Before the
Federal Trade Commission
Washington, DC

In the Matter of	)
	)
Facebook, Inc. and the	)
Facial Identification of Users	)
	)
_____	)

Complaint, Request for Investigation, Injunction, and Other Relief

1. Introduction

1. This complaint concerns covert biometric data collection by Facebook, the largest social network service in the United States. The secretive collection compilation and subsequent use of facial images for automated online identification adversely impacts consumers in the United States and around the world.

2. Facebook's "Tag Suggestions" techniques converts the photos uploaded by Facebook users into an image identification system under the sole control of Facebook. This has occurred without the knowledge or consent of Facebook users and without adequate consideration of the risks to Facebook users.

3. These business practices violate Facebook's Privacy Policy, as well as public assurances made by Facebook to users. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.

4. There is every reason to believe that unless the Commission acts promptly, Facebook will routinely automate facial identification and eliminate any pretence of user control over the use of their own images for online identification.

5. Facebook's actions are unprecedented. Facebook possesses the largest collection of photographs of individuals of any corporation in the world. According to an extrapolation of photo upload data reported by Facebook, the company now possesses about 60 billion

photographs compared to Photobucket's 8 billion, Picasa's 7 billion and Flickr's 5 billion.[1]

6. Facebook's practices impact 500 million users of the social networking site, approximately 150 million of whom fall within the jurisdiction of the United States Federal Trade Commission.[2]

7. Given these extraordinary circumstances, the Electronic Privacy Information Center, The Center for Digital Democracy, Consumer Watchdog, and the Privacy Rights Clearinghouse, urge the Commission to investigate Facebook, determine the extent of the harm to consumer privacy and safety, require Facebook to cease collection and use of users' biometric data without their affirmative opt-in consent, require Facebook to give users meaningful control over their personal information, establish appropriate security safeguards, limit the disclosure of user information to third parties, and seek appropriate injunctive and compensatory relief.

2. The Parties

8. The Electronic Privacy Information Center ("EPIC") is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. EPIC first brought the Commission's attention to privacy risks of targeted marketing and then to the privacy risks of online advertising.[3] In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, which had failed to safeguard consumer information in the firm's possession.[4] As a result of the EPIC complaint, the FTC fined Choicepoint $15 million, the largest fine in the history of the FTC at the time.[5] EPIC also initiated the complaint to the FTC regarding Microsoft

[1] Online Marketing Trends, Facebook Photo Statistics and Insights (Mar. 1, 2011), http://www.onlinemarketing-trends.com/2011/03/facebook-photo-statistics-and-insights.html

[2] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Jun. 9, 2011).

[3] *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), *available at* http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[4] *In the Matter of Choicepoint*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[5] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties*, $5 Million for Consumer Redress, http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited Dec. 13, 2009).

Passport.[6] The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services that reduced the risk of the profiling of Internet users.[7] EPIC filed a complaint with the FTC regarding the marketing of amateur spyware,[8] which resulted in the issuance of a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology sold for individuals to spy on other individuals.[9] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and March 30, 2011 subsequent settlement concerning the social networking service.[10] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[11]

9. The Center for Digital Democracy ("CDD") is one of the leading non-profit groups analyzing and addressing the impact of digital marketing on privacy and consumer welfare. Based in Washington, D.C., CDD has played a key role promoting policy safeguards for interactive marketing and data collection, including at the FTC and Congress.

10. Consumer Watchdog was established in 1985 and is a nationally recognized nonpartisan, non-profit organization representing the interests of taxpayers and consumers. Its mission is to provide an effective voice for the public interest. Consumer Watchdog's programs include health care reform, oversight of insurance rates, energy policy,

---

[6] *In the Matter of Microsoft Corporation*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), *available at* http://epic.org/privacy/consumer/MS_complaint.pdf.

[7] *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 2002), *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm. *See also* Fed. Trade Comm'n, "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), *available at* http://www.ftc.gov/opa/2002/08/microst.shtm.

[8] *In the Matter of Awarenesstech.com, et al.*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, *available at* http://epic.org/privacy/dv/spy_software.pdf.

[9] *FTC v. Cyberspy Software*, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), *available at* http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf.

[10] Federal Trade Commission, *FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network*, 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.").

[11] *Id*.

protecting legal rights, corporate reform, political accountability, and protecting consumer privacy. Consumer Watchdog is based in Santa Monica, California.

11. The Privacy Rights Clearinghouse ("PRC") is a non-profit, consumer education and advocacy organization based on San Diego, CA and established in 1992. PRC represents consumers' interests regarding informational privacy at the state and federal levels. PRC's website provides numerous guides on how to protect personal information. www.privacyrights.org.

3. The Importance of Privacy Protection

12. The right of privacy is a personal and fundamental right in the United States. The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.

13. The excessive collection of personal data in the United States coupled with inadequate legal and technological protections have led to a dramatic increase in the crime of identity theft.

14. As the Supreme Court has made clear, and the Court of Appeals for the District of Columbia Circuit has recently held, "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."[12]

15. The Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that "the right of individuals to access and challenge personal data collection is generally regarded as perhaps the most important privacy protection safeguard."

16. The Madrid Privacy Declaration explicitly "calls for a moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, . . . subject to a full and transparent evaluation by independent authorities and democratic debate."[13]

---

[12] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989), cited in *Nat'l Cable & Tele. Assn. v. Fed. Commc'ns. Comm'n*, No. 07-1312 (D.C. Cir. Feb. 13, 2009).

[13] The Madrid Privacy Declaration: Global Privacy Standards for a Global World, Nov. 3, 2009, *available at* http://thepublicvoice.org/madrid-declaration/.

17. According to the Restatement of Torts, "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[14]

18. The appropriation tort recognizes the right of each person to exercise control over their image in a commercial setting. The tort is recognized in virtually every state in the United States.

