COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE FEDERAL TRADE COMMISSION

In the Matter of Facebook, Inc.

"FTC File No. 092 3184"

December 27, 2011

---

By notice published on December 5, 2011, the Federal Trade Commission ("FTC") has proposed a consent agreement with Facebook that would settle "alleged violations of federal law prohibiting unfair or deceptive acts or practices or unfair methods of competition."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the final order adequately protects the privacy of Facebook users and addresses the issues raised in the complaints.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[2] EPIC's 2010 complaint concerning Google Buzz provided the

[1] Facebook, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 76 Fed. Reg. 75883 (proposed Dec. 5, 2011), http://www.ftc.gov/os/fedreg/2011/12/111205facebookfrn.pdf [hereinafter "Facebook, Inc Proposed Consent Order"].

[2] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

basis for the Commission's investigation and October 24, 2011 subsequent settlement concerning the social networking service.[3] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[4]

The current settlement arises from a Complaint filed by EPIC and a coalition of privacy and civil liberties organization in December 2009 and a Supplemental Complaint filed by EPIC in February 2010.[5]

Section I details the procedural history of the investigation concerning the business practices that gave rise to this Consent Order. Section II describes EPIC's involvement and expertise in the matter. Sections III and IV detail the FTC Complaint and summarize the FTC Consent Order. Section V sets out EPIC's comments and recommendations that would strengthen privacy protections and more effectively address the issues raised in the Complaint.

EPIC supports the findings in the FTC Complaint and supports, in part, the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the proposed Order is insufficient to address the concerns originally identified by EPIC and the consumer coalition, as well as those findings established by the Commission. Consistent with this earlier determination, to protect the interests of Facebook users, and in light

[3] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").
[4] *Id.*
[5] Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [hereinafter EPIC 2009 Facebook Complaint]; Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief) [hereinafter EPIC 2009 Facebook Supplement]; Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [hereinafter EPIC 2010 Facebook Complaint].

of recent changes in the company's business practices, EPIC urges the Commission to require Facebook to:

- Restore the privacy settings that users had in 2009, before the unfair and deceptive practices addressed by the Complaint began;
- Allow users to access all of the data that Facebook keeps about them;
- Cease creating facial recognition profiles without users' affirmative consent;
- Make Facebook's privacy audits publicly available to the greatest extent possible;
- Cease secret post-log out tracking of users across web sites.

In a separate letter, EPIC has also asked the Commission to determine whether Facebook's Timeline, which makes essentially archived and inaccessible information widely available without the consent of the user, is consistent with the terms of the Order.[6] EPIC also recommends that the Commission determine whether other business practices, detailed in these comments, violate the terms of the Order.

These obligations are responsive to the unfair and deceptive trade practices alleged in the Complaint. Improving the Order would also serve the public interest.[7] EPIC would like to call the FTC's attention to the many public comments submitted during the course of this proceeding. The Center for Digital Democracy signed on to EPIC's analysis of the proposed Order, and over 220 Facebook users have also "liked" or signed on to EPIC's recommendations.

[6] Letter from EPIC to Federal Trade Comm'n, (Dec. 27, 2011).

[7] The Federal Trade Commission Act directs that enforcement actions be commenced against unfair and deceptive trade practices "if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public." 15 U.S.C. § 45(b) (2010); *see also FTC v. Cinderella Career & Finishing Schools, Inc.*, 404 F.2d 1308, 1314 (D.C. Cir. 1968) (noting that "the Commission is charged by the broad delegation of power to it to eliminate unfair or deceptive business practices in the public interest . . . ."); *Scientific Mfg. Co. v. Fed. Trade Comm'n*, 124 F.2d 640, 643-44 (3d Cir. 1941) ("The change effected by the amendment lay in the fact that the Commission could thenceforth prevent unfair or deceptive acts or practices in commerce which injuriously affected the public interest alone, while under the original Act the Commission's power to safeguard the public against unfair trade practices depended upon whether the objectionable acts or practices affected competition."); *Rothschild v. Federal Trade Comm'n*, 200 F.2d 39, 42 (7th Cir. 1952) ("One of the purposes of the Act has been the protection of the public, and public interest may exist even though the practice deemed to be unfair does not violate any private right.").

## I. Procedural History

In 2009, Facebook changed its users' privacy settings in a way that made users' personal information, such as Friend lists and application usage data, more widely available to the public and to Facebook's business partners.[8]

On December 17, 2009, EPIC, and a coalition of consumer and civil liberties organizations, filed a complaint with the Federal Trade Commission urging the Commission to investigate Facebook, require Facebook to restore privacy settings that were previously available, and require Facebook to give users meaningful control over their personal information.[9] In the initial complaint, EPIC alleged that Facebook changed the privacy settings available to users in a way that made personal information, such as their friends lists, publicly available.[10] EPIC further alleged that Facebook made personal information available to application developers without users' knowledge or consent; that Facebook Connect decreased users' control over disclosure of personal information; that Facebook's iPhone syncing secretly disclosed personal information; that Facebook's social plugins revealed user information without user consent; and that Facebook allowed developers to retain user data indefinitely.[11]

In response, EPIC received a letter from David Vladeck, head of the FTC Bureau of Consumer Protection, on January 14, 2010, stating that "[y]our most recent complaint raises issues of particular interest for us at this time."[12]

On January 14, 2010, EPIC supplemented the original complaint and described Facebook's practices for access to users' passwords, representations regarding Facebook

[8] Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint) 7, http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.
[9] EPIC 2009 Facebook Complaint.
[10] *Id.* at 8-12.
[11] *See generally id.*
[12] Letter from David Vladeck, Director, FTC Bureau of Consumer Protection, to Marc Rotenberg, Director, EPIC (Jan. 14, 2010), https://epic.org/privacy/inrefacebook/Facebook_Vladeck_Letter.pdf.

