing these tactics to safeguard against illegal activity and providing a less restrictive social media platform that will engage users.” The author writes that “[s]canning users’ content is not new terrain for Facebook,” citing information leaked that April [2012?] “showing the kinds of user information Facebook releases to authorities when subpoenaed” and the “Information for Law Enforcement Authorities” section of Facebook’s website. The author quotes Facebook’s then-Chief Security Officer Joe Sullivan, who says, ““We’ve never wanted to set up an environment where we have employees looking at private communications, so it’s really important that we use technology that has a very low false-positive rate.”” He concludes that “[s]canning technologies of this design are just beginning to come to the forefront for various websites,” and that Facebook’s “example highlights the tactics used and suggests a possible upward trend in surveillance by social media platforms.”
29	FB000000395	Michael Walsh, <u>Did You Know that Facebook Monitors Postings and Chats for Sexual Predators?</u> , NY Daily News (July 16, 2012), <i>available at</i> http://www.nydailynews.com/news/crime/facebook-monitors-postings-chats-sexual-predators-article-1.1115392/ .	The author of this article writes that Facebook “uses monitoring software that can scan and flag suspicious messages to minors from potential predators.” Citing an instance in which Facebook’s software effectively flagged “suspicious conversations between a man in his early thirties and a 13-year old girl,” the author opines that Facebook’s “surveillance practice is fraught with legal complexity” and “Facebook tends to avoid comment on this practice, because the organization doesn’t want to create scare stories or stir surveillance paranoia.” The author quotes Facebook’s then-Chief Security Officer Joe Sullivan, who says, ““We’ve never wanted to set up an environment where we have employees looking at private communications, so it’s really important that we use technology that has a very low false-positive rate.”” The author concludes that “[t]o minimize the risk of inappropriate surveillance the software and procedures are designed to err on the side of monitoring caution.”
30	FB000000399	Jemima Kiss, <u>Facebook Puts Faith in its Software Smarts to See Off Sexual Predators</u> , The Guardian (April 15, 2010), <i>available at</i> http://www.theguardian.com/technology/2010/apr/16/facebook-software-sexual-predators/ .	This article reports that “Facebook has developed sophisticated algorithms to monitor its users and detect inappropriate and predatory behaviour, bolstering its latest raft of initiatives to improve the safety of its users.” The author writes that “[h]aving launched an education campaign, an improved reporting procedure and a 24/7 police hotline,” Facebook indicated that it “has introduced a number of algorithms that track the behaviour of its users and flag up suspicious activity.” The author also notes that Facebook has another filter, “common on web publishing sites [] [that] scans photo uploads for skin tones and blocks problem images.” She quotes Facebook employee Matt Kelly, who says that Facebook “balance[s] its duty to respect its users while meeting its legal obligations,” and that Facebook’s “corporate philosophy about data is that the user is in control, and they choose how to share and distribute it. She ends by noting that one privacy campaigner believes Facebook “needed to do more to stop persistent stalkers and bullies who could use multiple identities, and cautioned against the automated profiling of users.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
31	FB000000420	Josh Wolford, <u>Should Facebook Monitor Chats to Help Snag Child Predators?</u> , WebProNews (August 23, 2012), available at http://www.webpronews.com/remember-how-facebook-is-monitoring-chats-for-criminal-activity-well-it-worked-kind-of-2012-08/ .	Here, the author begins by stating that “social networks are social – you’re actively sharing content with the world,” and “anybody who thinks they can maintain a pristine level of privacy and security while still enjoying the benefits of a social community is probably deluding themselves.” He writes that “recently, it was revealed that Facebook actively patrols user communications for unlawful activities,” and that “Facebook is actively monitoring our chats and messages.” The author notes that Facebook “revealed that it’s common practice for their teams to scan chats, searching for criminal activity” and that “[i]t’s mostly algorithms that handle this part, but once something is flagged Facebook employees make the final decision on whether or not it merits calling the authorities.” He posits that “[t]here’s really no denying that it can work,” as “[s]canning chats for suspicious activity can help to thwart child predation,” noting that “there are still privacy concerns to consider.” He writes that “[n]ot everyone is convinced that Facebook has the right to monitor ‘private’ communications,” but states, “Then again, you are using their (free) service to send and receive communications, and at least now it’s with the public knowledge that the company may be monitoring them.” He adds that Facebook is “not the only one[] engaging in this type of monitoring.”
32	FB000000066	Sue Keogh, <u>How accurate is the Facebook Like count?</u> , The Wall (April 8, 2011), available at http://wallblog.co.uk/2011/04/08/how-accurate-is-the-facebook-like-count/ .	Referencing a blog post that suggests that the “accuracy” of the number of “Likes” indicated for a given Facebook page on the website may be as low as 39%, the author of this article writes that the “Like” count on a third-party website also reflects additional actions other than affirmative clicks on the “Like” button. The author quotes Facebook’s Developer Guidance, which explains that “[t]he number shown is the sum of . . . [actions including] [t]he number of inbox messages containing this URL as an attachment.” She concludes that “the information is out there, if you know where to look. I might even click Like to help spread the word.”
33	FB000000068	Bianca Bosker, <u>Facebook’s Paid Messages Test Taxes You For Being Social</u> , Huffington Post Tech (December 20, 2012), available at http://www.huffingtonpost.com/bianca-bosker/facebook-messages-test-_b_2341521.html .	This article concerns Facebook’s testing of a new program that permits individuals with whom a user is connected to “pay to re-route their message from the ‘other’ heap straight to your inbox.” The author notes that this feature “is being rolled out in conjunction with new filters for Facebook’s messaging system that aim to ensure important messages don’t go unseen in the ‘Other’ inbox.” She also writes that “[a]s a user who receives no shortage of spam messages, I’m all for cutting back on clutter or fining advertisers who want to get hold of me in my inbox, uninvited,” but she labels the payment proposal “anti-social.” The author quotes Facebook’s statement explaining that the test is “‘designed to address situations where neither social nor algorithmic signals are sufficient. For example, if you want to send a message to someone you heard speak at an event but are not friends with, or if you want to message someone about a job opportunity, you can use this feature to reach their Inbox. For the receiver, this test allows them to hear from people who have an important message to send them.’” Acknowledging that “[k]eeping savvy scammers at bay is a gargantuan challenge for Facebook,” she argues that “Facebook profits from allowing people—and, most likely, brands—to take up your time when you made clear you didn’t want them to,” and she expresses concerns that the test is “more like a fix for Facebook’s profit push than a solution to overcrowded inboxes.”
34	FB000000073	<u>How to get share counts using graph API</u> , Stack Overflow (June 15, 2012), available at http://stackoverflow.com/questions/5699270/how-to-get-share-counts-using-graph-api/ .	On this developer forum, a user requests “a way to get share counts of an URL using graph API.” A user named “Jim Rubenstein” responds on June 15, 2012, clarifying that Facebook’s Graph API is a way to get the “share count,” which is “not equal to the one you see on the Like button, since that number is the sum of [items including] [t]he number of inbox messages containing [the] URL as an attachment.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
35	FB000000077	Jessican Guynn, <u>Facebook Looks To Cash In On User Data</u> , Los Angeles Times (April 17, 2011), available at http://articles.latimes.com/2011/apr/17/business/la-fi-facebook-ads-20110417/ .	In this article, the author notes that “[p]rofiles, status updates and messages all include a mother lode of voluntarily provided information,” and that Facebook uses this information “to help advertisers find exactly who they want to reach.” The author describes how Facebook is helping advertisers reach their target audiences with precision: “Facebook doesn’t have to guess who its users are or what they like. Facebook knows, because members volunteer this information freely—and frequently—in their profiles, status updates, wall posts, messages and ‘likes.’ It’s now tracking this activity, shooting online ads to users based on their demographics, interests, even what they say to friends on the site—sometimes within minutes of them typing a key word or phrase.” The author also suggests that Facebook’s ability to “mine data and sell advertising based on what its members voluntarily share amounts to electronic eavesdropping on personal updates, posts and messages that many users intended to share only with friends,” but she concedes that “any information users post on the site—hobbies, status updates, wall posts—is fair game for ad targeting.” The article concludes by quoting a Facebook user who says she enjoys “receiving ads from merchants”: “I don’t feel any weird privacy thing. We are all putting everything out there already.”
36	FB000000083	Rove Monteux, <u>Facebook Graph API exploit that let[s] you pump up to 1800 ‘Likes’ in an hour</u> , Rove Monteux (October 5, 2012), available at http://rmonteux.wordpress.com/2012/10/05/facebook-graph-api-exploit-that-lets-you-pump-up-to-1800-likes-in-an-hour/ .	In this post, the blogger explains that “simply private messaging an URL to some people on Facebook will increase the ‘like’ count for the given URL.”
37	FB000000087	Bianca Bosker, <u>Facebook Home’s Ultimate Goal: Ingesting Your Messages</u> , Huffington Post Tech (April 11, 2013), available at http://www.huffingtonpost.com/2013/04/11/facebook-home-messages_n_3063609.html/ .	Reporting on the launch of Facebook Home, Facebook’s smartphone software, the author writes that “tech industry analysts note that the sooner people channel their chatting through Facebook, the sooner Facebook can turn messaging from communication between friends into a moneymaker that involves brands. More messaging will give Facebook more data it may use to provide advertisers with personal, personalized ways of interacting with its members.” The author notes that “Facebook’s Messenger app currently gives people the option to attach location information to each post,” and that Facebook next “might analyze the content of messages to serve up ads targeted to each conversation, much like Gmail.” She quotes an analyst who says, “[Facebook’s messaging platform] is not just for connecting people. It’s for connecting brands, too.” The author also suggests that “[w]hether users would accept advertising via messages—private, personal and traditionally off-limits to brands—remains to be seen,” quoting an analyst who says that “[t]here’s a certain creepy factor to that, but users are getting much more comfortable trading privacy for convenience.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
38	FB000000097	<p>Emil Protalinski, <u>Facebook Confirms It Is Scanning Your Private Message For Links To Increase Like Counters</u>, The Next Web (October 4, 2012), available at http://thenextweb.com/facebook/2012/10/04/facebook-confirms-it-is-scanning-your-private-messages-for-links-so-it-can-increase-like-counters/.</p>	<p>Here, the author writes that Facebook “is monitoring your private messages for links that have Like buttons and should be increased,” and he quotes a Facebook spokesperson’s statement about the issue: “We did recently find a bug within our social plugins where at times the count for the Share or Like goes up by two, and we are working on [a] fix to solve the issue now. To be clear, this only affects social plugins off of Facebook and is not related to Facebook Page likes. This bug does not impact the user experience with messages or what appears on their timelines.” The author indicates that while this was “news” to him, “this was clearly the case before as on the Like button web page over on Facebook Developers, the social networking giant says the number shown on a Like button is the sum of [items including] [t]he number of inbox messages containing this URL as an attachment.” The author writes that he had “known for a while that the Like button isn’t a counter of just Likes,” but he opines that “private messages . . . have privacy questions attached to them.” He notes that Facebook confirmed that “[w]hen the count is increased via shares over private messages, no user information is exchanged, and privacy settings of content are unaffected. Links shared through messages do not affect the Like count on Facebook Pages.” In an update to the article, the author quotes Facebook’s explanation of the situation: “Our systems parse the URL being shared in order to render the appropriate preview, and to also ensure that the message is not spam.”</p>
39	FB000000104	<p>Alicia Eler, <u>Facebook Is Using Your Data Whether You Like It Or Not</u>, Read Write (November 28, 2011), available at http://readwrite.com/2011/11/28/facebook-is-using-your-data-whether-you-like-it-or/.</p>	<p>Here, the author discusses the implications a European Commission Directive that purportedly “ban[s] targeted advertising unless users specifically say they want it” may have on Facebook. In response to the question, “Why isn’t this happening in America?,” the author writes, “[Because] [a]ll 800 million Facebook users agree to let the company use their personal information.” She further writes that “Facebook has information about a user’s friends, family, education background in addition to Facebook such as ‘likes’ and everything that gets posted to Facebook Walls . . . Messages and ‘chats’ are stored, too, even if the user deletes them.” She also highlights that “Facebook denies tracking peoples’ behavior to serve advertising . . . denies selling users’ personal information to third parties . . . claims that advertisers only see ‘anonymous and aggregate information,’ using that to serve up targeted ads . . . [and] does not target individual users.” The author also notes that “with an IPO in the works, and Facebook’s move toward becoming self-sufficient, there’s no denying that advertising on the site has increased,” concluding by noting recent Federal Trade Commission scrutiny of Facebook’s practices.</p>
40	FB000000106	<p><u>Facebook Launches Messaging System With In-Bound Message Filter</u>, Out Law (November 10, 2010), available at http://www.out-law.com/page-11555/.</p>	<p>This article reports on Facebook’s launch of the Messages product and its features. The author quotes Facebook’s statement that “[i]t seems wrong that an email message from your best friend gets sandwiched between a bill and a bank statement . . . It’s not that those other messages aren’t important, but one of them is more meaningful. With new Messages, your Inbox will only contain messages from your friends and their friends. All other messages will go into an Other folder where you can look at them separately.” Noting that “[c]ritics of Facebook’s past approaches to user privacy will be assessing the system closely,” the author quotes a researcher who states that “Facebook announced it will not utilize the content of users’ personal messages to target advertising . . . This is surprising, considering doing so is typical among web-based email clients; both Gmail and Yahoo Mail scan users’ messages for keywords in order to better serve relevant advertising.” The author concludes by quoting a technology consultant who opines that “Facebook would be able to track vital information through the Messages system.”</p>