19. Commercial entities are routinely required to obtain explicit consent prior to making use of a person's image.[15]

20. The Federal Trade Commission is "empowered and directed" to investigate and prosecute violations of Section 5 of the Federal Trade Commission Act where the privacy interests of Internet users are at issue.[17]

4. The Significance of Facial Recognition

21. Facial recognition systems include computer-based biometric techniques that detect and identify human faces.[18]

22. The National Academy of Sciences has stated recently:

> The success of large-scale or public biometric systems is dependent on gaining broad public acceptance of their validity. To achieve this goal, the risks and benefits of using such a system must be clearly presented. Public fears about using the system, including . . . concerns about theft or misuse of information, should be addressed.[19]

23. There is significant controversy surrounding the use of facial recognition technology.

24. The British police are "investigating how to incorporate facial recognition software into a new national mug shot database so they can track down criminals faster."[20]

---

[14] Restatement (Second) of Torts § 652C (1977).

[15] *See, e.g.,* "A person may not use an individual's identity for commercial purposes during the individual's lifetime without having obtained previous written consent." Ind. Code Ann. § 32-36-1-8; - 10.

[17] 15 U.S.C. § 45 (2006).

[18] EPIC, "Recognition Recognition," http://epic.org/privacy/facerecognition/. *See also* John D. Woodward, et al, Rand, *Biometrics: A Look at Facial Recognition* 8-9 (2003), *available at* http://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/DB396.pdf.

[19] National Academy of Sciences, *Biometric Recognition: Challenges and Opportunities (Report in Brief)* 7 (2010), *available at* http://sites.nationalacademies.org/cstb/CurrentProjects/CSTB_059722.

[20] Silcon.com, "Police build national mugshot database," *available at* http://www.silicon.com/management/public-sector/2006/01/16/police-build-national-mugshot-database-39155636/.

25. The Chinese government is currently building an elaborate network infrastructure to enable the identification of people in public spaces. The "All-Seeing Eye" relies on the massive deployment of facial recognition technology.[21]

26. According to documents obtained by EPIC under the Freedom of Information Act, the US Department of Homeland Security is pursuing a far-reaching program to automate the identification and tagging of individuals, both citizens and non-citizens, based upon their facial images.[22]

27. Among other programs, DHS is promoting face recognition technology so that federal marshals can surreptitiously photograph people in airports, bus and train stations, and elsewhere leading to the creation of new capabilities for government monitoring of individuals in public spaces.[23]

28. Facial recognition technology and its application for mass surveillance was described by Adm. John Poindexter, the architect of "Total Information Awareness."[24]

29. However, several proposals for facial recognition by the US Department of Homeland Security have been scrapped after objections by local communities.

30. Social networking services have played a transformative role in several regions of the world, but governments also seek access to images of political organizers to obtain actual identities and to enable investigation and prosecution.

31. In Iran, government agents have posted pictures of political activists online and used "crowd-sourcing" to identify individuals.[25] There is also evidence that Iranian

---

[21] Naomi Klein, "China's All-Seeing Eye," The Rolling Stone, May 14, 2008, http://www.naomiklein.org/articles/2008/05/chinas-all-seeing-eye. See also, Keith Bradsher, Theft Reveals Lapses in Chinese Museum's Security, N.Y. TIMES, May 12, 2011, available at http://www.nytimes.com/2011/05/13/world/asia/13beijing.html. ("Cameras are required at Chinese Internet cafés, allowing police using facial recognition software to monitor and catalog individuals' Internet usage."); Michael Wines, In Restive Chinese Area, Cameras Keep Watch, N.Y. TIMES, Aug. 2, 2010, at A1, *available at* http://www.nytimes.com/2010/08/03/world/asia/03china.html ("These cameras are part of a network of millions of surveillance cameras that could become feeders for facial recognition software.")

[22] *See* EPIC, "EPIC FOIA: DHS Biometric Program," http://epic.org/privacy/biometrics/foia_biometric_program.html.

[23] Thomas Frank, "Face recognition next in terror fight," May 10, 2007, http://www.usatoday.com/news/washington/2007-05-10-facial-recognition-terrorism_N.htm

[24] *See generally*, EPIC, "~~Total~~ "Terrorism" Information Awareness (TIA)," http://epic.org/privacy/profiling/tia/. ("A further crucial component was the development of biometric technology to enable the identification and tracking of individuals. DARPA had already funded its "Human ID at a Distance" program, which aimed to positively identify people from a distance through technologies such as face recognition or gait recognition.")

researchers are working on developing and improving facial recognition technology to identify political dissidents.[26]

32. Facebook currently grants government access to user information on merely a "good faith belief" that the disclosure is required by law or when it is necessary to protect Facebook from people it believes are violating its "Statement of Rights of Responsibilities."[29]

33. Central to the meaningful design of face recognition technology with meaningful safeguard is (1) subject control over image enrollment, (2) subject control over the processing and identification of images, (3) transparency in the functioning, use, and purpose of the facial recognition system, and (4) independent accountability of the image processing entity.

34. Some commercial implementations of facial recognition technology adapt one or more of these safeguards.[30]

---

[25] Robert Mackey, *The Lede: Updates on Iran's Disputed Election*, N.Y. TIMES, June 24, 2009, available at http://thelede.blogs.nytimes.com/2009/06/24/latest-updates-on-irans-disputed-election-5/.

[26] Melika Abbasian Nik, Mohammad Mahdi Dehshibi, and Azam Bastanfard, *Iranian Face Database and Evaluation with a New Detection Algorithm*, In Proc. of 2nd BEC, 2007, available at http://dehshibi.com/files/papers/Iranian%20Face%20Database%20and%20Evaluation%20with%20a%20new%20detection.pdf.

[29] Facebook, "Privacy Policy," http://www.facebook.com/policy.php

[30] *See, e.g.,* Apple, "iPhoto – Organize, browse, and share your photos," http://www.apple.com/ilife/iphoto/what-is.html; *see generally* Apple Support Communities, "Concerning the recent privacy hype, can one shut off Faces and locations in iPhoto?" (May 7, 20110< https://discussions.apple.com/thread/3041943?start=0&tstart=0 ("Similarly, if you don't assign faces then there is no data for anyone to steal. So there is no security risk.)