Connect, and representations regarding iPhone syncing were unfair and deceptive.[13] On May 5, 2010, EPIC filed a second complaint with the Federal Trade Commission over Facebook's disclosure of users' previously-restricted personal information to Facebook's business partners and the general public. The information disclosed by Facebook included employment history, education, location, hometown, film preferences, music preferences, and reading preferences.[14]

On November 29, 2011, the FTC reached a proposed settlement agreement with Facebook over the company's unfair and deceptive business practices. The FTC identified eight specific counts, including changes to users' privacy settings, application access to user data, advertiser access to use data, photo and video deletion, and violations of the Safe Harbor Framework.[15] In announcing the proposed Consent Order, the Commission noted that "Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups."[16]

## II. EPIC's Complaint Concerning Facebook's Business Practices

EPIC's complaints to the FTC described Facebook's changes to privacy settings that made users' personal information more widely available to the public and to Facebook's business partners.[17] EPIC alleged that the company's actions constituted unfair and deceptive practices under Section 5 of the FTC Act.[18] The main allegations in EPIC's complaints are described below.

[13] EPIC 2009 Facebook Supplement.
[14] EPIC 2010 Facebook Complaint.
[15] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order), http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[16] Press Release, Federal Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.
[17] EPIC 2009 Facebook Complaint; EPIC 2010 Facebook Complaint.
[18] EPIC 2009 Facebook Complaint; EPIC 2010 Facebook Complaint.

### A. Facebook Changed Users' Privacy Settings

EPIC alleged that on November 19, 2009, and December 9, 2009, Facebook updated its privacy policy and changed the privacy settings available to users in a way that made personal information, such as their friends lists, publicly available.[19] Around April 18, 2010, Facebook designated as "publicly available" information that had previously been protectable under users' privacy settings, such as hometown, education, work, activities, likes, and interests.[20]

### B. Facebook Made Personal Information Available to Application Developers Without Users' Knowledge or Consent

EPIC further alleged that when a Facebook user adds an application, by default that application then gains access to everything on Facebook that the user can see.[21] Under the original privacy settings, users had a one-click option to prevent the disclosure of personal information to third-party application developers. Under the revised privacy settings, the one-click option was replaced with a more complicated screen requiring users to uncheck multiple boxes, and users were told that their publicly-available information would always be disclosed to application developers.[22]

### C. Facebook Connect Decreased Users' Control Over Disclosure of Personal Information

EPIC further alleged that Facebook Connect, which allowed Facebook users to log in to third-party websites using their Facebook credentials, forced users to share Facebook Connect activity with everyone or no one, regardless of the other privacy settings the user might have had in place.[23]

---

[19] EPIC 2009 Facebook Complaint at 8-12.
[20] EPIC 2010 Facebook Complaint at 9-15.
[21] EPIC 2009 Facebook Complaint at 12-16.
[22] *Id.*
[23] EPIC 2009 Facebook Supplement at 5-6.

### D. Facebook's iPhone Syncing Secretly Disclosed Personal Information

EPIC further alleged that Facebook's iPhone syncing application transferred the users' iPhone contact list to Facebook without notifying the user.[24]

### E. Facebook's Social Plugins Revealed User Information Without User Consent

EPIC further alleged that social plugins, such as "Like" buttons on third-party websites, allowed third parties to access the personal information of a user who interacted with the plugin, such as name, profile picture, gender, user ID, connections the user has made, and information the user has shared with "everyone."[25]

### F. Facebook Allowed Developers to Retain User Data Indefinitely

Finally, EPIC alleged that after establishing a 24-hour data retention time limit for developers, Facebook announced that this time limit no longer existed.[26]

### G. EPIC's Requested Relief

In December 2009, EPIC and a coalition of consumer and civil liberties organizations urged the Commission to "investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users."[27] Specifically, EPIC urged the FTC to:

> Compel Facebook to restore its previous privacy settings allowing users to choose whether to publicly disclose personal information, including name, current city, and friends;
>
> Compel Facebook to restore its previous privacy setting allowing users to fully opt out of revealing information to third-party developers;
>
> Compel Facebook to make its data collection practices clearer and more comprehensible and to give Facebook users meaningful control over personal information provided by Facebook to advertisers and developers; and

[24] *Id.* at 6-8.
[25] EPIC 2010 Facebook Complaint at 16-21.
[26] *Id.* at 22.
[27] *Id.* at 37; *see also* EPIC 2009 Facebook Complaint at 28.

Provide such other relief as the Commission finds necessary and appropriate.[28]

EPIC also urged the Commission to "[c]ompel Facebook to restore its previous requirement that developers retain user information for no more than 24 hours."[29]

## III. FTC Complaint Allegations

The Commission's 8-count Complaint addresses many of the issues set out in EPIC's filings. Counts 2 and 3 addressed Facebook's changes to users' privacy settings. The Complaint alleged that Facebook changed the privacy settings of users in a way that made public certain information that users had previously restricted.[30] In Count 4, the Complaint also alleged that Facebook allowed application developers to access nearly all of a users' information, whether or not it was necessary for the function of the application.[31]

The FTC Complaint also addressed in part the issues first raised in EPIC's complaint. Counts 1 and 6 addressed Facebook's deceptive practices regarding third-party applications. In addition to application developers' access to personal information, the Complaint explained that Facebook allowed users' personal information to be disclosed to the applications that the users' friends used.[32] This disclosure occurred despite Facebook's representation to users that they could restrict certain information to a limited audience, such as "Only Friends." Furthermore, Facebook had represented that it certified the security of certain applications that participated in its "Verified Apps" program, when, in fact, it took no steps to verify the security of the application.[33]

---

[28] EPIC 2009 Facebook Complaint at 28.
[29] EPIC 2010 Facebook Complaint at 37.
[30] Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint) 7-9, http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.
[31] *Id.* at 10-11.
[32] *Id.* at 4-7.
[33] *Id.* at 14-15.