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
41	FB000000109	Ellis Hamburger, <u>How To Find All The Private Messages Facebook Is Hiding From You</u> , Business Insider (December 12, 2011), <i>available at</i> http://www.businessinsider.com/facebook-messages-other-folder-2011-12/ .	This article explains how to access the “Other Messages” folder in Facebook Messages, noting that “Facebook often groups messages from people you aren’t ‘Friends’ with into a spam-box-evoking ‘Other Messages’ folder.” The author writes, “While most messages that get filtered into your Other folder are in fact spam, it’s definitely worth digging through once in a while.”
42	FB000000110	Kashmir Hill, <u>Facebook Scans Private Messages To Hand Out Public ‘Likes’</u> , Forbes (October 4, 2012), <i>available at</i> http://www.forbes.com/sites/kashmirhill/2012/10/04/facebook-scans-private-messages-to-hand-out-public-likes/ .	The author writes that Facebook “scans [] private messages to friends, and when it sees a link to a ‘Likeable’ page, it doles out ‘Likes’ accordingly.” The article summarizes the findings of the Wall Street Journal article on this topic written by Ashkan Soltani and states, “We already know that Google scans our Gmail to target us with ads and that Facebook scans our inboxes looking for sexual predators and child porn, but many users may not have realized that the links they were exchanging privately resulted in a public—though anonymous—endorsement of said links.” The author includes a statement by a Facebook spokesperson on the issue: “‘Many websites that use Facebook’s ‘Like’, ‘Recommend’, or ‘Share’ buttons also carry a counter next to them. This counter reflects the number of times people have clicked those buttons and also the number of times people have shared that page’s link on Facebook. When the count is increased via shares over private messages, no user information is exchanged, and the privacy settings of content are unaffected. Links shared through messages do not affect the Like count on Facebook Pages.’” The article also includes an update that reads, “A spokesperson also emphasizes that this [is] a third-party Social Plug-in version of the ‘Like’ button and that it is meant to reflect engagement rather than endorsement.”
43	FB000000119	Ken Yeung, <u>Facebook Updates Messages Feature With Filtering, Tests A Service To Let People Pay To Send Them</u> , The Next Web (December 20, 2012), <i>available at</i> http://thenextweb.com/facebook/2012/12/20/facebook-messages-now-with-filters/ .	Here, the author reports on Facebook’s addition of two “filters to help solve the problem of finding messages that should be seen and seeing those that shouldn’t” to the Messages product. The author notes that “[t]here are many signals that go into determining what gets through to a user’s Message inbox, but one new signal Facebook is testing is allowing some users the ability to pay in order to help get their messages delivered, regardless of friendship status on the network.” He mentions the “Other” folder in Facebook Messages that “basically acts as the catch-all for all communications that it deems to have low relevancy,” positing that “[i]t’s too bad that a few innocent messages get tagged and removed because of this filter.” He concludes by explaining that the settings for the new filters will be “visible right with the Messages screen.”
44	FB000000148	Doug Gross, <u>How You Help Facebook Make Millions</u> , CNN Tech (May 16, 2012), <i>available at</i> http://www.cnn.com/2012/05/16/tech/social-media/facebook-users-ads/ .	In this article, the author writes that the following are the “building blocks” of Facebook as “a multibillion-dollar company”: “Every post you ‘like.’ Every friend you add or fan page you join. Every place you check in, and every Web page you recommend.” The author writes that “Facebook’s unprecedented advertising advantage is built upon the service it provides. As users interact with the site, they gradually build a fuller and fuller picture of themselves. That, in turn, lets Facebook sell advertisers on its ability to put their product in front of the people most likely to be interested.” He notes that Facebook’s advertising model has “made some folks antsy,” quoting an Associated Press/CNBC poll that found that “three out of five users say they have little or no faith that the company will protect their personal information.” The author concludes by quoting an analyst who “‘expects’” that Facebook’s “‘data-driven model [will] keep making money well into the future.’”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
45	FB000000180	Phil Villarreal, <u>Rescue Messages From Facebook's De Facto Spam Filter</u> , Consumerist (December 11, 2011), available at http://consumerist.com/2011/12/15/rescue-messages-from-facebooks-de-facto-spam-filter/ .	In this article, the author discusses Facebook's "Other" folder in the Messages product, writing that "[w]hen Facebook thinks you don't particularly want to read a message that's sent your way, it redirects it into" that folder. He writes that "[s]ome users forget to check the box regularly, and others may not even be aware that they have it," and he provides information about how to access the folder.
46	FB000000194	Greg Finn, <u>The Formula Behind The Facebook 'Like' Number</u> , Marketing Land (October 17, 2012), available at http://marketingland.com/the-formula-behind-the-facebook-like-number-24069/ .	Here, the author reports on the "uproar" surrounding reports that "messages were not only being crawled, but also used towards the overall 'Like data' of a page." He writes that "[o]ne of the important lessons that marketers learned from the situation was that the "'Like count' wasn't really about likes, rather other interactions (and messaging) that occurs on Facebook." He examines what goes into "Facebook Like data," quoting Facebook's Developer site and noting that "four different variables make up the Like number [including] [t]he number of inbox messages containing this URL as an attachment." He writes that a Facebook spokesperson confirmed that the listed elements are "all counted into the overall Facebook Like data."
47	FB000000217	JVG, <u>Facebook Tweaks Messages With Inbox Filters and Tests Pay-to-Deliver Option</u> , Venture Beat (December 20, 2012), available at http://venturebeat.com/2012/12/20/facebook-messages-inbox/ .	Here, the author reports on Facebook's announcement that it was "tweaking the Facebook Messages inbox experience to better ensure that relevant messages get to your inbox." The author writes that "[t]he new inbox filters, which are rolling out globally, are Facebook's way of correcting a broken system. The company currently routs messages to your inbox or other folder based on your settings, but it has found that it pushes too many 'high signal' messages (read as: messages you probably want to go to your Other folder, where they likely go unseen. To fix the problem, Facebook has created two filters, basic and strict, that will allow certain types of messages to reach your inbox that otherwise would not . . . Both options, however, use the 'mostly' terminology to allow for instances when Facebook puts its algorithmic magic to work and determines that a high signal message should get through." The author also reports that Facebook is launching a "small test" to allow people that are not your Facebook friends to pay a fee to send messages directly to your inbox.
48	FB000000237	Oliver Chian, <u>Facebook Messages Isn't a Gmail Killer—And That's the Problem</u> , Forbes (November 15, 2010), available at http://www.forbes.com/sites/oliverchiang/2010/11/15/facebook-messages-isnt-a-gmail-killer-and-thats-the-problem/ .	In this article, the author reports on the launch of the Facebook Messages product, arguing that it's a "problem" that the product is not a "Gmail killer." He provides a "quick rundown" of the features of Facebook Messages, writing that the product "takes all these bits of conversation and keeps a collective conversation history" and "filters messages based on your Facebook social graph." He notes, for example, that "[t]raditional spam emails will end up in Junk" and that Facebook users "will have control over this filtering too" because they can "move it manually [and] [t]he system will remember your choices and change your filtering preferences accordingly." The author writes that the "main problem" about Facebook Messages is that it "has no way of telling if your mother is sending an important email about your cousin's wedding, or a forwarded email about the billionth funny cat video ever made."
49	FB000000276	Jay Yarow, <u>How to Find Facebook Messages that Facebook is Hiding From You</u> , Business Insider (June 15, 2012), available at http://www.businessinsider.com/facebook-messages-spam-filter-2012-6/ .	Here, the author writes that Facebook "has a pretty aggressive spam filter to keep messages from creepers, and trolls from hitting your Facebook message inbox," opining that the spam filter is "sometimes too aggressive, and grabs messages that aren't spam." The author also provides instructions about how to check Facebook messages in the "Other" folder.

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
50	FB000000312	Donna Tam, <u>To Facebook, A Shared Link is As Good as a Like</u> , Cnet (October 4, 2012), available at http://www.cnet.com/news/to-facebook-a-shared-link-is-as-good-as-a-like/ .	Here, the author reports that “[a] recent bug adds two Likes to the count instead of one, and Facebook said it’s working to fix that.” The author writes that “the feature may rankle some users who don’t want to be part of an overinflated counter” or others who “feel violated” that Facebook “know[s] what you’re sending a Friend.” She notes Facebook says “this feature doesn’t affect Like counts on Facebook pages and it’s not an invasion of privacy since the Likes on the plugs-ins are anonymous,” quoting a Facebook spokesperson’s statement on the issue in full. She writes that a Facebook representative also confirmed that “Facebook does scan any links that pass through the network to look for spam,” including “links you send to a friend through messages,” and that “Facebook automatically reviews the links before generating a link preview.” The author concludes by noting that “even if you were sharing a link to show a friend something you don’t like, you’d still be adding to the page’s Like numbers.”
51	FB000000314	Mark Langshaw, <u>Facebook Adding Likes on Users’ Behalf</u> , <i>Says Report</i> , Digital Spy (October 5, 2012), available at http://www.digitalspy.com/tech/news/a410470/facebook-adding-likes-on-users-behalf-says-report.html#~p6spSJD5SKvz21/ .	This author reports that a “security expert discovered that sending a web address to a friend automatically adds two likes to that page, suggesting that [Facebook] is scanning private messages.” The author notes that “Facebook has responded to the report’s findings and issued a statement denying that privacy information has been exposed,” quoting certain portions of Facebook’s official statement, including the following: “Absolutely no private information has been exposed Each time a person Shares a URL to Facebook, including through messages, the number of Shares displayed on the social plugin for that website increases. Our systems parse the URL being shared in order to render the appropriate preview, and to also ensure that the message is not spam. These counts do not affect the privacy settings of content, and URLs shared through private messages are not attributed publicly with user profiles.” The author concludes that “[a]lthough Facebook also stressed that the additional likes are anonymous and will not appear on users’ timelines, critics have pointed out that people who share pages to highlight negative content are making the site appear more popular.”
52	FB000000335	Liz Klimas, <u>Why is the Privacy of Personal Facebook Messages Being Called Into Question—Again?</u> , The Blaze (October 5, 2012), available at http://www.theblaze.com/stories/2012/10/05/why-is-privacy-of-personal-facebook-messages-being-called-into-question-again/ .	This author writes that the other publications have reported that “including links in private messages [on Facebook]—if these links had a ‘like’ button associated with them –would increase the “likes” on that actual page by two.” The author writes that “Facebook has responded saying that there was a bug identified in the system that was accidentally counting one ‘like’ or ‘share’ of a link or post as two” and was “working to fix it.” She writes that “Facebook emphasized that ‘no private information has been exposed,’” and that this means that “if you receive a message containing a link that has a ‘like’ button, you are not automatically ‘liking’ this item on your Timeline.” The author continues by noting that “it’s probably news for many” that the social plugin counter “is not just measuring clicks but sharing content as well,” and she quotes another publication that reported that “[O]n the Like button Web page over on Facebook Developers, the social networking giant says the number shown on a Like button is the sum of: [t]he number of likes of this URL; [t]he number of shares of this URL (this includes copy/pasting a link back to Facebook); [t]he number of likes and comments on stories on Facebook about this URL; [t]he number of inbox messages containing this URL as an attachment.” The author concludes by quoting a reporter who “writes that Facebook has ‘not crossed a line with this latest news, any more than they have on hundreds of other occasions.’”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
53	FB000000347	Greg Finn, <u>Your Private Facebook Messages Aren't So Private: Shared Links Count Toward 'Like' Data</u> , Marketing Land (October 8, 2012), available at http://marketingland.com/your-private-facebook-messages-arent-so-private-as-links-count-towards-like-data-23400/ .	Here, the author reports that Facebook's "Like button is an aggregate score from a variety of Facebook actions, including links shared within private messages." He continues, "Facebook did confirm that the issue of double counts was a bug, but did also confirm that shared messages do count towards the overall 'like' data," and he quotes the Facebook Developer site that "clearly states the following about Like buttons": "'The number shown is the sum of: [t]he number of likes of this URL; [t]he number of shares of this URL (this includes copy/pasting a link back to Facebook); [t]he number of likes and comments on stories on Facebook about this URL; [t]he number of inbox messages containing this URL as an attachment.'" He reports that "[t]he fact that private shares gave an endorsement (even if an anonymous one) drew a bit of an uproar" because users sharing a link of a product they don't like "will still be counted as a 'like.'" He concludes by quoting Facebook's statement on the issue.
54	FB000000361	Louis Goddard, <u>Facebook Analyzes Relationships and Chats to Flag Up Sexual Predators</u> , The Verge (July 13, 2012), available at http://www.theverge.com/2012/7/13/3156499/facebook-paedophile-scanning/ .	In this article, the author reports that "Facebook automatically scans posts and chat logs for criminal activity, using big data processing techniques similar to those used in targeting advertising to determine the most vulnerable users." He writes that Facebook's "scanning tools use factors such as mutual friends, past interaction, distance and age difference—alongside simple phrase searches—to flag potentially nefarious conversations for human moderators" and "rely on archives of previous conversations that are known to have led to sexual assaults, identifying patterns and searching for similar ones." The author quotes Facebook's then-Chief Security Officer Joe Sullivan, who says, "'We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate.'" The author writes, "Privacy issues aside, it would be practically impossible for human moderators to effectively trawl through the vast amount of data generated by more than 900 million users each day."
55	FB000000388	Fahmida Y. Rashid, <u>Facebook Scans Chats for Criminal Activity</u> , PC Mag (July 13, 2012), available at http://securitywatch.pcmag.com/security/300288-facebook-scans-chats-for-criminal-activity/ .	Here, the author reports that "Facebook has technology in place to monitor user conversations for suspicious activity and notify police when necessary." She writes that Facebook's "scanning technology monitors chats for words or phrases that may signal that something is wrong, such as personal information being exchanged or explicit language being used." The author writes that Facebook stated, "'We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate,'" and she notes that "Facebook security employees don't see any of the conversations until the scanning technology actually flags the exchange." She reports that one security advisor found the news to be "'scary and more than a bit surprising,'" but the author opines that "it's nice to know that Facebook is keeping a distant eye on chat logs for criminal behavior." She provides "tips" for people to protect themselves on Facebook and other social networking sites, and she writes that "Facebook relying on software to pre-scan chats protects the company from privacy concerns that someone is monitoring all conversations."
56	FB000000397	Walter Pacheco, <u>Facebook Scans Conversations For Criminal Activity</u> , Orlando Sentinel (July 13, 2012), available at http://www.orlandosentinel.com/business/technology/os-facebook-scans-criminal-activity-20120713-post.html/ .	Here, the author cites a Reuters report stating that "Facebook is scanning users' chats and posts for possible criminal activity." The author writes that Facebook's then-Chief Security Officer Joe Sullivan stated that "Facebook monitors conversations for words and phrases that suggest potential criminal activity, as well as the exchange of personal information between users with a wide age gap," and that Facebook software "'searches for words often found in the chat records of convicted criminals, including sex offenders, who used social media to find their victims.'"