5. Factual Background

A. Facebook's Size and Reach Is Unparalleled Among Social Networking Sites

35. Facebook is the largest social network service provider in the United States. According to Facebook, there are more than 500 million active users, with about 150 million in the United States. 50% of active users log-on to Facebook in any given day. People spend over 700 billion minutes per month on Facebook and install 20 million applications per day.[31]

36. More than 3 billion photos are uploaded to the site each month.[32] Facebook is the largest photo-sharing site in the world by a wide margin.[33] Each day people add more than 100 million tags to photos on Facebook.[34]

B. Facebook Made Changes to Its Photo Technology in 2010-2011

37. Divvyshot, a photo-sharing website, announced on April 2, 2010 that it had been acquired by Facebook.[35] The founder of Divvyshot explained that Facebook was interested in Divvyshot's method of tagging online photos to reflect the event at which they were taken.[36]

38. On July 1, 2010, Facebook introduced face detection technology for photos:

> You now can add tags with just a couple of clicks directly from your home page and other sections of the site, using the same face detection technology that cameras have used for years. . . . With this new feature, tagging is faster since you don't need to select a face. It's already selected for you, just like those rectangles you see around your friends' faces when you take a photo with a modern digital camera. All that's left for you to do is type a name and hit enter.[37]

---

[31] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited June 8, 2011).

[32] Caitlin McDevitt, *Pros and Cons to Facebook's Fast Growing Role in Digital Photograph* (March 14, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/03/13/AR2010031300090.html.

[33] *Id.*

[34] The Facebook Blog, *Making Photo Tagging Easier,* http://www.facebook.com/blog.php?blog_id=company&blogger=13#!/blog.php?post=467145887130 (June 7, 2011).

[35] Caroline McCarthy, Facebook Buys Photo Service Divvyshot, CNET (Apr. 2, 2010), *available at* http://news.cnet.com/8301-13577_3-20001693-36.html.

[36] Jennifer Van Grove, Facebook Acquires Divvyshot to Improve Facebook Photos, Mashable (Apr. 2, 2010), *available at* http://www.mashable.com/2010/04/02/facebook-acquires-divvyshot.

[37] Sam Odio, Making Photos Better, Facebook Blog (July 1, 2010), *available at* http://blog.facebook.com/blog.php?post=403838582130.

39. On September 30, 2010, Facebook introduced a bulk tagging technology for photos:

> When people upload a set of photos, they are often of events like weddings and birthday parties where people are with the same group of friends and family. With our new uploader, you will be able to tag multiple photos in the same album all at once, as well as tag photos of the same person with a lot less effort.[38]

40. At the outset, Sam Odio, Facebook Photo Products Manager, attempted to distinguish Facebook's "face detection" and "bulk tagging" techniques from facial recognition technology:

> This isn't face recognition. . . . Picasa and iPhoto--they'll detect a face and say, "This is Sam," and they'll suggest that it's Sam. We're not doing that. We're not linking any faces to profiles automatically. Right now, we want to stay away from that because it's a very touchy subject.[39]

41. On June 7, 2011, Facebook's Justin Mitchell revised the characterization of photo tagging Facebook Photos, acknowledging that Facebook was now deploying "face recognition" techniques.

> When you or a friend upload new photos, we use face recognition software—similar to that found in many photo editing tools—to match your new photos to other photos you're tagged in. We group similar photos together and, whenever possible, suggest the name of the friend in the photos. If for any reason you don't want your name to be suggested, you will be able to disable suggested tags in your Privacy Settings. Just click 'Customize Settings' and 'Suggest photos of me to friends.' Your name will no longer be suggested in photo tags, though friends can still tag you manually. We notify you when you're tagged, and you can untag yourself at any time. As always, only friends can tag each other in photos.[40]

C. Facebook Began Collecting Data on Users' Photos Without Knowledge or Consent in order to Develop Facial Recognition Technology

[38] Sam Odio, More Beautiful Photos, Facebook Blog (September 30, 2010), *available at* http://blog.facebook.com/blog.php?post=432670242130.

[39] Caroline McCarthy, Facebook Photos Get High Resolution, Bulk Tagging, CNET News.com (September 30, 2010), *available at* http://news.cnet.com/8301-13577_3-20018211-36.html.

[40] Justin Mitchell, Making Photo Tagging Easier, Facebook Blog, *available at* http://blog.facebook.com/blog.php?post=467145887130 (last updated June 7, 2011).

42. Facebook's facial recognition technology works by generating a biometric signature for users who are tagged in photos on Facebook, *i.e.* using "summary data" from "photo comparisons."

43. This representation of biometric information, based on the user's facial image, generated by Facebook, is available to Facebook but not to the user.

44. Facebook routinely encourages users to "tag," i.e. provide actual identifying information about, themselves, their friends, and other people they may recognize.

45. Facebook "associate[s] the tags with [a user's] account, compare what these tagged photos have in common and store a summary of this comparison."[42]

46. Facebook automatically compares uploaded photos "to the summary information we've stored about what your tagged photos have in common."[43]

47. Facebook gave no notice to users and failed to obtain consent prior to collecting "Photo Comparison Data," generating unique biometric identifiers, and linking biometric identifiers with individual users.

D. Facebook Began Making "Tag Suggestions" Using Facial Recognition Technology Without Obtaining Users' Consent

48. On December 15 2010, Facebook announced that it was implementing a facial recognition technology called "Tag Suggestions."[44]

49. On June 7, 2011, Facebook announced that it had deployed "Tag Suggestions" technology over the last several months, and that the technology had been available internationally.[45]

---

[42] Facebook Help Center, *What information does Facebook use to tell that a photo looks like me and to suggest that friends tag me? How can I turn off tag suggestions? How can I remove the information stored about me for tag suggestions*, https://www.facebook.com/help/?faq=19518.