In Counts 5 and 7, the FTC Complaint addressed other issues raised by EPIC. Count 5 alleges that despite Facebook's representation that it does not provide advertisers with information about its users, the company allowed advertisers to access the personal information of users who clicked on a Facebook ad.[34] Count 7 alleges that Facebook had provided third parties with access to a user's profile information even after the user had deleted or deactivated his or her account.[35]

Finally, Count 8 alleges that Facebook violated the U.S.-EU Safe Harbor Framework by violating the Safe Harbor Privacy Principles of Notice and Choice.[36]

## IV. FTC Proposed Consent Order

### A. Part I: Facebook barred from misrepresentations

Part I of the Order bars Facebook from misrepresenting "in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information . . . ."[37] The prohibition on misrepresentation includes, but is not limited to, the collection or disclosure of covered information, the extent to which a consumer can control the privacy of any covered information, and the extent to which Facebook has made covered information available to third parties.[38] "Covered information" is defined broadly, and includes "(a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet

[34] *Id.* at 11-14.
[35] *Id.* at 17.
[36] *Id.* at 17-19.
[37] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order), http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[38] *Id.*

Protocol ("IP") address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above."[39]

### B. Part II: Facebook must obtain affirmative, opt-in consent before exceeding users' privacy settings

Before any sharing of a user's information that "materially exceeds the restrictions imposed by a user's privacy setting(s)," Facebook must "clearly and prominently" disclose to the user (1) the type of information that will be disclosed, (2) the identity of the third parties, and (3) that such disclosure exceeds the restrictions imposed by the privacy settings in effect.[40] Facebook must also obtain the user's "affirmative express consent."[41]

### C. Part III: Facebook must allow for meaningful data deletion

The Order also requires Facebook to ensure that a user's information cannot be accessed by a third party from Facebook's servers "after a reasonable period of time, not to exceed thirty (30) days" from the time the user has deleted the account.[42]

### D. Part IV: Facebook must implement a comprehensive privacy program

Under the proposed Consent Order, Facebook must implement a "comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information."[43] The program must be "documented in writing" and appropriate to Facebook's size and complexity, nature and scope of activities, and the sensitivity of the covered information.[44]

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*

The program must identify "reasonably foreseeable, material risks" to privacy and describe the controls and procedures that Facebook will take to address those risks.[45] Facebook must also use reasonable steps to ensure that service providers are capable of protecting the privacy of covered information that they receive form Facebook.[46] Finally, Facebook must evaluate and adjust the privacy program.[47]

### E. Part V: Facebook must submit to biennial, independent privacy assessments for 20 years

The Order requires Facebook to obtain biennial assessments from a "qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession."[48] This person must have at least three years of experience in the field of privacy and data protection, and must be approved by the FTC.[49] The first report is dues 180 days after the order rakes effect; subsequent assessments are due every two years for the next 20 years.[50] The assessments must explain the privacy controls implemented and how they are appropriate to meet the requirements imposed by the Order.[51]

### F. Part VI: Other requirements for Facebook

Facebook must make available to the FTC copies of (1) widely disseminated statements that describe Facebook's privacy protections; (2) all consumer complaints directed at Facebook; (3) documents that call into question Facebook's compliance with the Order; (4) documents relating to the attempt to obtain the affirmative consent of users; and (5) materials relied upon to prepare the privacy assessments.[52]

---

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*

Facebook must deliver a copy of the Order to officers and directors who have supervisory responsibilities relating to the subject matter of the Order.[53]

Facebook must notify the Commission within fourteen days of any change that might affect compliance obligations arising under the Order.[54]

Facebook must file a report within ninety days of the order "setting forth in detail the manner and form of their own compliance with this order."[55]

The order will terminate twenty years from the date of issuance, or twenty years from the most recent FTC complaint alleging a violation of the order, whichever comes later.[56]

## V. EPIC's Assessment of the Propose Consent Order

Overall, EPIC supports the findings in the FTC Complaint and supports, in part, the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the proposed Order is insufficient to address the concerns originally identified by EPIC and the consumer coalition, as well as those findings established by the Commission's Complaint. To address the Commission's earlier determinations, better protect the interests of Facebook users, respond to recent changes in the company's business practices, and fulfill the Commission's statutory obligation to act in the public interest, [57] EPIC urges the Commission to strengthen the Order in the manner detailed below.

---

[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] The Federal Trade Commission Act directs that enforcement actions be commenced against unfair and deceptive trade practices "if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public." 15 U.S.C. § 45(b) (2010); *see also FTC v. Cinderella Career & Finishing Schools, Inc.*, 404 F.2d 1308, 1314 (D.C. Cir. 1968) (noting that "the Commission is charged by the broad delegation of power to it to eliminate unfair or deceptive business practices in the public interest . . . ."); *Scientific Mfg. Co. v. Fed. Trade Comm'n*, 124 F.2d 640, 643-44 (3d Cir. 1941) ("The change effected by the amendment lay in the fact that the Commission could thenceforth prevent unfair or deceptive acts or practices in commerce which injuriously affected

### A. The Commission Should Require Facebook to Restore the Privacy Settings that Users had in 2009, Before the Unfair and Deceptive Practices Addressed by the Complaint Began

The Order is purely prospective, and does not attempt to reverse or negate the unfair and deceptive business practices that resulted in the Complaint and Order. As the harm arose from Facebook's original decision to unilaterally change the privacy settings of its users, equitable relief requires the Commission to reestablish the privacy settings that were in place prior to the company's unfair acts. Moreover, the company should not profit from its unfair acts.

The Complaint details the changes that Facebook made to users' privacy settings. The Complaint notes that in November and December of 2009, "Facebook changed its privacy policy . . . and began implementing the changes referenced in its new policy . . . to make public in new ways certain information that users previously had provided."[58] "Although Facebook reinstated these [Friend List] settings shortly thereafter, they were not restored to the Profile Privacy Settings and instead were effectively hidden."[59] "Following the December Privacy Changes, Facebook users could no longer restrict the visibility of their Profile Picture and Pages through these settings, and all prior user choices to do so were overridden."[60]

The Order, however, does not remedy the effects of these changes nor require Facebook to reverse them. Instead, the Order's provisions barring the company from misrepresentations and unilateral privacy changes only take effect once the Order becomes final.[61] Thus, the Order will not affect users who restricted access to their Profile Pictures, Friend Lists, Networks, or

---

the public interest alone, while under the original Act the Commission's power to safeguard the public against unfair trade practices depended upon whether the objectionable acts or practices affected competition."); *Rothschild v. Federal Trade Comm'n*, 200 F.2d 39, 42 (7th Cir. 1952) ("One of the purposes of the Act has been the protection of the public, and public interest may exist even though the practice deemed to be unfair does not violate any private right.").