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
57	FB000000405	Justin Reynolds, <u>Facebook Monitors Potentially Illegal Posts, Chats</u> , Weston-Reddington-Easton Patch (July 13, 2012), <i>available at</i> http://patch.com/connecticut/weston-ct/facebook-eyes-posts-about-illegal-activity/ .	Here, the author reports that, “[u]sing data recognition software, Facebook employees monitor certain users’ posts and chats, scanning them for potentially illegal activity which in some cases has led the social media giant to contact police.” The author writes that CNET reports that Facebook “isn’t actively monitoring all communications on Facebook, as it wants its users to maintain their privacy” and that “[t]he software the company uses to analyze communications which are potentially illegal has a low false-positive rate.” The author concludes by noting that Facebook’s “scanning program looks for certain phrases found in previously obtained chat records from criminals, including sexual predators,” and that “[t]he relationship analysis and phrase material have to add up before a Facebook employee actually looks at communications and makes the final decision of whether to ping the authorities.”
58	FB000000416	Jillian Ryan, <u>Your Facebook Chats are Being Monitored, Find out Why: The Social Media Privacy Report</u> , The Private WiFi Blog (July 20, 2012), <i>available at</i> http://www.privatewifi.com/your-facebook-chats-are-being-monitored-find-out-why-the-social-media-privacy-report/ .	This article reports that “[w]hat you say in your private chats and messages on Facebook may not be as private as you think,” citing a Reuters report that indicated that Facebook “employs a mums-the-word technology that scans posts and chats for criminal activity.” The author notes that Facebook’s “monitoring came to light” earlier that year when Facebook’s software detected an alleged sexual predator. She quotes Reuters’s description of Facebook’s efforts for detecting criminal activity, which “generally start with automated screening for inappropriate language and exchanges of personal information, and extend to using the records of convicted pedophiles’ online chats to teach the software what to seek out.”
59	FB000000418	Lee Bell, <u>Facebook Scans Private Chats and Posts for Criminal Activity</u> , The Inquirer (July 13, 2012), <i>available at</i> http://www.theinquirer.net/inquirer/news/2191599/facebook-scans-private-chats-and-posts-for-criminal-activity/ .	This article reports that “Facebook scans private chats and posts for criminal activity,” noting that Facebook’s software for “scanning postings and chats” detected an alleged sexual predator. The article quotes a security consultant who states, “It shouldn’t surprise anybody that Facebook is trying to make its site a safer place by monitoring for illegal and suspicious behaviour which might bring it into disrepute. Obviously we have to hope that Facebook acts responsibly, and puts measures in place to prevent inappropriate monitoring - or risk a backlash from users.”
60	FB000000423	Kate Tummarello, <u>Facebook Knows When You’re Chatting About Your Illegal Activities</u> , DCInno (July 13, 2012), <i>available at</i> http://dcinno.streetwise.co/2012/07/13/facebook-knows-when-youre-chatting-about-your-illegal-activities/ .	In this article, this author writes that “[a]ccording to online reports, Facebook uses a software that screens private chats to determine if participants are discussing illegal activities.” She quotes a Mashable article on this topic that explains how Facebook’s software works, and she notes that Facebook commented on the issue as follows: “We’ve never wanted to set up an environment where we have employees looking at private communications, so it’s really important that we use technology that has a very low false-positive rate.” She ends by noting that “[b]y keeping most of the private chat records away from employees, Facebook is protecting itself from some privacy advocates.”
61	FB000000358	Will Oremus, <u>Facebook Monitors Your Posts and Chats to Catch Sexual Predators</u> , Slate (July 17, 2012), <i>available at</i> http://www.slate.com/blogs/future_tense/2012/07/17/online_privacy_facebook_monitors_your_posts_chats_to_catch_sexual_predators.html/ .	Here, the author opens by asking, “Ever wonder if Facebook is reading your posts?” He answers, “Well, it is—or, its computers are, at least,” quoting a Reuters article that recounted a case in which Facebook’s software detected a man in his thirties allegedly trying to set up a meeting with a 13-year-old girl for sex. The author writes that “[i]n Facebook’s case, the scanning hasn’t stirred outrage—probably because it seems to be focused on catching sexual predators.” He concludes by writing, “It seems clear that this technology has the potential to do some good. But that shouldn’t blind us to the fact that it represents a further erosion of our online privacy, one more serious than selling our personal information to advertisers.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
62	FB000000364	Emil Protalinski, <u>Facebook Scans Chats and Posts for Criminal Activity</u> , CNet (July 12, 2012), <i>available at</i> http://www.cnet.com/news/facebook-scans-chats-and-posts-for-criminal-activity/ .	The author of this article reports that “Facebook has added sleuthing to its array of data-mining capabilities, scanning your posts and chats for criminal activity.” He writes that Facebook’s “scanning program looks for certain phrases found in previously obtained chat records from criminals, including sexual predators,” noting that the “relationship analysis and phrase material have to add up before a Facebook employee actually looks at communications and makes the final decision of whether to ping the authorities.” The author also writes that “details of the tool are still scarce,” and that “Facebook likely wants to avoid discussing the existence of the monitoring technology in order to avoid further privacy concerns” because “[m]any users don’t like the idea of having their conversations reviewed, even if it’s done by software and rarely by Facebook employees.”
63	FB000000367	Alex Fitzpatrick, <u>Facebook Monitors Your Chats for Criminal Activity</u> , Mashable (July 12, 2012), <i>available at</i> http://mashable.com/2012/07/12/facebook-scanning-chats/ .	This article notes that “Facebook and other social platforms are watching users’ chats for criminal activity.” The author writes that Facebook’s “screening process begins with scanning software that monitors chats for words or phrases that signal something might be amiss,” and that Facebook’s “scanning program is also ‘smart’ [because] it’s taught to keep an eye out for certain phrases found in the previously obtained chat records from criminals including sexual predators.” He suggests that “[k]eeping most of the scanned chats out of the eyes of Facebook employees may help Facebook deflect criticism from privacy advocates, but whether the scanned chats are deleted or stored permanently is yet unknown.” He ends by quoting Facebook’s then-Chief Security Officer Joe Sullivan, who says, “‘We’ve never wanted to set up an environment where we have employees looking at private communications, so it’s really important that we use technology that has a very low false-positive rate.’”
64	FB000000095	Emil Protalinski, <u>Facebook is hiding your messages from you</u> , ZDNet (December 10, 2011), <i>available at</i> http://www.zdnet.com/blog/facebook/facebook-is-hiding-your-messages-from-you/6017/ .	This article concerns Facebook’s “Other” Messages folder and Facebook’s filtering mechanism for the Messages product. The author writes that the “Other” Messages folder is “supposed to work as a junk/spam folder, “ and that while he mainly received “mass” and “spam” messages in his own folder, other people were “really annoyed that Facebook classified some [messages] incorrectly because they missed important information.” The article quotes Facebook’s description of the new filtering service: “‘It seems wrong that an email from your best friend gets sandwiched between a bill and a bank statement . . . It’s not that those other messages aren’t important, but one of them is more meaningful. With new Messages, your Inbox will only contain messages from your friends and their friends. All other messages will go into an Other folder where you can look at them separately.’” The author writes, “I have no problem with such a folder existing: even my friends who say they missed an important message admit that most of their messages in there are not worth their time,” and he concludes by suggesting that Facebook make the “Other Messages” folder more “obvious.”
65	FB000000123	Elizabeth Weingarten, <u>Furious At Facebook Again</u> , Slate (December 9, 2011), <i>available at</i> http://www.slate.com/articles/technology/technology/2011/12/facebook_s_other_messages_mail_you_are_probably_missing.html .	In this article, the author recounts a story where Facebook filtered a message into the “Other” Messages folder that she had wanted to receive. She indicates that she spoke with a Facebook representative, who explained Facebook’s filtering technology and that its move to a “Social Inbox” in November 2010 was a means for “sift[ing] out ‘meaningful’ messages from less meaningful ones.” The author quotes a Facebook statement about the “Other” Messages folder: “‘It seems wrong that an email message from your best friend gets sandwiched between a bill and a bank statement. It’s not that those other messages aren’t important, but one of them is more meaningful. With new Messages, your Inbox will only contain messages from your friends and their friends. All other messages will go into an Other folder where you can look at them separately.’” She concludes by asking, “So do I curse Facebook because it hid [the] messages, or praise it for allowing him to get in touch? I’m going to do both. Thanks, Facebook, for helping this nice man return my laptop. But please try to explain your services better. I suspect many people would be grateful.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
66	FB000000139	Dave Copeland, <u>Facebook's Email Scanning Isn't A Privacy Issue, It's A Credibility Issue</u> , Read Write (October 5, 2012), <i>available at</i> http://readwrite.com/2012/10/05/facebook-email-scanning-isnt-a-privacy-issue-its-a-credibility-issue/ .	Reporting that "Facebook confirmed [that week] that it scans private messages for links and records them as likes, according to the Wall Street Journal and other news outlets," the author opines that this practice injures Facebook's credibility. The author writes that "Facebook has not kept secret its scanning of private messages for references to criminal activity," but he suggests that it is "new [] that it also looks for links and records those at likes," which he claims "gives the appearance that more people are liking more things on the social network." Quoting Facebook's statement that the "scanned links were counted as engagement, not endorsement," the author opines that Facebook's statement "misses the point" because "Facebook's practice of scanning messages and counting links as likes isn't a privacy issue." He writes that "[i]t's common knowledge that what users do online—even in so-called private messaging—is potentially public." Instead, the author opines, "Facebook's activity raises a credibility issue" because "[i]t shows that the company is fudging the numbers when it comes to advertising."
67	FB000000209	Jim Edwards, <u>This Flaw In Facebook Lets You Create As Many Fake Likes As You Want</u> , Business Insider (October 5, 2012), <i>available at</i> http://www.businessinsider.com/this-flaw-in-facebook-lets-you-create-as-many-fake-likes-as-you-want-2012-10/ .	Here, the author writes that his publication previously reported that Facebook "quietly scans your messages, searching for URLs that you've sent to your friends [and] [w]hen it sees one, it increases the number of Facebook Likes on that URL." He notes that while other publications have "portrayed this as a privacy invasion," he believes that "more importantly, it appears to be a massive source of bogus Likes." The author goes on to describe the Facebook bug that increased the social plugin count on third-party websites by two instead of one, and he includes an example of an instance where he attempted to "generate some fake clicks." He quotes a Facebook spokesperson's statement acknowledging that the company "did recently find a bug with our social plugins where at times the count for the Share or Like goes up by two" and that the company was working on a "fix" for that issue, and the author notes that "those likes may actually reflect negative consumer sentiment."
68	FB000000226	<u>Social Networks: Can Robots Violate User Privacy?</u> , High-Tech Bridge (August 7, 2013), <i>available at</i> https://www.htbridge.com/news/social_networks_can_robots_violate_user_privacy.html/ .	This article indicates that High-Tech Bridge conducted a "a simple technical experiment to verify how the 50 largest social networks, web services and free emails systems respect—or indeed abuse—the privacy of their users." The article purportedly confirms that Facebook, Twitter, Google+, and Formspring are crawling URLs, with Facebook allegedly crawling a "[p]rivate message with a link." The article "tak[es] into consideration that some of the services may have legitimate robots (e.g. to verify and block spam links) crawling every user-transmitted link automatically," and it notes that High-Tech Bridge "created a robots.txt file on our web server that restricted bots accessing the server and its content." There are several comments to the article written by readers, one of which notes, "[N]ot surprised at all Facebook did it. Just take note that Facebook do[es] scrap[e] URLs . . . to construct previews . . . [and] to run those URLs against a malicious signaled table of URLs for the 'protection' of their production and users. I can be wrong but I see no space here for a lawsuit."
69	FB000000289	<u>Facebook 'Likes' Automatically Added Without User-Clicks</u> , BBC News Technology (October 4, 2012), <i>available at</i> http://www.bbc.com/news/technology-19832043/ .	This article reports that a security researcher recently "found that simply sending a web address to a friend using Facebook's private messaging function would add two likes to that page." The article quotes portions of a statement from a Facebook spokesperson confirming that Facebook discovered a bug where the Share or Like goes up by two and that Facebook was "working on a fix to solve the issue" and that "no user information is exchanged." The article continues by noting that "[i]n documentation relating to the function of the like button, Facebook details four criteria which cause the likes number to increase - only one of which involves clicking the like button." It further reads, "Facebook stressed that the added likes were anonymous, and would not appear on the user's timeline."