[43] *Id.*

[44] Helen A.S. Popkin, *Facebook's Facial Recognition Knows Who Your Friends Are*, MSNBC, http://technolog.msnbc.msn.com/_news/2010/12/16/5660488-facebooks-facial-recognition-knows-who-your-friends-are- (Dec. 16, 2010).

[45] *Id.*

50. Facebook did not provide users with any other notice about this facial recognition technology.[46]

51. Facebook admitted in a later statement that "we should have been more clear during the roll-out process when this became available to them."[47] However, as of the filing of this complaint, Facebook has made no effort to rectify that matter or to allow users to opt-in if they so choose.

52. Facebook routinely encourages users to confirm Facebook's indentification of facial images in user photos when users attempt to upload photos to their accounts on Faceook.

53. Facebook automated identification of facial images would occur in the absence of any user intervention.

54. Facebook enables "Tag Suggestions" by default; users do not enable "Tag Suggestions."

55. Facebook did not obtain users' consent before using the unique biometric identifiers generated by the "Photo Comparison Data" to identify individual users when a photograph containing their image is uploaded to Facebook.

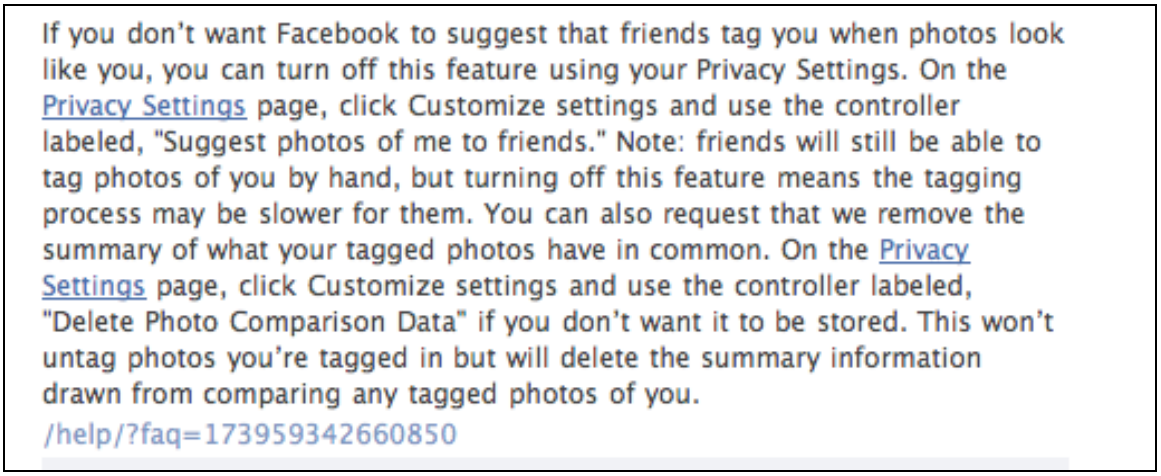
E. Facebook Recommendations to Delete Facial Images are False and Misleading

56. Attempts by a user to browse or search the Facebook help site for information on how to delete the facial recognition data that Facebook has collected leads the user to an incorrect method for deleting photo summary information through the user's Privacy Settings page. [48]

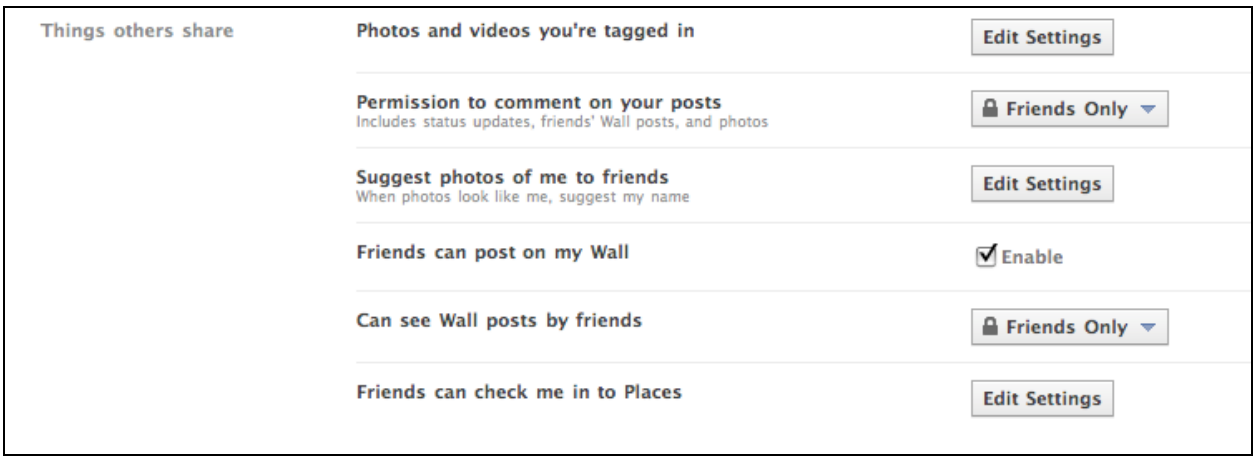
[46] Tiffany Kaiser, *Facebook Prompts More Privacy Anxieties with Facial Recognition Feature,* DailyTech, http://www.dailytech.com/Facebook+Prompts+More+Privacy+Anxieties+with+Facial+Recognition+Feature/article21848.htm?loc=interstitialskip (June 8, 2011).

[47] Alexei Oroskovic, *Facebook Facial Recognition Technology Sparks Renewed Concerns,* Reuter, http://www.reuters.com/article/2011/06/08/us-facebook-idUSTRE7570C220110608 (June 8, 2011).

[48] https://www.facebook.com/help/?faq=225110000848463.