[58] Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint) 7 http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.

[59] *Id.*

[60] *Id.*

[61] *See id.*

other personal information, and then had those settings altered by Facebook. Such information remains disclosed, unless the user manually resets his or her settings.

The failure to restore the original settings has been widely cited as a flaw with the proposed Order. "Facebook profiles are already splayed open for the world to see, just as Facebook intended when it misappropriated user data two years ago," one commentator stated.[62] "The commission could have forced Facebook to undo its misdeeds - misdeeds alleged by the commission itself - but chose not to."[63] Another commentator cited the fact that "Facebook won't have to roll back any changes to its default privacy settings," as the primary reason that "the agreement is likely to have little, if any, actual impact on Facebook users."[64] "Nothing in the FTC settlement requires Facebook to change that, so the big land grab Facebook made on your privacy two years ago remains a success."[65]

The consequence of the proposed Order's failure to mandate restoration of the previous privacy settings is that Facebook may continue to use, market, and disclose information that was unlawfully obtained from users. Thus, the Commission should revise the proposed Order and require Facebook to restore the 2009 privacy settings.

### B. The Commission Should Require Facebook to Allow Users to Access All of the Data that Facebook Keeps About Them

The Order does not give Facebook users the ability to access the data that Facebook keeps about them. Adding such a requirement would better address the data retention concerns

[62] Ryan Tate, *Facebook Just Played the Government*, GAWKER (Nov. 29, 2011 3:10 PM), http://gawker.com/5863493/facebook-just-played-the-government.
[63] *Id.*
[64] Declan McCullagh, *Facebook's FTC Settlement Won't Change Much, if Anything*, CNET (Nov. 29, 2011 4:15PM PST), http://news.cnet.com/8301-31921_3-57333398-281/facebooks-ftc-settlement-wont-change-much-if-anything/.
[65] Helen A.S. Popkin, *FTC Settlement Aside, Facebook Still Owns Your Privacy*, DIGITAL LIFE (Nov. 30, 2011 5:30P), http://digitallife.today.msnbc.msn.com/_news/2011/11/30/9122106-ftc-settlement-aside-facebook-still-owns-your-privacy?chromedomain=technolog.

raised in the original EPIC complaint and the FTC Complaint and Order, and would give users meaningful control over their personal information in the possession of Facebook.

Facebook collects over 50 data fields about Facebook's users, which it then discloses to its business partners who engage in a wide range of advertising practices including the manipulation of web site content, profile-based advertising, and the use of friend's image to create an implicit endorsement of a product or service.[66]

The information in a Facebook user's profile should be at least as accessible to the Facebook user as it is to Facebook's business partners. EPIC recently launched the KWTK (Know What They Know) campaign and is urging Facebook users to obtain their complete "data dossier" from the company.[67] EPIC's campaign follows the efforts of privacy advocates in Europe, who have used Article 12 of the European Data Protection Directive to access the information that Facebook keeps about individual users.[68] Facebook users in the United States have no similar right to access the personal information that companies hold about them. Although Facebook provides an option to "access your Facebook account information," this option does not compare to the data provided under Article 12, which includes previously deleted information, nor to the information that Facebook's business partner routinely obtain.[69]

Following an extensive investigation of Facebook practices, the Irish Data Protection Commissioner recently concluded that "if identifiable personal data is held in relation to a user or non-user, it must be provided in response to an access request within 40 days, in the absence

[66] *See* PowerPoint: Tore Steen, *Does Facebook Know More About Your Audience Than You Do?*, (July 18, 2011).
[67] EPIC, *#KWTK*, https://epic.org/privacy/kwtk/default.html.
[68] Council Directive 95/46, art. 12, (EC), http://www.dataprotection.ie/viewdoc.asp?docid=93.
[69] Miranda Miller, *Your Facebook Data File: Everything You Never Wanted Anyone to Know*, SEARCH ENGINE WATCH (Oct. 3, 2011), http://searchenginewatch.com/article/2114059/Your-Facebook-Data-File-Everything-You-Never-Wanted-Anyone-to-Know; Tom Loftus, *Europeans to Facebook: Where's My Data?*, WALL STREET JOURNAL TECHNOLOGY NEWS AND INSIGHTS (Sept. 29, 2011 5:58PM), http://blogs.wsj.com/digits/2011/09/29/europeans-to-facebook-wheres-my-data/?KEYWORDS=max+schrems.

of a statutory exemption."[70] This includes previously unavailable data, such as encrypted facial recognition identifiers, cookie-related information, and pages viewed and searches performed on Facebook while logged in.[71] Although the Commissioner cited the right to access personal data provided by the EU Data Directive, this right rests on principles of transparency, control, and awareness that transcend jurisdictional boundaries.

The Commission's Complaint centered on the lack of control Facebook gave to users before unilaterally changing their privacy settings. Count 2, for example, alleges that "Facebook also failed to disclose, or failed to disclose adequately, that the December Privacy Changes overrode existing user privacy settings that restricted access to a user's Name, Profile Picture, Gender, Friend List, Pages, or Networks."[72] Count 3 alleges that Facebook applied its changes to users "without their consent."[73] Control is also incorporated into the Order, which requires Facebook to "obtain the user's affirmative express consent" before materially changing that user's privacy settings.[74] The Order also requires Facebook to "ensure that covered information cannot be accessed by any third party from servers under Respondent's control after . . . the user has deleted such information or deleted or terminated his or her account."[75] By giving users the right to opt-in to changes that exceed their previously established settings, and by forcing Facebook to respect the user's request to terminate his or her account, the Order attempts to return control to Facebook's users.