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
70	FB000000296	Craig Lloyd, <u>Facebook Auto-Liking Pages for Users Without Permission [Updated]</u> , Slash Gear (October 4, 2012), available at http://www.slashgear.com/facebook-auto-liking-pages-for-users-without-permission-04250415/ .	In this article, the author cites reports indicating that “Facebook is scanning its users’ private messages and searching for links to Facebook fan pages . . . [and] supposedly automatically likes the pages for you without asking for your permission to do so.” The author writes that “it only seems that it increases the Like count of a page, and doesn’t actually ‘like’ the page on your behalf,” noting that “some users are reporting that it actually does like the page for you without your permission.” The author opines that “this can be a huge problem,” but he indicates that “[s]canning itself is nothing new” and notes that “Gmail does it to provide its users with targeted ads.” The author concludes by noting that “this auto-liking debacle takes it to another level that’s a little over the line and unnecessary.” He updates the article to include a Facebook spokesperson’s statement on the issue, which indicates, among other things, that “[a]bsolutely no private information has been exposed and Facebook is not automatically Liking any Facebook Pages on a user’s behalf” and that “[w]hen the count is increased via shares over private messages, no user information is exchanged, and privacy settings of content are unaffected.”
71	FB000000298	Ryan Singel, <u>Juking Your Facebook ‘Like’ Stats Is As Easy As Sending a Message</u> , Wired (October 4, 2012), available at http://www.wired.com/2012/10/facebook-likes-messages/ .	The author of this article reports that people “looking to artificially inflate their Facebook stats . . . can just simply send a raft of private messages that include a link to your page, and Facebook will add +2 to your page’s ‘Like’ count for each message.” He acknowledges that “[i]t’s long been known that Facebook scans internal messages for spam and security risks—and that it blocks users from sending links to torrent sites such as The Pirate Bay,” but that it’s “never been clear how much data mining [Facebook] is doing” of users’ Facebook messages. He summarizes Ashkan Soltani’s Wall Street Journal article on the topic, and then writes that Facebook’s behavior is “not a bug,” but is “something actually noted in the documentation for developers.” He updates his article to include Facebook’s spokesperson’s statement on the issue, which reads as follows: “‘Absolutely no private information has been exposed and Facebook is not automatically Liking any Facebook Pages on a user’s behalf. Many websites that use Facebook’s ‘Like’, ‘Recommend’, or ‘Share’ buttons also carry a counter next to them. This counter reflects the number of times people have clicked those buttons and also the number of times people have shared that page’s link on Facebook. When the count is increased via shares over private messages, no user information is exchanged, and privacy settings of content are unaffected. Links shared through messages do not affect the Like count on Facebook Pages.’”
72	FB000000340	Ed Oswald, <u>Facebook Private Messages Trigger ‘Likes’ Without Telling</u> , TechHive (October 5, 2012), available at http://www.techhive.com/article/2011278/facebook-private-messages-trigger-likes-without-telling.html/ .	In this article, the author notes that “[t]he next time you share a link with a Facebook friend via private message, be aware that you’re anonymously ‘liking’ that page publicly as well.” He writes that “[w]hile this may come as a surprise, evidence that the company was scanning our messages for these likable links has been public for at least a week,” citing Facebook’s “September 27 FAQ for developers that [states that] ‘the number of inbox messages containing this URL as an attachment’ is a factor in counting the number of likes that shows up on a page’s Like Button,” among other factors. The author writes that “[w]hile this information seems to have been public for some time, those of us who aren’t developers likely had no clue of Facebook’s actions,” but that “given how Facebook uses our activities to further its own business interests, this practice shouldn’t surprise us.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
73	FB000000342	Lisa Vaas, <u>Facebook Scans Private Messages to Inflate the 'Like' Counter on Websites</u> , Naked Security (October 8, 2012), <i>available at</i> https://nakedsecurity.sophos.com/2012/10/08/facebook-scans-private-messages-like-counter/ .	Here, the author writes that “Facebook has confirmed that it’s scanning private Facebook messages to boost ‘Like’ counters on third party websites.” She continues by noting that Facebook “confirmed that they had discovered a bug affecting Like counts” that “concerned inflating page counts by two Likes instead of one.” She reports that “[t]he fact that this is [sic] function is baked into Facebook code as opposed to being a potential fluke of privacy transgression is confirmed . . . on the Facebook Developers page, which states that a websites’ number of Likes is the sum of: [t]he number of likes of this URL; [t]he number of shares of this URL (this includes copy/pasting a link back to Facebook); [t]he number of likes and comments on stories on Facebook about this URL; [t]he number of inbox messages containing this URL as an attachment.” The author confirms that “Facebook’s scanning of private messages isn’t new” and that “[t]he power of the social media mammoth’s data mining technology when applied to private messages came to light in March, when Facebook was credited with quashing potential child molestation between a 13-year-old girl and a man in his 30s who were having a private Facebook conversation about sex.” She writes that Facebook’s “data mining technology scans postings and chats for criminal activity, analyzing relationships to find suspicious conversations between unlikely pairings.” Noting that “[e]mail providers such as Gmail also have a long-standing practice of reviewing messages to weed out spam and to target ads,” she opines that “[t]hose are reasonable uses of data mining technology, but it’s disconcerting to find what might be yet more intrusive forays into allegedly private messages.” For that reason, she writes that “it’s a bit of a relief to learn that Facebook later clarified the privacy issue, saying that ‘absolutely no private information’ is exposed in the private-message-derived Like inflation.” She concludes by writing, “Be prepared to add to your subjects’ Facebook counter glow, whether you want to or not, if you send URLs via private Facebook conversations.”
74	FB000000353	Joseph Menn, <u>Social Networks Scan for Sexual Predators, With Uneven Results</u> , Reuters (July 12, 2012), <i>available at</i> http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712/ .	This article discusses “Facebook’s extensive but little-discussed technology for scanning postings and chats for criminal activity,” which flagged a sexual predator chatting with a 13 year-old girl. The author writes that “Facebook is among the many companies that are embracing a combination of new technologies and human monitoring to thwart sex predators,” noting that “[s]uch efforts generally start with automated screening for inappropriate language and exchanges of personal information.” He writes that “[l]ike most of its peers, Facebook generally avoids discussing its safety practices to discourage scare stories, because it doesn’t catch many wrongdoers, and to sidestep privacy concerns [because] [u]sers could be unnerved about the extent to which their conversations are reviewed, at least by computer programs.” The author continues by noting that “[i]n part because of its massive size, Facebook relies more than some rivals on such technology.” He quotes Facebook’s then-Chief Security Officer Joe Sullivan, who says, “‘We’ve never wanted to set up an environment where we have employees looking at private communications, so it’s really important that we use technology that has a very low false-positive rate.’”
75	FB000000402	Chi Ibe, <u>Nowhere to Hide: Facebook Monitors Your Chats</u> , YNaija.com (July 13, 2012), <i>available at</i> http://ynaija.com/the-internet-has-no-privacy-settings-facebook-monitors-your-chats/ .	Writing that “[r]eports have revealed that Facebook and other social platforms are watching users’ chats” to “monitor criminal activity and notifying police if any suspicious behaviour is detected,” the author asks, “[W]hat ever [sic] happened to good old privacy?” She indicates that “a number of social networking sites have set up a screening process which works by a scanning software that monitors chats for words or phrases that signal something might be amiss.”

Exhibit E: Evidence of Implied Consent

Source	Bates Number	Publication	Summary
76	FB000000407	Tim Bukher, <u>Facebook Monitoring User Chats, Reporting to Police</u> , LawTechie (July 13, 2012), <i>available at</i> http://www.lawtechie.com/2012/07/facebook-monitoring-user-chats-reporting-to-police/ .	The author writes that “[a]ccording to a report via Mashable, Facebook does more than passively scan user profile settings for targeted advertising, it also monitors chats between users for potential criminal activity.”
77	FB000000409	Fox 13 Tampa Bay Staff, <u>Facebook Uses Technology to Spy on Private Chats</u> , My Fox - Tampa Bay (July 13, 2012), <i>available at</i> http://www.myfoxtampabay.com/story/19017765/2012/07/13/facebook-uses-technology-to-spy-on-private-chats/ .	This article reports that “Facebook’s chief security officer admits Facebook users are being monitored for any suspected criminal activity, and it’s not just the stuff you post on timelines.” It notes Facebook uses “smart software” to “monitor[]personal chats” and “scans those chats for certain phrases, exchanges of personal information and vulgar language.” The article adds that “Facebook says the technology has a very low false-positive rate to protect its users’ privacy, but as expected there has been a backlash from users” who “feel their private conversations are being violated.” The article acknowledges that Facebook’s technology “helped net an alleged sexual predator” and reports that the FBI is “on board with this technology and hopes more online sites use it.”

EXHIBIT F

How accurate is the Facebook Like count?

Posted 8 April, 2011 by [Sue Keogh](#) & filed under [Facebook](#).

Blogger Kevin Sablan from the [Almighty Link](#), which studies 'how people, journalists, and companies connect through links and social tools',

reckons it **could be as low as 39%**.



This rather knocks the wind out of the sails of the story I posted the other day about Lionel Messi getting an amazing **seven million Likes** on his Facebook page. Maybe that should have been 2,730,000. Good, but not *quite* as impressive.

Sablan took twelve Facebook-related stories and used the [RealShare tool](#) to measure how many of the Likes or Recommends were genuinely from people clicking the Like button and how many were shares or comments. The most popular story on the list, CNN's [Facebook event: Let's dump trash at Boehner's pad](#) posted a total of 2071 Recommends, when in reality it had 650, plus 769 shares and 653 comments.

Over the twelve stories the combined number of Likes was 4622 whereas the actual figure was 1790, or 39%.

On first sight it seems like a pretty hefty claim to be making, as it means that sites are misleading people as a matter of course about the popularity of their stories as they don't even realise they're doing it. Maybe the problem is the word 'Like', which you take to mean, well, that lots of individual people like the link enough to want to share it. And of course if someone Likes a story and leaves a comment this will be counted twice, thus distorting the figures.

But buried in the [Facebook developers](#) section it explains, 'The number shown is the sum of:

- The number of likes of this URL
- The number of shares of this URL (this includes copy/pasting a link back to Facebook)
- The number of likes and comments on stories on Facebook about this URL
- The number of inbox messages containing this URL as an attachment.'

So the information is out there, if you know where to look. I might even click Like

data:text/html;charset=utf-8,%3Cheader%20class%3D%22article-header%22%20style%3D%22display%3A%20block%3B%20color%3A%20rgb(38%2C%203... 1/2



« Government's £142k not a 'Twitter Tsar' to be paid less than last 'Twitter Tsar'
Mad makes Mark Zuckerberg cover star...in 'The 50 Worst Things About Facebook

Before commenting please read our [rules for commenting on articles](#).

Please note: Your name will appear together with your comment.