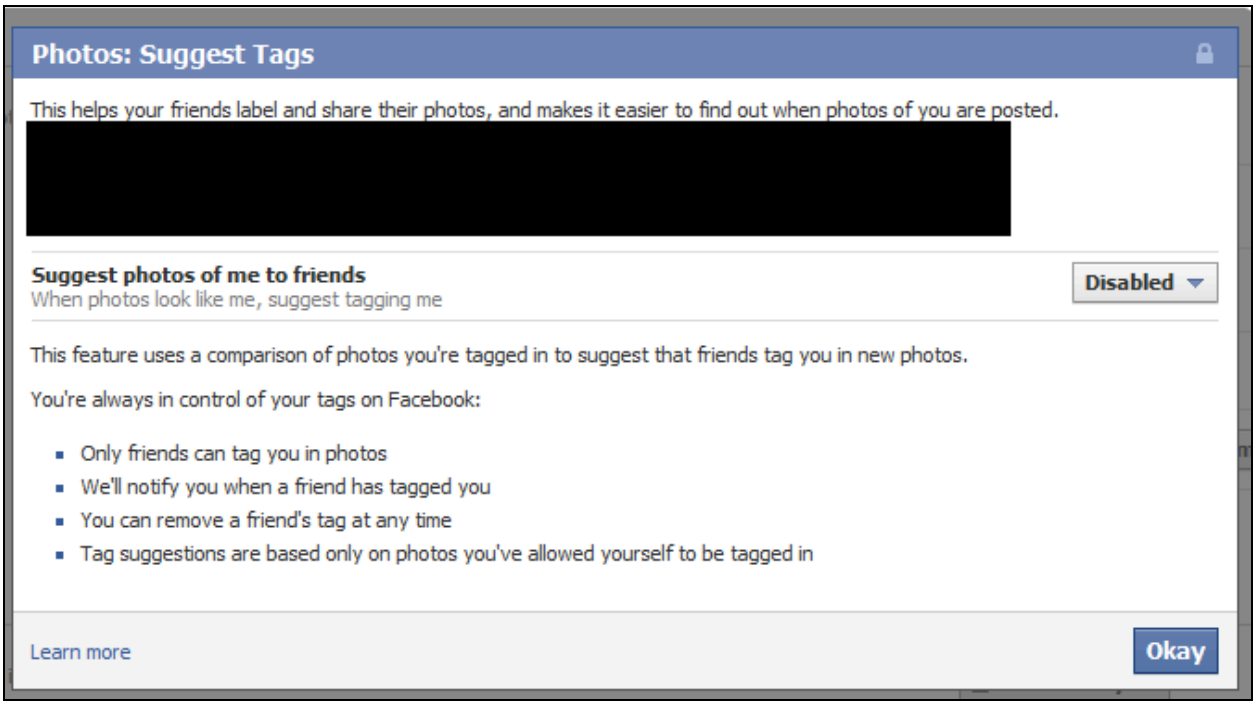


57. There is no option within a user's privacy preferences to delete or prevent Facebook's biometric data collection.

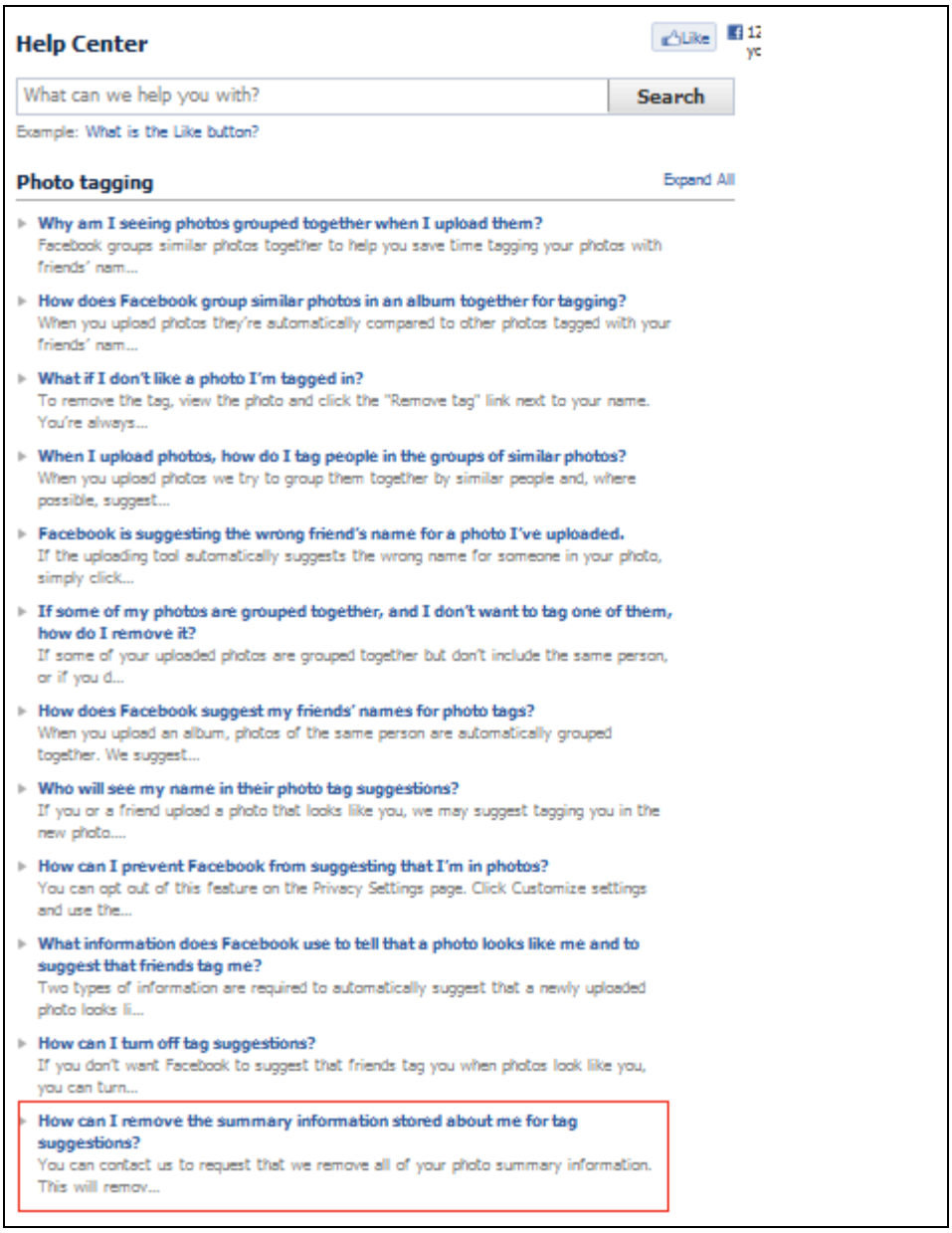


58. When a user wants to delete the biometric "summary" data associated with his account that can be used to pair his name to photos of him, he has to contact Facebook through a difficult-to-find link, https://www.facebook.com/help/?faq=225110000848463, that directs the user to a specific section on Facebook's help page.