[70] DATA PROTECTION COMM'R, REPORT OF AUDIT 68 (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf.
[71] *Id.* at 65-66.
[72] Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint) 9 http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.
[73] *Id.*
[74] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[75] *Id.*

The Order also addresses awareness by prohibiting misrepresentations and by requiring Facebook to "clearly and prominently" inform users, before exceeding their privacy settings, of "(1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user."[76]

The Commission should implement user control and awareness by requiring Facebook to give users the right to access the data that Facebook keeps about them. The right to access increases awareness by giving users the ability to see the full extent of the data collected about them by a company. The right to access increases users' control by placing the locus of ownership closer to the user, who gains the ability to inspect data and take steps to correct errors. Thus, the Commission should incorporate a right of access into the final Order.

### C. The Commission Should Require that Facebook Cease Creating Facial Recognition Profiles Without Users' Affirmative, Opt-In Consent

The Order does not specifically address the use of facial recognition technology by Facebook. Requiring that Facebook cease creating facial recognition profiles without users' consent would address the issues raised in the Complaint and further protect the privacy interests of consumers.

The issue of facial recognition technology is particularly timely. The Commission itself recently held a day-long workshop that "explor[ed] facial recognition technology and the privacy and security implications raised by its increasing use."[77] Senator John D. Rockefeller (D-WV) also recently sent a letter requesting that the Commission assess the use of facial recognition

[76] *Id.*
[77] Federal Trade Comm'n, *Face Facts: A Forum on Facial Recognition Technology*, http://www.ftc.gov/bcp/workshops/facefacts/.

technology and recommend legislation to protect privacy.[78] The letter cited mobile applications such as SceneTap, which "tracks the male/female ratio and age mix of the crowd [in bars]" and digital advertising at the Venetian Resort in Las Vegas that tailors ads to the person standing in front of the display based on recognition of that person's age and gender. The Hamburg Commissioner for Data Protection and Freedom of Information has also stated that Facebook's use of facial recognition technology is illegal, and announced legal action against the company.[79]

The Irish Data Protection Commissioner addressed facial recognition in its December 2011 audit, stating that "[i]t remains our position that [Facebook] should have handled the implementation of this feature . . . in a more appropriate manner."[80] Thus, the report indicates that by January 2012, Facebook will

> provide an additional form of notification for Tag Suggest. It will appear at the top of the page when a user logs in. If the user interacts with it by selecting either option presented then it will disappear for the user. If the user does not interact with it then it will appear twice more for a total of 3 displays on the next successive log-ins. Before making a selection more detail about how the feature works will appear behind a Learn More link and will also be shown if a user clicks Adjust Your Settings.[81]

On June 10, 2011, EPIC filed a complaint with the Commission regarding Facebook's compilation and subsequent use of facial images for automated online identification.[83] EPIC's complaint alleged that Facebook did not obtain the consent of users before "collecting 'Photo Comparison Data,' generating unique biometric identifiers, and linking biometric identifiers with

---

[78] Letter from John D. Rockefeller IV, Chairman, U.S. Senate Committee on Commerce, Science, and Transportation, to Jon Leibowitz, Chairman, Federal Trade Commission (Oct. 19, 2011), commerce.senate.gov/public/?a=Files.Serve&File_id=f15e7111-f9fb-4eee-b4e7-7cc48c6f003b.
[79] Press Release, Hamburg Commissioner for Data Protection and Freedom of Information, Facebook's biometric database continues to be unlawful (Nov. 10, 2011), https://epic.org/privacy/facerecognition/PressRelease-2011-11-10-Facebook_BiometricDatebase-1.pdf.
[80] DATA PROTECTION COMM'R, REPORT OF AUDIT 103 (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf.
[81] *Id.* at 105.
[83] Facebook, Inc., (2011) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [hereinafter EPIC 2011 Facebook Facial Recognition Complaint].

individual users."[84] Nor did Facebook obtain users' consent before implementing "Tag Suggestions," which uses the unique biometric identifiers generated by the photo comparison data to identify users when a photograph containing their image is uploaded to Facebook.[85] Facebook also misled users' regarding the process for deleting photo comparison information, did not allow users to disable Facebook's collection of biometric data, and did not establish that application developers, the government, and other third parties would not have access to such data.[86]

In building this biometric database, Facebook failed to "disclose the collection of this biometric photo comparison data to allow them to decide whether to use the technology."[87] Facebook also told users that they would "have extensive and precise controls available to choose who sees what among their network and friends, as well as tools that give them the choice to make a limited set of information available to search engines and other outside entities."[88] Finally, Facebook represented to users that they would retain control over their photographs, including the ability to untag themselves if they did not wish to be identified in photographs obtained by Facebook.[89]

EPIC's complaint requested that the Commission "investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users."[90] Specifically, EPIC requested that the Commission require Facebook to (1) suspend any form of Facebook-initiated "tagging"; (2) avoid misrepresenting the extent to which Facebook maintains and protects the privacy of consumer information; (3) prohibit sharing of identified

[84] *Id.* at 10.
[85] *Id.* at 11.
[86] *Id.* at 16-19.
[87] *Id.* at 21.
[88] *Id.* at 31-32.
[89] *Id.*
[90] *Id.* at 33.

information with any third party without clearly disclosing the practice and obtaining the affirmative consent of users; and (4) establish a comprehensive privacy program.[91]

The Commission's Complaint alleges that Facebook communicated to users that they could control the privacy of certain information and that certain information would not be shared with application developers and advertisers.[92] These unfair and deceptive practices are also at issue in EPIC's complaint regarding facial recognition, which alleges that Facebook deceived users by failing to inform them of its biometric data collection program and misleading users about the extent to which they can control the information contained in their photos. Furthermore, EPIC's complaint also addresses third parties by alleging that Facebook failed to restrict the access of application developers, advertisers, the government, and other third parties could to photo comparison data.