Facebook's Paid Messages Test Taxes You For Being Social

Posted: 12/20/2012 6:57 pm

EST | Updated: 02/19/2013

5:12 am EST

Couldn't load plug-in.

1.1k

Like

189

9

180

Tweet

LinkedIn

Comment

594

Share

am's monetization plans wasn't enough excitement for the week, facebook has announced an "experiment" that lets strangers pay to have their correspondence delivered directly to your messages inbox, rather than the "other" folder.

If ever there was a sign that Facebook has completed its transition from social network to commercial network, this is it. Facebook is trying to turn a profit in a way that subverts the original purpose of the site. Paying for special delivery doesn't encourage socializing. It penalizes it.

The tool, which Facebook said is being tested among a "small number of people" in the U.S., lets individuals with whom you are not connected pay to re-route their message from the "other" heap straight to your inbox. Special treatment for a message

will cost \$1 per note, though Facebook is testing other prices as well. At present, users can receive a maximum of one paid message in their inbox per week.

The test is being rolled out in [conjunction with new filters](#) for Facebook's messaging system that aim to ensure important messages don't go unseen in the "Other" inbox.

But back to the paying part.

Facebook promotes its experimental fee as an effort to improve the quality of the messages that do make it to the main inbox, calling it a "small experiment to test the usefulness of economic signals to determine relevance."

Let's call this payment proposal what it is: anti-social.

Charging for VIP message delivery edges dangerously close to a tax on being friendly. Want to reach out to someone who's not in your network? Cough up the cash.

Consider the example Facebook uses to explain the necessity of this tool:

This test is designed to address situations where neither social nor algorithmic signals are sufficient. For example, if you want to send a message to someone you heard speak at an event but are not friends with, or if you want to message someone about a job opportunity, you can use this feature to reach their Inbox. For the receiver, this test allows them to hear from people who have an important message to send them.

As a user who receives no shortage of spam messages, I'm all for cutting back on clutter or fining advertisers who want to get hold of me in my inbox, uninvited.

Yet Facebook's feature stands to penalize individuals who have a valid reason to contact me by charging them for access. And the explanation that receivers will benefit from better quality messages seems dubious. If I receive a sponsored message, it's because the sender thought it was valuable, not because I did, or would. Facebook, which seeks to make the world a "more open and connected place," is charging users to open up and connect with one another.

The fee also potentially stands to bias us against correspondence that ends up in the spam folder. So this Larry guy didn't pay \$1 to be sure I saw his note about applying for our job opening, huh? Well, he must not have wanted it *that* badly. There was no word from Facebook in its blog post on whether messages that have been sponsored by their sender will be labeled as such, though a Facebook spokeswoman noted that users will only be given the option to pay the fee if their message is destined for "other" -- meaning your BFF wouldn't have to wonder whether her messages are ending up in the spammy pile.

Even Facebook users who relish the thought of making strangers think twice about using Facebook to pitch them, bug them or stalk them via messages should have concerns about the experiment. With this new tool, Facebook is essentially allowing people to pay to override your personal settings and reach you even after you explicitly stated you didn't want them to. Facebook profits from allowing people -- **and, most likely, brands** -- to take up your time when you made clear you didn't want them to.

Keeping savvy scammers at bay is a gargantuan challenge for Facebook, **which recently cracked down on fake "likes."** Yet pay-for-delivery messages look more like a fix for Facebook's profit push than a solution to overcrowded inboxes. It's hard to believe that Facebook, of all companies, can't figure out the difference between "Help me to have more subscribers. Pleaseee?" and a long message from a user with a solid track record of normal behavior. The concern isn't so much opening your inbox to a colleague who wants to meet you or ask about job, but opening it to advertisers.

Follow Bianca Bosker on Twitter: www.twitter.com/bbosker

MORE: [Facebook Messages](#)[Facebook Messages Test](#)[Facebook Paid Messages](#)[Facebook Facebook Messages Fee](#)[Facebook Messages Charge](#)[Facebook Charging Messages](#)[Video](#)

Stack Overflow is a question and answer site for professional and enthusiast programmers. It's 100% free, no registration required.

Take the 2-minute tour


How to get share counts using graph API

I can get the share count of an URL using PHP SDK and using the deprecated rest API, but doesn't found a way to get the share counts of an URL using graph API.

Is there any way to find out?

facebook facebook-graph-api facebook-like

edited Jan 20 '13 at 13:01

 Peter O.
11.8k 6 35 45

asked Apr 18 '11 at 6:26

 Ashish Pethkar
415 1 8 7

Get the solution for you in here [stackoverflow.com/questions/6137414/...](http://stackoverflow.com/questions/6137414/) - Eren Yeager Jun 14 '13 at 14:28

9 Answers

It's possible with the Graph API, simply use:

```
http://graph.facebook.com/?id=YOUR_URL
```

something like:

```
http://graph.facebook.com/?id=http://www.google.com
```

Would return:

```
{
  "id": "http://www.google.com",
  "shares": 1163912
}
```

UPDATE: while the above would answer how to get the *share* count. This number is **not** equal to the one you see on the Like Button, since that number is the sum of:

- The number of likes of this URL
- The number of shares of this URL (this includes copy/pasting a link back to Facebook)
- The number of likes and comments on stories on Facebook about this URL
- The number of inbox messages containing this URL as an attachment.

So getting the Like Button number is possible with the Graph API through the `fq1` end-point (the `link_stat` table):

```
https://graph.facebook.com/fq1?q=SELECT url, normalized_url, share_count, like_count, comment_count, total_count, commentsbox_count, comments_fbid, click_count FROM link_stat WHERE url='http://www.google.com'
```

`total_count` is the number that shows in the Like Button.

edited Jun 15 '12 at 14:23

 Jim Rubenstein
5,062 2 18 41

answered Apr 18 '11 at 9:26

 ifaour
30.5k 1 51 13

I don't get the share count for certain objects. I know they should have at least one share. - Fair Dinkum Thinkum Aug 10 '11 at 10:15

@Fair, yes sometimes the number is not correct and it's a bit confusing. You may use the `fq1` table suggested by the other answer, but still...sometimes numbers there is not correct too! - ifaour Aug 10 '11 at 10:40

is it possible to take shares of few sites? – Aziz Feb 17 '12 at 8:24

@Aziz, what do you mean? – ifaour Feb 18 '12 at 13:04

i use this all the time – Dap Feb 5 '14 at 21:35

Here's a list of API links to get your stats:

Facebook*: <https://api.facebook.com/method/links.getStats?urls=%URL%&format=json>
 Twitter: <http://urls.api.twitter.com/1/urls/count.json?url=%URL%>
 Reddit: http://buttons.reddit.com/button_info.json?url=%URL%
 LinkedIn: <http://www.linkedin.com/countserv/count/share?url=%URL%&format=json>
 Digg: <http://widgets.digg.com/buttons/count?url=%URL%>
 Delicious: <http://feeds.delicious.com/v2/json/urlinfo/data?url=%URL%>
 StumbleUpon: <http://www.stumbleupon.com/services/1.01/badge.getinfo?url=%URL%>
 Pinterest: <http://widgets.pinterest.com/v1/urls/count.json?source=6&url=%URL%>

edited Jun 27 '14 at 9:38



Atharva
1,076 ● 9 ● 23

answered Oct 1 '13 at 14:58



chandrajeet
2,482 ● 5 ● 15 ● 10

2 Wow. Awesome set! – ruX Jan 16 '14 at 12:31

1 The linkedin one does not work (gives 403 access denied) – Darhazer Feb 23 '14 at 15:42

1 I have fixed the url for linkedin. – Ahmed Mar 18 '14 at 7:25

1 And not very convenient link to Vkontakte share counter - vk.com/share.php?act=count&index=1&url=%URL% – Artem Petrov Apr 21 '14 at 7:23

2 How much is the API call limit for each request? – SiErMi Dec 9 '14 at 16:53

You should not use graph api. If you either call:

- <http://graph.facebook.com/http://www.apple.com>

or

- <http://graph.facebook.com/?id=http://www.apple.com>

both will return:

```
{
  "id": "http://www.apple.com",
  "shares": 1146997
}
```

But the number shown is the sum of:

- number of likes of this URL
- number of shares of this URL (this includes copy/pasting a link back to Facebook)
- number of likes and comments on stories on Facebook about this URL
- number of inbox messages containing this URL as an attachment.

So you must use FQL.

Look at this answer: [How to fetch facebook likes, share, comments count from an article](#)

answered Oct 10 '11 at 1:45



freedev
3,660 ● 22 ● 30

you are absolutely right, by total_shares is sum of comments+likes+shares but the page i requested, shows shares_i_have = total_shares + likes – Aziz Feb 22 '12 at 5:58

The facebook like button does two things that the API does not do. This might create confusion

when you compare the two.

1. If the URL you use in your like button has a redirect the button will actually show the count of the redirect URL versus the count of the URL you are using.
2. If the page has a og:url property the like button will show the likes of that url instead of the url in the browser.

Hope this helps someone

answered Jun 2 '12 at 18:08



Roland
41 • 1

I don't think it's possible to get like count from the graph api, you should use [FQL link_stat table](#). FQL is not deprecated.

answered Apr 18 '11 at 6:33



himynameisjonas
325 • 2 • 5

Down voted because this isn't true, as per answer by @chandrajeet – [Coulton](#) Mar 18 '14 at 8:57

Check out [this gist](#). It has snippets for how to get the sharing count for the following services:

- Facebook
- Twitter
- Google plus
- Pinterest
- LinkedIn
- StumbledUpon

answered Dec 14 '14 at 14:14



Muhammad Reda
10.7k • 5 • 34 • 52

when i used FQL I found the problem (but it is still problem) the documentation says that the number shown is the sum of:

- number of likes of this URL
- number of shares of this URL (this includes copy/pasting a link back to Facebook)
- number of likes and comments on stories on Facebook about this URL
- number of inbox messages containing this URL as an attachment.

but on my website the shown number is sum of these 4 counts + number of shares (again)

answered Feb 22 '12 at 6:03



Aziz
870 • 4 • 12

Using FQL you could do that:

```
http://graph.facebook.com/fql?q=SELECT url, total_count FROM link_stat WHERE
url='PASTE_YOUR_URL_HERE'
```

answered Oct 16 '14 at 6:28



totas
768 • 5 • 7

There is a ruby gem for it - [SocialShares](#)

Currently it supports following social networks:

- facebook
- twitter
- google plus
- reddit
- linkedin
- pinterest
- stumbleupon
- vkontakte
- mail.ru
- odnoklassniki

Usage:

```
:000 > url = 'http://www.apple.com/'
=> "http://www.apple.com/"
:000 > SocialShares.facebook url
=> 394927
:000 > SocialShares.google url
=> 28289
:000 > SocialShares.twitter url
=> 1164675
:000 > SocialShares.all url
=> {:vkontakte=>44, :facebook=>399027, :google=>28346, :twitter=>1836, :mail_ru=>37,
:odnoklassniki=>1, :reddit=>2361, :linkedin=>nil, :pinterest=>21011, :stumbleupon=>43035}
:000 > SocialShares.selected url, %w(facebook google linkedin)
=> {:facebook=>394927, :google=>28289, :linkedin=>nil}
:000 > SocialShares.total url, %w(facebook google)
=> 423216
:000 > SocialShares.has_any? url, %w(twitter linkedin)
=> true
```

answered Oct 18 '14 at 14:39



[Timrael](#)

438 ● 1 ● 3 ● 7

protected by [Community](#) ♦ Jun 11 '13 at 9:43

Thank you for your interest in this question. Because it has attracted low-quality answers, posting an answer now requires 10 [reputation](#) on this site.

Would you like to answer one of these [unanswered questions](#) instead?

← Back to Original Article

Facebook looks to cash in on user data

Profiles, status updates and messages all include a mother lode of voluntarily provided information. The social media site is using it to help advertisers find exactly who they want to reach. Privacy watchdogs are aghast.

April 17, 2011 | By Jessica Guynn | Los Angeles Times Staff Writer

Reporting from Palo Alto — Julee Morrison has been obsessed with Bon Jovi since she was a teenager.

So when paid ads for fan sites started popping up on the 41-year-old Salt Lake City blogger's Facebook page, she was thrilled. She described herself as a "clicking fool," perusing videos and photos of the New Jersey rockers.

Then it dawned on Morrison why all those Bon Jovi ads appeared every time she logged on to the social networking site.

"Facebook is reading my profile, my interests, the people and pages I am 'friends' with, and targeting me," Morrison said. "It's brilliant social media but it's absolutely creepy."

For Facebook users, the free ride is over.

For years, the privately held company founded by Mark Zuckerberg in a Harvard dorm room put little effort into ad sales, focusing instead on making its service irresistible to users. It worked. Today more than 600 million people have Facebook accounts. The average user spends seven hours a month posting photos, chatting with friends, swapping news links and sending birthday greetings to classmates.