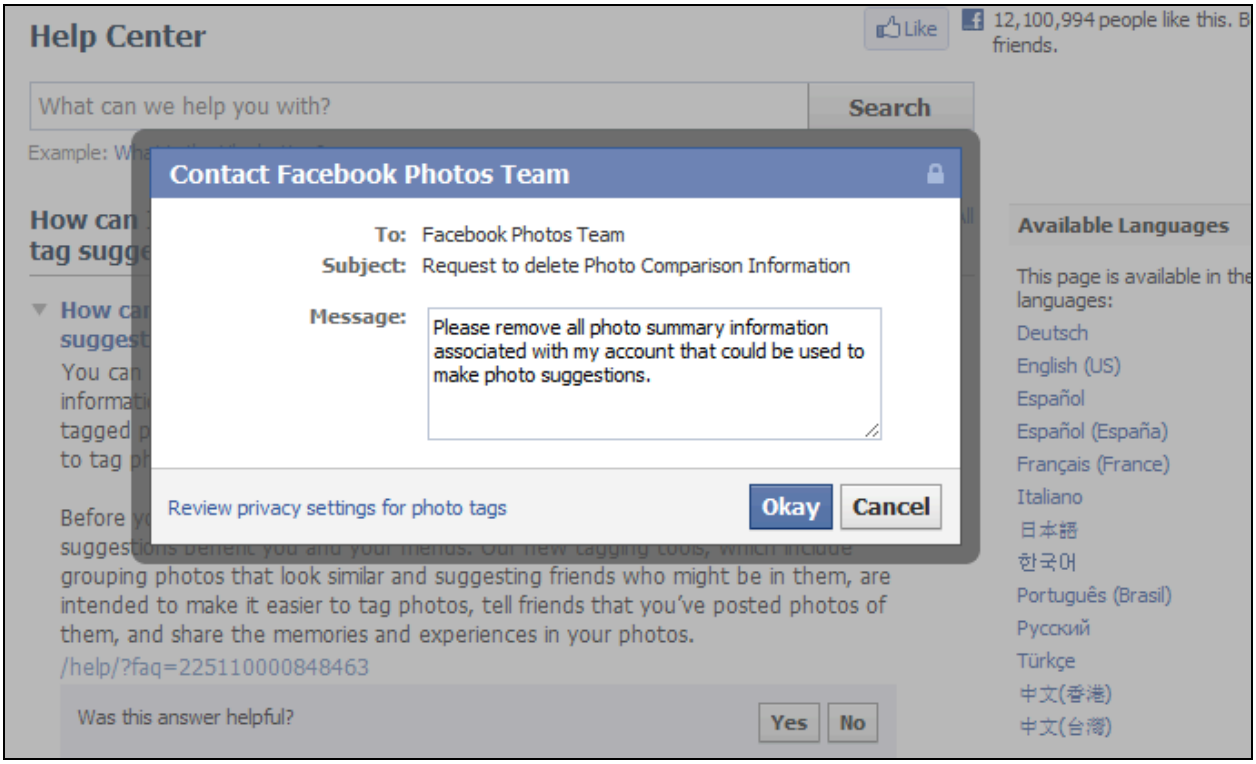
59. To access the link, a user must go to Privacy Settings – Customize Settings – Suggest Photos of me to friends—'Edit Settings' and click on the 'Learn more' link.



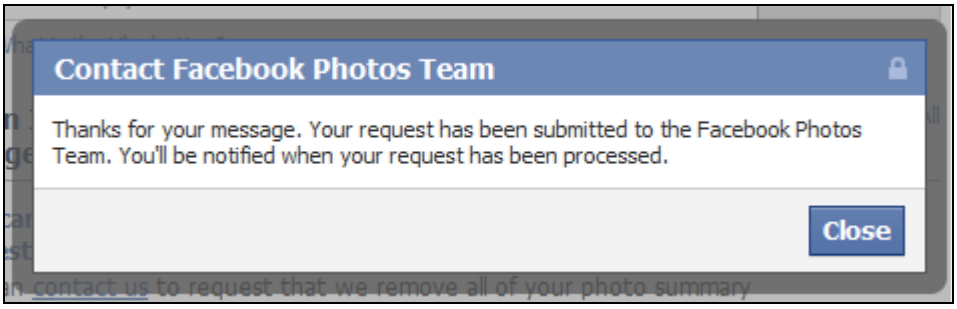
60. From there, the user is taken to a help center page - https://www.facebook.com/help/?page=1194. The last link on the page includes the correct instructions.