Indeed, the Order could be interpreted to cover facial recognition. The Order prohibits Facebook from "misrepresent[ing] . . . the extent to which it maintains the privacy . . . of covered information."[93] The Order defines "covered information" as "information from or about an individual consumer including, but not limited to: . . . (e) photos and videos."[94] Thus, by its own terms, the Order could extend to the use of facial recognition technology. Some have cited the terms of a similar Order between the Commission and Google as one possible reason that Google has required users to opt-in to the use of facial recognition technology.[95] However, neither the Order nor the Complaint mentioned the practice explicitly. Thus, the Commission should require that Facebook cease creating facial recognition profiles without users' consent. Moreover, the

[91] *Id.*
[92] Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint) http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.
[93] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[94] *Id.*
[95] Kashmir Hill, *Google+ Gingerly Rolls Out Facial Recognition*, FORBES (Dec. 9, 2011 12:07PM), http://www.forbes.com/sites/kashmirhill/2011/12/09/google-gingerly-rolls-out-facial-recognition/.

Commission should require Facebook to be far more transparent about the autotagging feature. Users should be able to obtain a readily accessible log of all the instances when their name-identified facial images were disclosed to third parties, including but not limited to those circumstances were they were tagged by a user at Facebook's suggestion. Finally, the Commission should specifically prohibit the use of Facebook's biometric image database by any law enforcement agency in the world, absent a showing of adequate legal process, consistent with international human rights norms.[96]

### D. The Commission Should Make Facebook's Privacy Audits Publicly Available to the Greatest Extent Possible

The Order does not require the results of Facebook's initial or biennial assessments to be made public. In order to fulfill the Order's emphasis on awareness and commitment to the independence of the assessments, the Commission should require the results of the assessments to be made public to the greatest extent possible under existing law. In Facebook terms, the setting for the audit should be "public" not "friends only."

The Complaint and the Order emphasized the lack of consumer information and notice involved in Facebook's unfair and deceptive practices. For example, the Complaint alleges that Facebook "failed to disclose that a user's choices made through Profile Privacy Settings have been ineffective against Friends' Apps"; "failed to disclose . . . that the December Privacy Changes overrode existing user privacy settings"; and "represented . . . that Facebook does not provide advertisers with information about its users."[97] Although barring Facebook from future misrepresentations and requiring affirmative consent, as the Order does, is the primary method of keeping users informed, users also receive information that is disseminated through the media,

[96] Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948), at art. 12, https://www.un.org/en/documents/udhr/index.shtml#a12.
[97] Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint) 6, 9, 14 http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.

nonprofit organizations such as EPIC, and through independent researchers and bloggers. These parties would benefit greatly from the public availability of Facebook's privacy audits, and, consequently, so would the public.

The Order also seeks to secure the independence of the privacy auditing process. The Order directs that the privacy audits be obtained from "independent" professionals, and that the auditor and the audits themselves be submitted to an outside entity (the FTC).[98] However, given the past unwillingness of government agencies to secure consumer privacy,[99] the accountability that transparency can provide throughout the audit process is the best way to ensure meaningful independence.

Transparency is particularly important in Facebook's case because the public is still without crucial information regarding Facebook's business practices. The Complaint states that, as a result of Facebook's practices, "Platform Advertisers *potentially could* take steps to get detailed information about individual users."[100] However, the Commission has not stated whether advertisers actually took the steps outlined in the Complaint.

The lack of transparency regarding Facebook advertising was also cited by the Irish Data Protection Commissioner in its December 2011 Facebook audit.[101] The Commissioner found that there was "an absolute necessity that members be fully aware of what information generated in their use of the service will be used for advertising purposes thereby allowing them to exercise

[98] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[99] ROBERT GELLMAN AND PAM DIXON, MANY FAILURES: A BRIEF HISTORY OF PRIVACY SELF-REGULATION IN THE UNITED STATES (2011), http://www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf (describing how waning regulatory interest in privacy encouraged industry to abandon self-regulatory efforts).
[100] Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint) 13 http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.
[101] DATA PROTECTION COMM'R, REPORT OF AUDIT (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf.

choice."[102] To address concerns over the transparency of advertising, the Commissioner concluded that "Facebook must be transparent with users as to how they are targeted by advertisers," recommended that Facebook "move the option to exercise control over social ads to the privacy settings from account settings to improve [its] accessibility," and stated that "[t]he current policy of retaining ad-click data indefinitely is unacceptable."[103]

Although companies may exempt trade secrets or confidential commercial information, Part V indicates that portions of the assessments should be able to be completed without revealing any confidential information, such as "the specific privacy controls that [Facebook] has implemented," an explanation of how such controls are "appropriate" to the nature of Facebook's activities, and a certification that such controls are sufficiently effective to protect privacy and comply with the terms of the order.[104]

In the past, the Commission has stated that similar privacy assessments by other companies would be available to the public, subject to applicable laws. After finalizing a consent order with Google that required similar independent assessments, the Commission wrote to EPIC and stated that "[t]o the extent permissible under law, the public may have access to the submissions required pursuant to the order."[105] Furthermore, the experience of the international community provides evidence of the feasibility of such transparency. In 2009, Canadian Privacy Commissioner conducted an investigation of Facebook's privacy policies and released a 113-page report that described in detail the findings of the investigation and the office's recommendations.[106] More recently, the Irish Data Protection Commissioner's investigation into

[102] *Id.* at 44.
[103] *Id.* at 62.
[104] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[105] Letter from Federal Trade Comm'n, Office of Secretary, to EPIC (Oct. 13, 2011), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzepic.pdf.
[106] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE

Facebook, cited above, produced a 150-page report and 77 pages of "technical analysis" that were made publicly available.[107]

### E. The Commission Should Require that Facebook Cease Secret Post-Log Out Tracking of Users Across Web Sites

On September 30, 2011, EPIC and several other privacy and consumer organizations sent a letter to the FTC requesting an investigation over Facebook's use of persistent identifiers ("cookies") to track the internet activity of users even after they have logged off of Facebook.[108] Although EPIC believes that the definitions and mandate of the current Order could be interpreted to cover such post-log out tracking, the Commission should state explicitly that these business practices fall within the terms of the Order.

Under the Order, Facebook is prohibited from "misrepresent[ing] in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to: its collection or disclosure of any covered information."[109] "Covered information," is defined as "information from or about an individual consumer including, but not limited to: . . . (f) Internet Protocol ("IP") address, User ID or other persistent identifier; . . . or (h) any information combined with any of (a) through (g) above."[110] Facebook stated that "[i]f you log-out of Facebook, we will not receive this information [from persistent identifiers] about partner websites but you will also not see personalized experiences

---

CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. (2009), http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm#complaint.