Now the Palo Alto company is looking to cash in on this mother lode of personal information by helping advertisers pinpoint exactly whom they want to reach. This is no idle boast. Facebook doesn't have to guess who its users are or what they like. Facebook *knows*, because members volunteer this information freely — and frequently — in their profiles, status updates, wall posts, messages and "likes."

It's now tracking this activity, shooting online ads to users based on their demographics, interests, even what they say to friends on the site — sometimes within minutes of them typing a key word or phrase.

For example, women who have changed their relationship status to "engaged" on their Facebook profiles shouldn't be surprised to see ads from local wedding planners and caterers pop up when they log in. Hedgehog lovers who type that word in a post might see an ad for a plush toy version of the spiny critters from Squishable.com. Middle-aged men who list motorcycling as one of their hobbies could get pitches from Victory Motorcycles. If a Facebook user becomes a fan of 1-800-FLOWERS, her friends might receive ads telling them that she likes the floral delivery service.

Marketers have been tracking consumers' online habits for years, compiling detailed dossiers of where they click and roam. But Facebook's unique trove of consumer behavior could transform it into one of the most powerful marketing tools ever invented, some analysts believe. And that could translate into a financial bonanza for investors in the 7-year-old company as it prepares for a public offering, perhaps as soon as next year.

But privacy watchdogs say Facebook's unique ability to mine data and sell advertising based on what its members voluntarily share amounts to electronic eavesdropping on personal updates, posts and messages that many users intended to share only with friends.

"Facebook has perfected a stealth digital surveillance apparatus that tracks, analyzes and then acts on your information, including what you tell your friends," said Jeffrey Chester, executive director of the Center for Digital Democracy. "Facebook users should be cautious about whether the social networking giant ultimately has their best interests at heart."

Bon Jovi fan Morrison has removed some information from her profile to make it more difficult for advertisers to target her. "I thought, 'Wait a minute, I didn't give you permission to look into my life,'" she said.

Facebook says it does not disclose information that would allow advertisers to identify individual users, but filters them based on geography, age or specific interests. It also lets users control whether companies such as 1-800-FLOWERS can display the users' names to others to promote products. But any information users post on the site — hobbies, status updates, wall posts — is fair game for ad targeting.

Facebook's first experiment with paid ads was a flop. In 2007 it rolled out Beacon, which broadcast information on Facebook about users' activities and purchases elsewhere on the Web without their permission. Facebook pulled the program after settling a lawsuit brought on behalf of Facebook users.

This time around, company officials appear to be proceeding more cautiously. David Fischer, Facebook's vice president of advertising and global operations, says Facebook delivers ads that are relevant to users' lives.

"This is an opportunity for brands to connect with you," Fischer said. "When someone likes a brand, they are building a two-way conversation, creating an ongoing relationship."

A lot is riding on getting it right. Last year, online advertising in the U.S. grew 15% to \$26 billion, according to the Internet Advertising Bureau.

People familiar with Facebook say its ad revenue doubled to \$2 billion in 2010, and is expected to double again this year as more major advertisers including American Express, Coca Cola and Starbucks climb aboard.

In February, more than a third of all online display ads in the U.S. appeared on Facebook, more than three times as many as appeared on its closest competitor, Yahoo, according to research firm ComScore Inc. Facebook's moneymaking potential has wowed investors. Its market value is estimated at \$55 billion on the private exchange SharesPost.

"If you take a look at the history of media, ad dollars go where the eyeballs are," Wedbush Securities analyst Lou Kerner said. "If you look at Google today, with annual revenue of \$29 billion, it's not hard to think of Facebook generating that kind of revenue in four or five years. That's why we continue to be bullish on Facebook even at these price levels."

Facebook still faces some skepticism from big brands that question how often people click on the ads or how effective they are in getting people to buy something. One recent survey found that Facebook ads performed about half as well as traditional banner ads.

But Facebook's ability to pinpoint paying customers has dazzled some small-business owners, including Chris Meyer. Over the last 18 months, the Minneapolis wedding photographer had Facebook aim his ads specifically at female users who divulged the following information about themselves on the social networking site: college graduates, aged 24 to 30, who had just gotten engaged and lived within a 50-mile radius of Minneapolis.

Meyer says his \$1,700 ad buy generated \$110,000 in sales.

"I could not have built my business without Facebook," he said.

It's much the same for Anne Puthoff. Her store, Emmy's Bridal, is located in Minster, Ohio, population 2,800. She managed to pack the shop for a special weekend trunk show of prom dresses — in February, no less. Her secret weapon: \$200 worth of Facebook ads targeting high school girls from the surrounding area.

"Our fan base has grown steadily in an economy where stores are going out of business or not thriving," Puthoff said. "I think that's due largely to the new customers we are bringing in via Facebook."

Indeed, Facebook users such as Kara-Noel Lawson say they enjoy receiving ads from merchants they like instead of useless spam. The 30-year-old mother of three from Rancho Santa Margarita in Orange County routinely "friends" businesses on the social media site and clicks on advertising that interests her. More often than not, she said, she is rewarded with coupons, gift cards and discounts.

"I don't feel any weird privacy thing," she said. "We are all putting everything out there already."

jessica.guynn@latimes.com

FACEBOOK

Facebook Allows Users to Upgrade to the New Messages Product, Why You Should



SHARES By Josh Constine on Jan. 10, 2011 - 1:43 PM [Comment](#)

Some users are seeing a prompt when they visit their Facebook Messages inbox allowing them to upgrade to the [New Messages product](#) launched in closed beta in November. The product automatically filters non-essential communications into an Other folder, allowing the main inbox to show only important messages. It also routes sent messages to whichever device or interface Facebook deems is the most convenient for the recipient, whether that's Chat, Messages, SMS, or email. While initially only available to press and an early tester-base, it appears all users will soon be able to upgrade to New Messages.

The New Messages



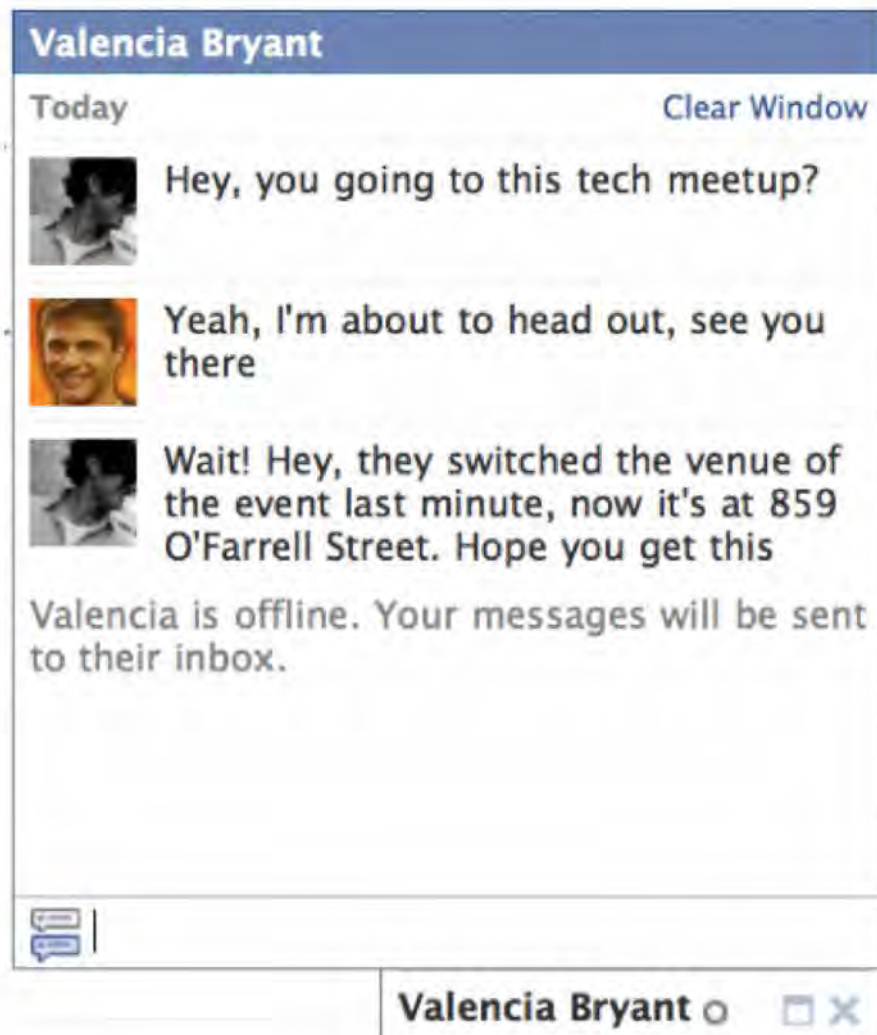
At the product's launch event, CEO Mark Zuckerberg explained that New Messages was built to facilitate modern communication which is simple, immediate, lightweight, and personal like SMS and instant messaging, opposed to more formal, asynchronous email. Though users get an @facebook.com email address, Facebook doesn't expect users to shift things like payment receipts and newsletters there. Instead, the product reduces noise, eases cross-interface conversation, and creates a more comprehensive record of the communication users already perform. Users who don't see the prompt to upgrade on their

a full rollout to occur in the next month or so, similar to how the profile redesign is now being pushed to all users.

For more information, read the top questions about the new Messages.

[Request an Invitation](#)

The best part about New Messages is how it brings Chat into threaded, searchable conversation history. If someone sends you Message, but you're online, you'll see it as a Chat. If you send them back a Chat and they've already logged off, it will be routed to their New Messages inbox, and shown in the same thread as your previous Chat. This means you don't have to worry about conversations breaking down because one person changed the interface through which they were communicating. Or if you accidentally close your last Facebook web interface window or head out the door, you'll still be able to access those Chats from your phone in the form of Messages.



This system is similar to the interplay of Gchat and Gmail, and its adoption could pull users away from Google who use that company’s product for their reliability of delivery. The New Messages product also separates conversations by people rather than by interface, between which the lines are blurring as users increasingly use Chat, email, and Facebook Messages from their mobile device as well as the web. Other useful features of New Messages include forwarding and attachment support, and a one-click “Mark as Read/Unread” option.

The main problem with New Messages at present is the filtering of conversations. Event, Page, and Group updates are usually filtered properly into the Other inbox, leaving a high-signal, low-noise main inbox of one-to-one messages. However, Messages, including time-sensitive businesses communications, from people who aren’t your friend and don’t have mutual friends are filtered into the Other inbox as well. Without the red notification counter on your home page or gray counters on your Messages sidebar navigation link, it’s easy to forget that important Messages may be being filtered out.



For instance, I didn’t check my Other inbox for a few weeks and had multiple Messages from people who wanted to show me their soon-to-launch products. When Facebook sought to inform users of the five-day window to give feedback on proposed changes to its privacy terms via the Facebook Site Governance Page, that Message was also filtered out. Some users prefer to Message someone

one Messages might not reach their recipients until much later. Users can move a conversation between inboxes once it has started, but Facebook could address part of the problem by allowing users to opt to have the first Message from someone they aren't connected to routed to their main inbox.

Overall, Messages will help most Facebook users. It anticipates the shift to using multiple devices and interfaces to conduct a single conversation. It also declutters the inbox by removing spammy and low-value Page and Event updates. Professionals who are frequently contacted by those they aren't connected to will need to pay attention to their Other inbox. But for most, we advise upgrading or requesting an invitation to New Messages because it improves one of the core uses of Facebook — instant communication with friends.

[Note: it's currently unclear when Facebook shows counters for the Other inbox. This feature is still undergoing rapid development.]