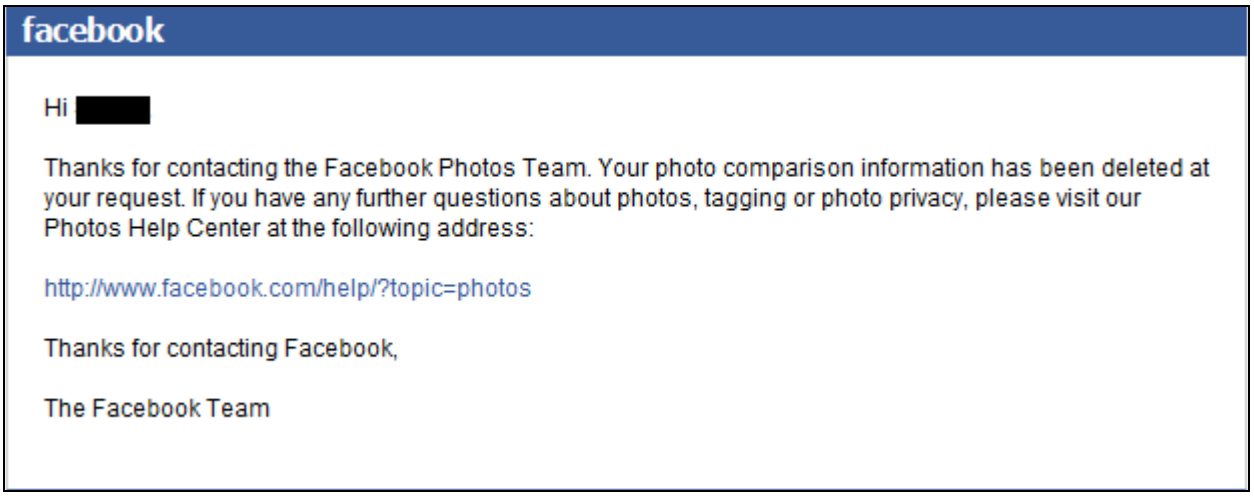
61. After clicking on "How can I remove the summary information stored about me for tag suggestions?" the user is presented with the contact link. Clicking on 'contact us' leads the user to send a message to Facebook's Photo Team.



62. Upon submitting a request to the Facebook Photo Team, the user is notified through a pop-up message that he or she will be notified when the request has been processed.



63. After the Facebook Photo Team deletes the biometric data that Facebook has collected, Facebook sends an email to the user stating that the "photo comparison information has been deleted . . ."


facebook

Hi [redacted]

Thanks for contacting the Facebook Photos Team. Your photo comparison information has been deleted at your request. If you have any further questions about photos, tagging or photo privacy, please visit our Photos Help Center at the following address:

http://www.facebook.com/help/?topic=photos

Thanks for contacting Facebook,

The Facebook Team

64. None of the help pages inform the user regarding whether or not Facebook will resume collecting biometric photo comparison data when pictures of him are manually tagged in the future.

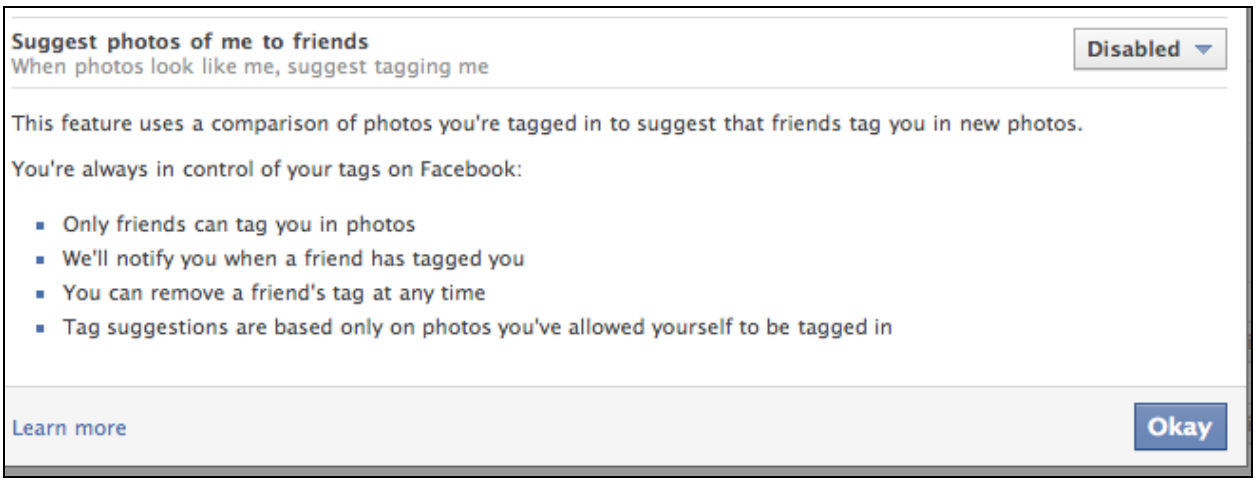
65. None of the help pages inform the user if the deleted biometric photo comparison data will ever be re-collected and used at a later time, like if the user subsequently enables the default name/face-pairing technology.

F. Facebook Provides an Option for Users to Disable the Company's Tag Suggestion Technology, But this Option Does not Disable Facebook's Collection of Users' Biometric Data

66. A Facebook user can opt-out of portions of Facebook's facial recognition program by disabling Facebook's default use of unique biometric identifiers generated by the "Photo Comparison Data" to identify individual users when a photograph containing their image is uploaded to Facebook.

67. When the default name pairing setting is disabled, the user's friends will have to manually type and select his name during the photo tagging process instead of having Facebook automatically generate his name when it recognizes his face.

68. A user can disable the name pairing default by clicking Account: Privacy Settings: Customize Settings: Edit Settings next to "Suggest photos of me to friends": and Disable.



69. This option disables Facebook's suggestion.

70. Facebook's opt-out for "Tag Suggestion" is cumbersome. A user must go through three screens and seven clicks to opt-out of having the user's name ppear as a "Tag Suggestion."[49]

G. Facebook Fails to Establish that Application Developers, the Government, and Other Third Parties Will Not Be Able to Access "Photo Comparison Data"

71. The Facebook Platform, used for creating applications ("apps") and for external websites implementing apps, makes a variety of information available to applications and external websites and applications.[50] Users give applications access to their basic account information when they connect with an application.[51] Applications may also make use of users' friends' data, in the context of the user's experience on an application,[52] and also use connections between users who have both connected to an application.[53]

72. App developers have access to the Facebook graph API. It "presents a simple, consistent view of the Facebook social graph, uniformly representing objects in the graph (e.g.,

[49] The User must click on Account → Privacy Settings → Custom → Customize Settings → "Edit Settings" next to "Suggest Photos of Me to Friends" → Change "Enable" to "Disable" → Okay.
[50] Facebook Platform Policies, Storing and Using Data You Receive From Us, https://developers.facebook.com/policy [hereinafter "Platform Policies"].
[51] *Id.* at ¶5.
[52] *Id.* at ¶4.
[53] *Id.* at ¶11.

people, photos, events, and pages) and the connections between them (e.g., friend relationships, shared content, and photo tags)."[54] Developers may leverage this API within apps.