[107] *See* DATA PROTECTION COMM'R, REPORT OF AUDIT (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf.

[108] Letter from EPIC to Federal Trade Comm'n, (Sept. 29, 2011), https://epic.org/privacy/facebook/EPIC_Facebook_FTC_letter.pdf.

[109] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

[110] *Id.*

on these sites."[111] Thus, if Facebook places persistent identifies on a user's browser that track that user's browsing activity in a manner contrary to the company's representations, then Facebook is "misrepresent[ing] . . . the extent to which it maintains the privacy . . . of covered information."

Although the terms of the order appear to contemplate secret post-log out tracking, neither the Order nor the Complaint mentioned the practice explicitly. Indeed, several news reports have already concluded that the Order "won't stop Facebook from monitoring and sharing users' Web-browsing habits, which is a way for the company and others like it to make money."[112] Thus, the Commission should make clear that the Order applies to post-log out tracking.

## D. The Commission Should Determine Whether Other Recent Changes by Facebook Violate the Terms of the Order

Facebook has recently changed its business practices in other ways that alter the privacy of users' personal information and give the company greater ability to disclose this information than in the past. Several of these changes have been brought to the Commission's attention by EPIC in a previous letter.[113] Other changes appear to be new. In either case, because the changes impact the privacy and security of users' covered information, the Commission should determine whether they comply with the terms of the Order.

### *1. Timeline*

On September 30, 2011, EPIC and several other privacy and consumer organizations signed a letter to the FTC requesting an investigation into Facebook Timeline, a digital

[111] Facebook Help Center, *What information does Facebook receive about me when I visit a website with a Facebook social plug in?*, http://www.facebook.com/help/?faq=186325668085084 (last visited Dec. 27, 2011).
[112] *Editorial: Time to enact 'Do Not Track'*, USA TODAY (Dec. 12, 2011 8:30PM), http://www.usatoday.com/news/opinion/editorials/story/2011-12-11/Time-to-enact-Do-Not-Track/51816904/1.
[113] Letter from EPIC to Federal Trade Comm'n, (Sept. 29, 2011), https://epic.org/privacy/facebook/EPIC_Facebook_FTC_letter.pdf.

scrapbook that contains all the information about a user that has ever been disclosed to Facebook.[114] Until December 24, Timeline will be deployed on an opt-in basis for users who wish to make use of this new technology. However, after December 24, Facebook will automatically replace the profiles of users with Timeline, regardless of the users' preferences.

EPIC's letter noted that Timeline's "level of exposure is vastly different from that of the old Facebook Profile."[115] With Timeline, any information about a user that has ever been shared with Facebook—by the user or by third parties—can appear on Timeline. Thus, every aspect of a user's life that Facebook can access—"all the way back to where you were born," according to Mark Zuckerberg[116]. Facebook claims:

> The way your profile works today, 99% of the stories you share vanish. The only way to find the posts that matter is to click "Older Posts" at the bottom of the page. Again. And again. With Timeline, now you have a home for all the great stories you've already shared. They don't just vanish as you add new stuff.[117]

But of course, this description is only accurate to the extent that Facebook retains control over the disclosure of user data. If users were given the ability to post their data as they wish, then users and not Facebook would be able to decide what appears and what "vanishes."

Facebook's reconfiguration of the user's wall both wrests control from the user over the display of the user's data and creates new privacy risks. Security experts have said that Timeline makes it "a heck of a lot easier" for computer criminals to unearth personal details that can be used to craft attacks.[118] "Because people often use personal information to craft passwords or [in] the security questions that some sites and services demand answered before passwords are

---

[114] *Id.*
[115] *Id.* at 6.
[116] Eric Eldon, *Live Blog: Facebook's f8 Developer Conference 2011 Keynote*, INSIDE FACEBOOK (Sept. 22, 2011), http://www.insidefacebook.com/2011/09/22/live-blog-facebooks-f8-developer-conference-2011-keynote/.
[117] Samuel W. Lessin, *Tell Your Story With Timeline*, THE FACEBOOK BLOG (Sept. 22, 2011 1:30PM), https://blog.facebook.com/blog.php?post=10150289612087131.
[118] Gregg Keizer, *Facebook's Timeline will be boon for hackers*, COMPUTERWORLD (Sept. 23, 2011 3:32 PM), https://www.computerworld.com/s/article/9220240/Facebook_s_Timeline_will_be_boon_for_hackers.

changed, the more someone adds to Timeline, the more they put themselves at risk."[119] Timeline's treasure trove of personal information can also provide a tempting target for stalkers, government agents, or employers. As a writer for the Vancouver Sun commented, "the kind of people who would want to spend hours digging through the minutiae of your life are not your friends . . .but those who don't know you that well and are really motivated to find out."[120]

The Order requires Facebook to "clearly and prominently" notify users and obtain their "affirmative express consent" before sharing their nonpublic user information in a way that "materially exceeds the restrictions imposed by a user's privacy setting(s)."[121] "Nonpublic user information" is defined as "covered information that is restricted by one or more privacy setting(s)."[122] "Privacy setting" is defined as "any control or setting provided by [Facebook] that allows a user to restrict which individuals or entities can access or view covered information."[123] Finally, "materially" means "one which is likely to affect a consumer's choice of or conduct regarding a product."[124]

By introducing Timeline, Facebook could be in violation of the Order's requirements. The old Profile design required users to click "Older Posts" repeatedly to view the past personal information of others. Accordingly, the Profile design can be seen as a "privacy setting" that "restrict[s] which individuals or entities can access or view covered information" by effectively preventing disclosure to individuals that are unwilling or unable to click through a user's posting

---

[119] *Id.*
[120] Chad Skelton, *Facebook Timeline: The privacy settings it should have, but doesn't*, CURIOUS DAD (Dec. 20, 2011, 1:34 PM), http://blogs.vancouversun.com/2011/12/20/facebook-timeline-privacy-settings/. Skelton goes on to ask for a privacy setting that allows users to restrict everything on Timeline to "only me" or, alternatively, a setting that allows them to set viewer-specific controls.
[121] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[122] *Id.*
[123] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[124] Facebook, Inc., FTC File No. 092 3184 (2011) (Analysis of Proposed Consent Order to Aid Public Comment), http://www.ftc.gov/os/caselist/0923184/111129facebookanal.pdf.

history. Furthermore, Timeline affects consumers' "conduct regarding a product," as numerous web sites have devoted articles to explaining how consumers should conduct themselves now that their personal information is more widely available.[125] Thus, Timeline represents a "material change." Because Timeline arguably falls within the terms of the Order, the Commission should clarify whether Facebook is required to obtain the affirmative express consent of users before introducing Timeline.