Rove Monteux

Facebook Graph API exploit that let's you pump up to 1800 'Likes' in an hour

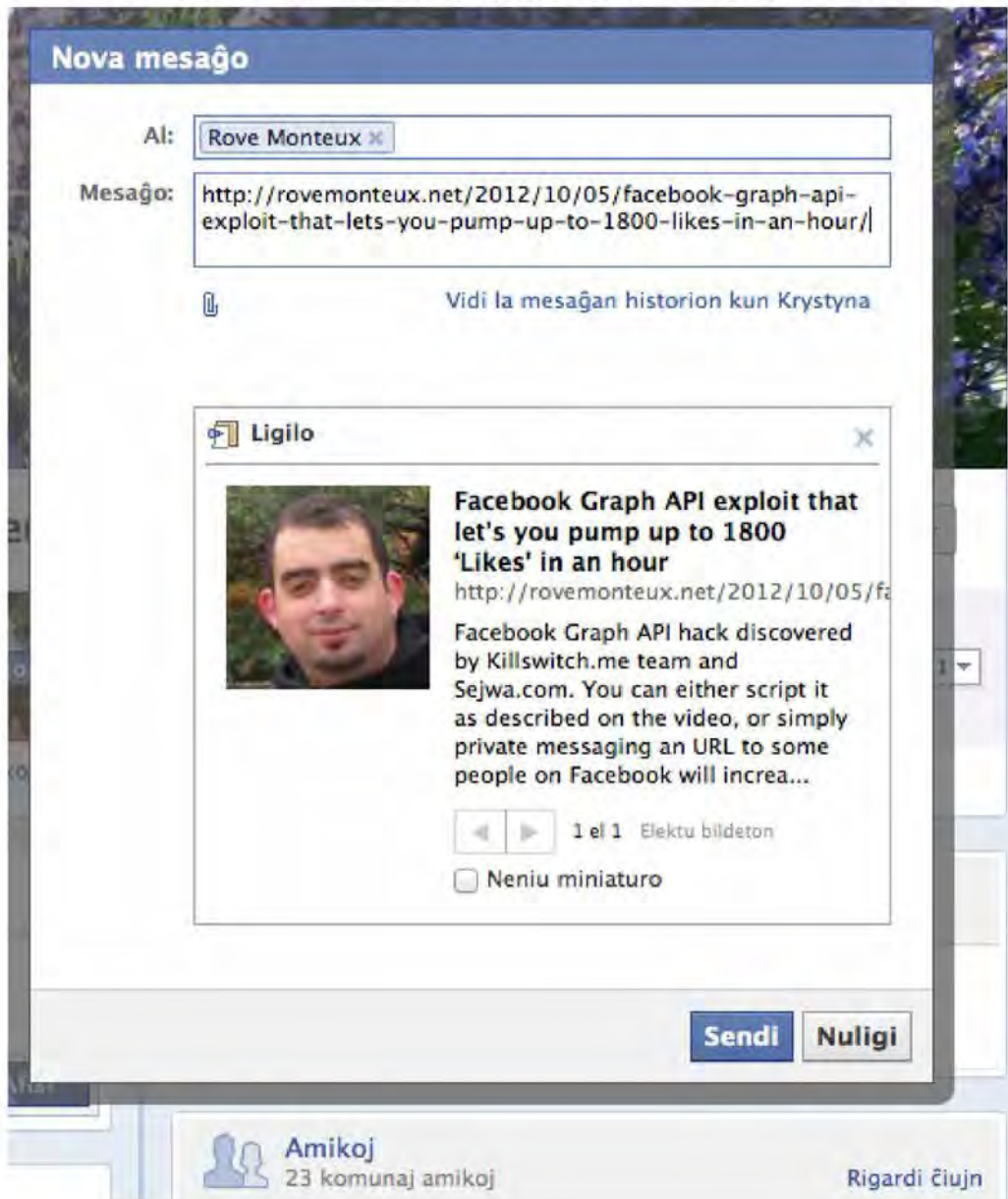
Posted on October 5, 2012 by rmonteux

[Facebook](http://en.wikipedia.org/wiki/Facebook) (<http://en.wikipedia.org/wiki/Facebook>) [Graph API](http://developers.facebook.com/docs/api) (<http://developers.facebook.com/docs/api>) hack discovered by Killswitch.me team and Sejwa.com.

You can either script it as described in the video, or simply private messaging an [URL](http://en.wikipedia.org/wiki/Uniform_Resource_Locator) (http://en.wikipedia.org/wiki/Uniform_Resource_Locator) to some people on Facebook will increase the "like" count for the given URL.

I tested it, and I can confirm that indeed that is correct as of the 5th of october 2012; it also works if you private message the URL to yourself.

To message yourself, go to the page of any of your friends, press the button to private message the person, then delete the person's name by clicking the "x" button beside it, and put your name in place. From then on, in the message menu you will find a tab to privately chat and share URLs with yourself.



(<https://rmonteux.files.wordpress.com/2012/10/screen-shot-2012-10-05-at-10-44-23.png>)

 **Rove Monteux** antaŭ 2 minutoj
<http://rovemonteux.net/2012/10/05/facebook-graph-api-exploit-that-lets-you-pump-up-to-1800-likes-in-an-hour/>

 **Facebook Graph API exploit that let's you pump up to 1800 'Likes' in an hour**
 rovemonteux.net

Facebook Graph API hack discovered by Killswitch.me team and Sejwa.com. You can either script it as described on the video, or simply private messaging an URL to some people on Facebook will increa...

Konigi

 **Rove Monteux** antaŭ 2 minutoj
<http://rovemonteux.net/2012/10/05/facebook-graph-api-exploit-that-lets-you-pump-up-to-1800-likes-in-an-hour/>

 **Facebook Graph API exploit that let's you pump up to 1800 'Likes' in an hour**
 rovemonteux.net

Facebook Graph API hack discovered by Killswitch.me team and Sejwa.com. You can either script it as described on the video, or simply private messaging an URL to some people on Facebook will increa... **Tajpu respondon...**

Konigi

<http://rovemonteux.net/2012/10/05/facebook-graph-api-exploit-that-lets-you-pump-up-to-1800-likes-in-an-hour/> **Respondi**

 ↵

Ligilo ✕

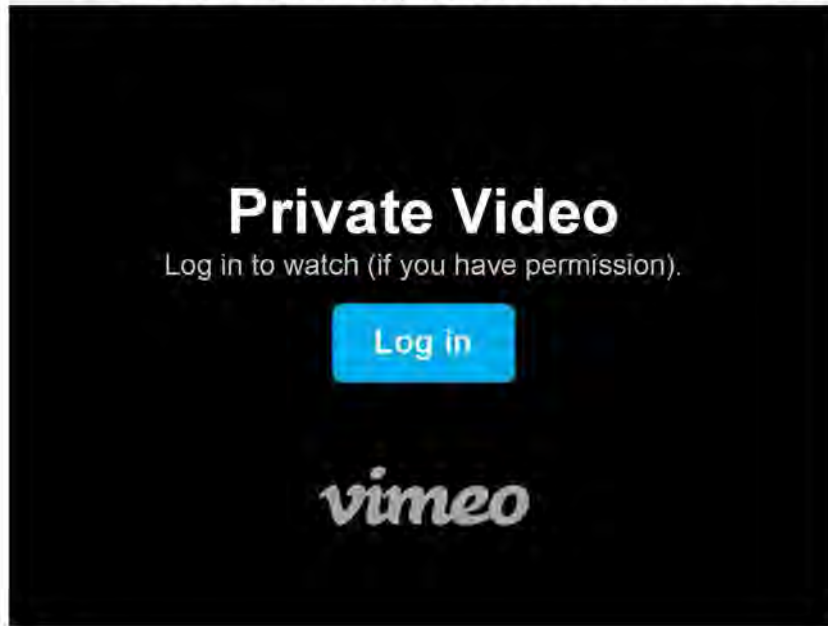
 **Facebook Graph API exploit that let's you pump up to 1800 'Likes' in an hour**
<http://rovemonteux.net/2012/10/05/f>

Facebook Graph API hack discovered by Killswitch.me team and Sejwa.com. You can either script it as described on the video, or simply private messaging an URL to some people on Facebook will increa...

  1 el 1 Elektu bildeton

Neniu miniaturo

(<https://rmonteux.files.wordpress.com/2012/10/screen-shot-2012-10-05-at-10-43-10.png>)



This entry was posted in [English](#), [IT](#) and tagged [Access token](#), [api](#), [Application programming interface](#), [facebook](#), [Facebook Graph](#), [graph](#), [graph api](#), [hack](#), [like](#), [likes](#), [Online Communities](#), [people](#), [Personal message](#), [Uniform Resource Locator](#), [url](#), [vimeo](#). Bookmark the [permalink](#).

[Create a free website or blog at WordPress.com.](#) | [The Confit Theme.](#)

Ⓞ Follow

Follow “Rove Monteux”

Build a website with WordPress.com

Facebook Home's Ultimate Goal: Ingesting Your Messages

Posted: 04/11/2013 5:19 pm

EDT | Updated: 04/11/2013

7:32 pm EDT

Couldn't load plug-in.

Facebook interaction buttons showing counts: Like (124), Share (89), Tweet (128), Comment (3), and LinkedIn (38).

...ly rejected the notion that Facebook Home, the social network's new Facebook-tied smartphone software, is a "phone."

In a sense, he's right: Home isn't a phone so much as it's a three-by-five-inch messaging center designed to get the world hooked on chatting via Facebook.

The social network's foray into smartphones underscores a push to make every interaction with phones into an interaction with Facebook. But more specifically, Home marks an effort to make Facebook the hub for all conversations. On a phone that puts Facebook front and center, Facebook has put messaging front and center.

Zuckerberg asserts that messaging is what people want, telling Wired, "the big stuff that we're seeing now is sharing with smaller groups."

Yet tech industry analysts note that the sooner people channel their chatting through

Facebook, the sooner Facebook can turn messaging from communication between friends into a moneymaker that involves brands. More messaging will give Facebook more data it may use to provide advertisers with personal, personalized ways of interacting with its members.

"They're just trying to make sure that you don't use anyone else's messaging service," said Carl Howe, an analyst with the Yankee Group, of Home's messaging capabilities. "They make it so convenient that you would never think about using what are actually very popular other services ... Once you're really invested in their messaging, maybe you won't mind as much when they start showing you ads on your messaging as well."

Facebook did not respond to a request for comment.

In the version of Home that launches Friday, the most compelling offering -- and greatest differentiator -- is a feature dubbed "chat heads." The chatting tool combines Facebook messaging with texting, and replaces friends' names with their Facebook profile photos. The circular chat heads pop up on the screen with each new incoming message, and allow people to open and answer their messages without exiting whatever app they're using.

"Messages reach you no matter what you're doing -- whether you're checking email, browsing the web, or listening to music," wrote Facebook in a press release. When users first open Home, Facebook encourages them to log into Facebook so they can "keep chatting no matter what you're doing." It's a pitch that sounds almost as much like an order as an offer.

Home ultimately lets Facebook interrupt whatever activity a user might be doing, and chat heads ensure that any action on a phone can instantly become Facebook-focused.

"Messaging carries that Facebook experience across other apps," said Chris Silva, an analyst with Altimeter Group, a research and advisory firm. "If ... you leave the Facebook app to go to Chrome or some other app, messaging is still there at the forefront. It becomes a lot more persistent in the interface than any other messaging has been to-date."

Beyond the convenience and prominence of messages on Facebook's software, the service also stands to gain users by virtue of being budget-friendly. Much like Apple's iMessage or BlackBerry Messenger, chat heads bring together text messaging and Facebook's own chat service, making them appear interchangeable. But while each text leaves users one step closer to exceeding their monthly limit, Facebook Messages draws from people's more generous data allowances. Data show that given the option between the two, people will opt for messaging apps. This trend to replace texting with messaging isn't one being cheered by carriers, who, according to Ovum data obtained by the Wall Street Journal, lost \$23 billion in text messaging fees by the end of 2012.

Analysts say Home's spiffy messaging tools suggest a plan to deliver new forms of advertising that more closely target members' behavior.

"Gmail was the Trojan horse to get us hooked on Google services, from which they were able to advertise to us, mine our data and create really detailed profiles of who we were," said Silva. "Messaging tends to be the Trojan horse in these situations. It was for Google. It probably will be for Facebook."

Facebook's Messenger app currently gives people the option to attach location information to each post. Next, say experts, the social network might analyze the content of messages to serve up ads targeted to each conversation, much like Gmail. An exchange via Facebook Messages about feeling lonely after a breakup and hoping to find a new love interest could yield banner ads from online dating sites, matchmaking services or therapists.

Facebook is not only embracing a Google-like approach, it's also using Google's own Android software, on which Home is based, to conquer a new frontier of mobile advertising. Though Google is chasing the same advertising dollars as Facebook, the company's highly-publicized commitment to keep Android open and free for people to customize leaves them little ability to thwart Facebook's plan to leverage Google's own software against its rival.

Advertisers might also contact users directly via messages. Facebook has recently tried [charging people to guarantee that a message to a stranger arrives in her Facebook inbox](#), rather than spam folder, and those tracking Facebook anticipate that the social network might adapt that model for brands. Instead of showing up in the News Feed, advertisers could pay to ensure a Samsung or Microsoft chat head appears when you're walking by the Apple Store.

"[Facebook's messaging platform] is not just for connecting people," said Howe. "It's for connecting brands, too."

Whether users would accept advertising via messages -- private, personal and traditionally off-limits to brands -- remains to be seen (Home, as a whole, could itself be a total flop). Facebook said in a recent earnings call that adding ads to its mobile News Feed yielded only a small decrease in engagement. But can the company go so far -- if it so chooses -- as to add marketing into individual messages without alienating its users?

"There's a certain creepy factor to that, but users are getting much more comfortable trading privacy for convenience," said Silva. "If the targeting works the way it should, and it's hyper-contextual, targeted and users like it, engagement [with ads] will go up."

Facebook's emphasis on messaging follows a [wave of interest in mobile applications](#), such as WeChat and WhatsApp, that offer an alternative to text messaging.

WhatsApp, for example, boasts hundreds of millions of users, [processed 18 billion messages a day in January](#), has been valued at \$1 billion and fended off an acquisitions attempt by Google, [according to a Digital Trends report](#). Like [Facebook's Snapchat clone](#) before it, chat heads on Home may mark just another attempt by Facebook to [copy its way to success](#) and avoid losing users' time to competing social apps. While a Facebook-sponsored study by IDC found that smartphone users spent [a quarter of their phone time on Facebook](#), [Mobidia](#), a company tracking data usage, reported that Facebook [accounted for just 9 percent of the time](#) U.S. Facebook users spend on their phones. In Spain, Mexico and Argentina, WhatsApp actually occupied more time than Facebook, [Mobidia](#) found.