*2. Behavioral Tracking and Analysis by Facebook and Its Business Partners*

Facebook has not disclosed to users the extent to which it and its business partners track, analyze, and operationalize user behavior for business purposes. Facebook tells its business partners that "[Facebook] is a great place to learn who your customers are and what they think about you. Facebook makes it easy to incorporate your customers into your product development cycle and marketing campaigns and iterate quickly."[126] Through Facebook Insights, Facebook's business partners can access data about user behavior, allowing them to:

1. Track and analyze new and lifetime Likes for your Page, and identify their source
2. View your Page's weekly and maximum (theoretical) reach
3. Identify how many people are talking about your Page (and brand)
4. Measure the impact of your Page's content
5. View the user demographics for your Page, including gender, age, location and language
6. Track how you reached people by reach and frequency
7. Measure your Page's unique visitors and page views[127]

[125] *See, e.g.*, Kristin Burnham, *Five Facebook Changes You Can't Wait to Make*, MACWORLD (Dec. 21, 2011 1:10PM), https://www.macworld.com/article/164442/2011/12/five_facebook_timeline_changes_you_cant_wait_to_make.html ; Jim Royal, *Timeline and Privacy: What You Need to Know*, DAILY FINANCE (Dec. 20, 2011 8:33AM), http://www.dailyfinance.com/2011/12/20/facebook-timeline-and-privacy-what-you-need-to-know/; Ian Paul, *Prep for Facebook's Timeline Layout: 6 Must-Do Privacy Tweaks*, PC WORLD (Dec. 16, 2011), https://www.pcworld.com/article/246371/prep_for_facebooks_timeline_layout_6_mustdo_privacy_tweaks.html.

[126] FACEBOOK, BEST PRACTICE GUIDE: MARKETING ON FACEBOOK 13.

[127] Shea Bennett, *Page Insights: All You Need to Know*, THE FACEBOOK MARKETING BIBLE.

Facebook's Preferred Developer Consultant Program allows companies to operationalize users' personal information by contacting "experienced developers who have built numerous Facebook integrations."[128]

The Order prohibits Facebook from "misrepresenting in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including . . . its collection or disclosure of any covered information . . . [and] the extent to which [Facebook] makes or has made covered information accessible to third parties."[129] Thus, Facebook's lack of transparency regarding the operationalization of users' information could constitute a "misrepresentation . . . by implication" regarding the "privacy . . . of covered information." The Commission should determine whether this lack of transparency violates the terms of the Order.

*3. Tagging*

Facebook has recently reduced users' ability to untag themselves from photos and posts created by others. Now, the only simple, "one-click" option merely allows users to hide the photo or post from their profile rather than remove the tag altogether.[130] A user who wishes to actually remove the tag must now navigate a series of dialogue boxes and option selections:

> You have to hunt down the page to find an option for reporting or untagging images. Clicking brings up a dialogue box with several options to review. Choosing the "untag" option brings up a second dialogue box. Choosing "untag" in that dialogue box brings up a third dialogue box that confirms the untagging. Instead of one click, that's four clicks, three boxes and two sets of option selections. Now, imagine repeating that across dozens of photos that might get posted after a night out. The process quickly becomes onerous.[131]

---

[128] Facebook, *Preferred Developer Consultant Program*, https://developers.facebook.com/preferreddevelopers/.
[129] Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order) http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.
[130] Ivor Tossell, *Facebook's photo-tagging tweaks rig the game against privacy*, THE GLOBE AND MAIL (Oct. 5, 2011 10:11AM), https://www.theglobeandmail.com/news/technology/digital-culture/ivor-tossell/facebooks-photo-tagging-tweaks-rig-the-game-against-privacy/article2191666/; *see also* Facebook, *About Tagging*, https://www.facebook.com/about/tagging.
[131] Tossell, *supra* note 125.

The untagging process for status updates or posts is similar, requiring users' to navigate several dialogue boxes and select multiple options.[132]

In reviewing the tagging function of Facebook, the Irish Data Protection Commissioner concluded that "there does not appear to be a compelling case as to why a member cannot decide to prevent tagging of them once they fully understand the potential loss of control and prior notification that comes with it."[133] Accordingly, the report directs Facebook to "examine the broader implications of this recommendation and will engage further on this issue in the July 2012 review."[134]

Facebook changed the tagging function without the "affirmative express consent" of users. The changes also affect "nonpublic user information" because the tagging function allows users to control access to pictures or messages about themselves. Because these changes could be material if they are "likely to affect a consumer's choice of or conduct regarding a product," the Commission should determine whether they satisfy the terms of the Order.

## VI. Conclusion

EPIC supports the findings made by the Federal Trade Commission in the investigation of Facebook. However, the remedies proposed are insufficient to address the problems identified. EPIC urges the Commission to adopt the changes to the proposed Order set out above.

[132] Facebook, *About Tagging*, https://www.facebook.com/about/tagging (describing the options for untagging: removing the tag, sending the owner of the post a message asking to remove the post, reporting the post as abusive, or blocking the owner of the post).
[133] DATA PROTECTION COMM'R, REPORT OF AUDIT 128 (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf.
[134] *Id.*

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
Lillie Coney, EPIC Assistant Director
David Jacobs, EPIC Consumer Protection Fellow
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

Center for Digital Democracy
1220 L Street NW, Suite 300
Washington, DC 20005
202-986-2220