Home could help Facebook convince people to make the social network their mobile home.

"For Facebook, it's about putting Facebook at center of your experience," said Forrester's Charles Golvin. "If messaging is going through Facebook ... it's providing more loyalty and retention in the Facebook experience."

Couldn't load plug-in.

MORE: [Facebook Home Messaging](#)[Social Media](#)[Facebook Talking Heads](#)[Facebook Home Android](#)[Facebook Messages](#)[Facebook Messaging Advertising](#)[Facebook Home Messaging](#)[Facebook Android Phone](#)[Facebook](#)[Facebook Home Phone](#)[Facebook Phone](#)

Facebook is hiding your messages from you

Summary: Facebook has a hidden Other Messages folder! You should probably go check yours and see what's waiting for you inside, just in case it's something important that Facebook shouldn't have put there.

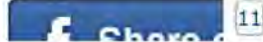


By Emil Protalinski for [Friending Facebook](#) | December 10, 2011 -- 16:12 GMT (08:12 PST)

Get the ZDNet Must Read News Alerts - US translation now

Comments

15



Share

The screenshot shows the Facebook interface for user Emil Protalinski. On the left, the 'FAVORITES' menu includes 'News Feed', 'Messages', 'Other' (highlighted with a red box), and 'Events'. On the right, the 'Other Messages' section displays a message from Addison Bolsey: 'hello there · what's up Emil, you appear impressive. email'.

Head over to [Facebook](#) right now. How many unread private messages do you have in your Messages folder? You'll either reply 0, or however many the little number red number at the top says you have. Guess what? Chances are you have many, many more messages waiting for you.

Open up the Messages folder. Yes, if you haven't already clicked on it, do so now. Now, look over at the left-hand Favorites menu. What's that under the Messages option? There's another folder, slightly indented, labeled as Other. Click on it. There you go, now you're in the hidden folder, called Other Messages.

This Other option only appears when you're already in Messages. That's why nobody ever sees it: once they click on Messages, they only ever look at the middle of the screen. There's no obvious way to access Other Messages from anywhere else on Facebook. The only other way to get here is to directly go to [tofacebook.com/messages/other/](https://facebook.com/messages/other/).

When I look through this folder, I mainly see mass messages sent to myself and other invitees of various Facebook Events and members of numerous Facebook Groups. The rest comprise of spam messages, like the obvious one you can see in the screenshot above (thanks Addison, I think I'm impressive as well).

When I pointed out this folder to my friends a while back, however, many said that it included items that should not be in there. In other words, they're not spam and they're not mass messages. A few even got really annoyed that Facebook classified some of them incorrectly because they missed important information.

If you want to move a message from one folder to the other, you have to open the item in question, and choose the corresponding option from the Actions menu at the top. Alternatively, if you respond to any item in the Other Messages folder, the conversation is moved to your main Messages folder. That's rather intuitive, unlike the location of the Other Messages folder.

So, when did Facebook add Other Messages? It happened way back in [November 2010](#). That's right: most people have been unaware of this folder for over a year. You may of course have messages in this folder sent before November 2010, because Facebook automatically moved them there from your inbox when it created the folder. What follows is how Facebook described its decision to add it.

"It seems wrong that an email message from your best friend gets sandwiched between a bill and a bank statement," a Facebook spokesperson said in a statement. "It's not that those other messages aren't important, but one of them is more meaningful. With new Messages, your Inbox will only contain messages from your friends and their friends. All other messages will go into an Other folder where you can look at them separately. If someone you know isn't on Facebook, that person's email will initially go into the Other folder. You can easily move that conversation into the Inbox, and all the future conversations with that friend will show up there. You can also change your account settings to be even more limited and bounce any emails that aren't exclusively from friends."

In short, messages only appear in the main inbox if they're from friends or friends-of-friends, and if they aren't sent to mailing lists or broad distribution groups. Although Other Messages is supposed to work as a junk/spam folder on Facebook, it's not working perfectly for everyone. I have no problem with such a folder existing: even my friends who say they missed an important message admit that most of their messages in there are not worth their time.

That's not the problem here though. I don't believe Facebook should remove this folder, but I do think they need to make it more visible. I would wager that 99 percent of Facebook's 800 million monthly active users are completely unaware of its existence.

Facebook likely won't start displaying notifications for Other Messages, but I do hope they make it more obvious. Until then, it thus seems the best way to make sure you don't miss anything is to check the Other Messages folder on a regular basis, just like you should for your Junk/Spam folder in your e-mail account.

I first saw talk of Other Messages show up on TNW last month, but it has resurfaced again this week at RedheadWriting and Slate. Since the change was made over a year ago, I'm sure others have written about it before these two publications. If you'd like to be added to the list, comment below or contact me directly and I'll see that your article is included.

See also:

- [Facebook increases status update character limit to 63,206](#)
- [You have 1 lost message on Facebook \(e-mail scam\)](#)
- [Facebook Messenger version 1.5 is out: BlackBerry, iOS 5 support](#)
- [Facebook Messenger for iPhone getting video chat \(leak\)](#)
- [Facebook testing Messenger for Windows desktop client](#)

Topics: Collaboration, Social Enterprise

FACEBOOK [HTTP://THENEXTWEB.COM/FACEBOOK/]

SOCIAL MEDIA [HTTP://THENEXTWEB.COM/SOCIALMEDIA/]

Facebook confirms it is scanning your private messages for links to increase Like counters



23 days until TNW Conference Europe. Join 3,500 people on April 23-24.

[<http://thenextweb.com/conference/europe/>]



EMIL PROTALINSKI

4 October '12, 08:47pm

 Follow

Yesterday I spotted a video submitted to [Hacker News \[http://news.ycombinator.com/item?id=4601538\]](http://news.ycombinator.com/item?id=4601538) by the Polish startup [Killswitch.me \[http://killswitch.me\]](http://killswitch.me) that clearly showed sending a link in a Facebook private message increases the Like counter on the link's originating third-party website. This would suggest Facebook is scanning your private messages for shared links to Web pages with Like buttons, so it can increase the number of corresponding Likes for those pages. Facebook confirmed this information with me today, though it did emphasize this only happens for third-party websites with Facebook plugins, not Facebook Pages.

The original video included NSFW imagery and was promptly taken down by YouTube (for reference, it's still up on [Vimeo \[http://vimeo.com/50608606\]](http://vimeo.com/50608606)). In addition to the potential privacy problems of performing such scans, the short clip also showed a curious oddity: when

Facebook detects a link to a “Likeable” page, it increases the counter by two Likes.

Facebook sent me the following statement about this issue today:

We did recently find a bug with our social plugins where at times the count for the Share or Like goes up by two, and we are working on fix to solve the issue now. To be clear, this only affects social plugins off of Facebook and is not related to Facebook Page likes. This bug does not impact the user experience with messages or what appears on their timelines.

I had to clarify something though. Was the bug in question the fact that the counter goes up by two, or the fact that the counter goes up in the first place, when links are shared privately? The Facebook spokesperson told me that it was indeed the fact that it went up by two. In other words, Facebook is monitoring your private messages for links that have Like buttons and should be increased.

This is news to me. Yet this was clearly the case before as on the Like button Web page over on [Facebook Developers \[https://developers.facebook.com/docs/reference/plugins/like/\]](https://developers.facebook.com/docs/reference/plugins/like/), the social networking giant says the number shown on a Like button is the sum of:

- The number of likes of this URL.
- The number of shares of this URL (this includes copy/pasting a link back to Facebook).
- The number of likes and comments on stories on Facebook about this URL.
- The number of inbox messages containing this URL as an attachment.

I’ve known for a while that the Like button isn’t a counter of just Likes: it also includes Shares as well as comments on Liked and Shared items on the social network. Private messages, however, are something completely different, and they have privacy questions attached to them.

The most important one: if I use Facebook to privately share a link (especially if it’s to something controversial), and the company increases the Like counter, will the Like button on that site show my name to my Facebook friends who also visit that site? I don’t expect anything to show up on my Timeline, but maybe on the site itself, since Facebook already does this for things I actively hit the Like button for.

Thankfully, this isn’t the case. When I asked for clarification, Facebook sent along this statement:

Absolutely no private information has been exposed and Facebook is not automatically Liking any Facebook Pages on a user’s behalf.

Many websites that use Facebook's 'Like', 'Recommend', or 'Share' buttons also carry a counter next to them. This counter reflects the number of times people have clicked those buttons and also the number of times people have shared that page's link on Facebook. When the count is increased via shares over private messages, no user information is exchanged, and privacy settings of content are unaffected. Links shared through messages do not affect the Like count on Facebook Pages.

Well, there's another privacy disaster avoided. Facebook seems to have to deal with this type of thing every week.

Update at 4:55PM EST: Facebook got in touch again to further explain the situation. Here's what's happening: "Our systems parse the URL being shared in order to render the appropriate preview, and to also ensure that the message is not spam."

See also: [Facebook confirms it shut down The Cool Hunter's Facebook Page over copyright infringement](http://thenextweb.com/facebook/2012/10/05/facebook-confirms-it-shut-down-the-cool-hunters-facebook-page-over-copyright-infringement/) [<http://thenextweb.com/facebook/2012/10/05/facebook-confirms-it-shut-down-the-cool-hunters-facebook-page-over-copyright-infringement/>]

Update on October 5: Facebook called to tell me the bug has been fixed. The counter now only goes up by one Like instead of two.

Image credit: [Justin Sullivan / Getty Images](http://www.gettyimages.com/Search/Search.aspx?assettype=image&artist=Justin%20Sullivan) [<http://www.gettyimages.com/Search/Search.aspx?assettype=image&artist=Justin%20Sullivan>]

SOCIAL

Facebook Is Using Your Data Whether You Like It Or Not

The European Commission is cracking down on the way Facebook gathers information about European users. A new EC Directive will ban targeted advertising unless users specifically say they want it. This is great news for European Facebook users, especially after the case of 24-year-old Austrian law student Max Schrems who, in late October, started an...

ALICIA ELER · NOV 28, 2011

The European Commission is **cracking down** on the way Facebook gathers information about European users. A new EC Directive will ban targeted advertising unless users specifically say they want it. This is great news for European Facebook users, especially after the case of 24-year-old Austrian law student Max Schrems who, in late October, started an online campaign aimed at forcing Facebook to abide by **European data privacy laws**.

The real question is: Why isn't this happening in America? All 800 million Facebook users agree to let the company use their personal information.

European Commission Vice President Viviane Redding **called for streamlining** of the continent's laws regarding how service providers protect personal data. ReadWriteWeb's Scott Fulton III reports:

"Rather than a single, federalized approach (which Reding is quoted as having called for, and which in actuality she did not), she spoke on behalf of new guidelines that would hold each European service provider responsible not for 27 member states' laws simultaneously, but only the laws in that provider's native country."

All the data Facebook harvests is stored at data centers in the U.S., like this new one in [Oregon](#). Facebook has information about a user's friends, family, educational background in addition to Facebook activity such as "likes" and everything that gets posted to Facebook Walls. With the [integration of Spotify](#) and [social news apps](#) for The Guardian and The Washington Post, Facebook also has data about what its users are reading and listening to - if they care to use those apps. Messages and "chats" are stored, too, even if the user deletes them.

Facebook denies tracking peoples' behavior to serve advertising. It also denies selling users' personal information to third parties. Facebook claims that advertisers only see "anonymous and aggregate information," using that to serve up targeted ads. It said that it does not target individual users.

We reached out to a Facebook spokesperson specifically about the [Telegraph](#) story.

"The Sunday Telegraph article is sensational and misrepresents both how Facebook's advertising model works and the current advertising privacy debate across Europe. Crucially, people on Facebook have given consent to receive targeted advertising through our terms when they sign up to our free service - unlike other online advertising models. We have spent considerable time and effort building an ads model which allows people to see relevant advertising whilst respecting their privacy.

We are fully compliant with EU law, have our international headquarters in Dublin and unlike some other online services, we do not use tracking technology to serve adverts. Our system only provides advertisers with anonymised and aggregated information for the purpose of targeting ads. We do not share people's names with an advertiser without a person's explicit consent and we never sell personal information to third parties."

Yet with an [IPO in the works](#), and Facebook's move toward becoming self-sufficient, there's no denying that advertising on the site has increased. Earlier this year, sponsored stories started showing up in the [right rail](#). Facebook recently added sponsored stories to the [news ticker](#) (a.k.a. stalker feed).

Last month, the Federal Trade Commission [expressed concern](#) about Facebook privacy. In early November, the Wall Street Journal reported that Facebook was nearing a [settlement with the FTC](#) on charges that they had acted in a deceptive manner regarding the site's privacy settings.