73. Websites implementing Facebook plugins can use the Graph API "to access the user's Facebook profile. . . to access the user's social graph, bring their friends directly to your site all in your own custom experience."[55]

74. To obtain data necessary to develop applications, developers may only request the information that they need to operate their application. However, Facebook does not define what is necessary, and the terms leave developers to determine what they need.[56]

75. Facebook maintains different standards for information provided to advertisers and information Facebook will use to target advertisements to users. Facebook may make use of underlying, non-profile user data. For example, while Facebook may not provide users' IP addresses directly to advertisers, Facebook Ads uses IP addresses to determine users' locations and target ads to those locations.[57]

76. Facebook does not always maintain control over how user data is used by advertisers. An advertiser was caught using profile pictures in singles dating service advertisements, and Facebook spokesperson Barry Schnitt announced that "the ads that spooked people were from rogue networks. . . . ." Policing over 500,000 apps and advertisers is impracticable, as advertisers and rogue networks can choose not to disclose what they are actually doing with Facebook-provided user data.[58] Advertisers may cache Facebook user data indefinitely.[59]

77. Facebook's published privacy policy states that the Company may "disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law."[60] The U.S. Department of Justice ("DOJ") has stated that the "standard data production" from

[54] Facebook Developers, Graph API, https://developers.facebook.com/docs/reference/api.
[55] Facebook for Websites, Personalization, https://developers.facebook.com/docs/guides/web/#personalization.
[56] Platform Policies at ¶1.
[57] Reach and Targeting, Reach Real People With Precise Targeting, at Location Targeting, https://www.facebook.com/adsmarketing/index.php?sk=targeting_filters.
[58] Kim-Mai Cutler, *New data storage rules, permissions could rekindle Facebook privacy concerns*, Social Beat (Apr. 28, 2010) http://venturebeat.com/2010/04/21/facebook-privacynew-data-storage-rules.
[59] Ethan Beard, A New Data Model, Facebook Developer's Blog (Apr. 21, 2010) https://developers.facebook.com/blog/post/378.
[60] Facebook's Privacy Policy, Facebook, Dec. 21, 2010, available at https://www.facebook.com/policy.php

Facebook includes "photoprint," contact information, and Internet Protocol logs, while noting that "other data" is available and that Facebook is "often cooperative with emergency requests."[61]

78. Government has an interest in accessing the information present on Facebook and other social networking sites[62] and law enforcement has used Facebook in pursuing investigations.[63] Training materials used by DOJ have suggested that law enforcement agents can use evidence gathered from social networks to "reveal personal communications; establish motives and personal relationships; provide location information; prove and disprove alibis; [and] establish crime or criminal enterprise," among other "instrumentalities or fruits of crime."[64] The same training materials include a screenshot of the picture "tagging" process[65] and makes reference to the one billion pictures being added every month.[66]

H. Facebook's Terms of Service

79. Facebook requires users to obtain consent from others before they tag a photo: "You will not tag users or send email invitations to non-users without their consent."[73]

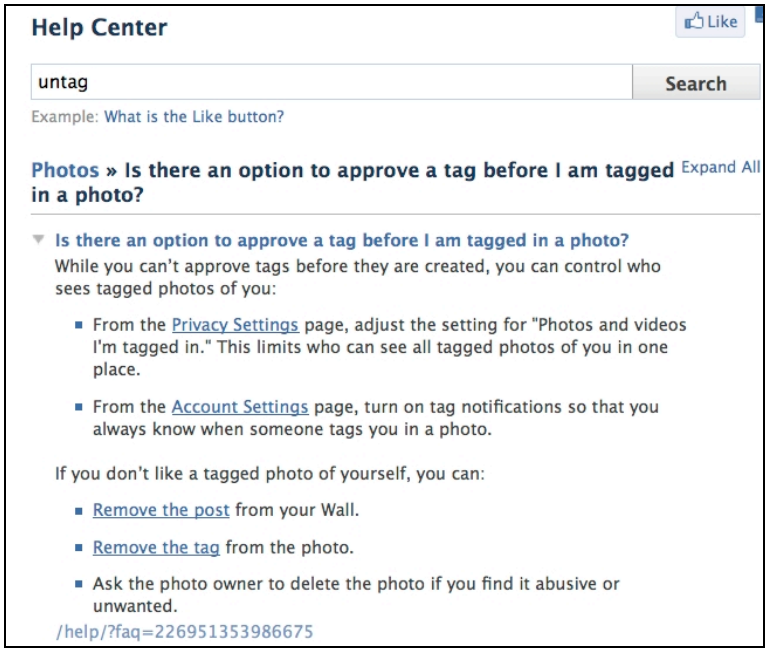
80. However, Facebook does not provide users with a technological means to enforce this obligation, telling users: "you can't approve tags before they are created."[74]

81. Facebook does not inform or remind the user that they must gain consent before tagging. And with the "tag suggestions" Facebook likely may cause users to decide to tag people in photos when they might not otherwise have done so.

---

[61] John Lynch & Jenny Ellickson, U.S. Dept. of Justice, Computer Crime and Intellectual Property Section, Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, Linkedln, and More, (Mar. 2010), 17, available at http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.
[62] *Id.*
[63] *See e.g.* Julie Masis, Is this Lawman your Facebook Friend?, BOSTON GLOBE, Jan. 11, 2009, http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend?mode=PF.
[64] John Lynch & Jenny Ellickson, U.S. Dept. of Justice, Computer Crime and Intellectual Property Section, Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, Linkedln, and More, (Mar. 2010), 11, available at http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.
[65] *Id*. at 15.
[66] *Id*. at 13.
[73] *Id*. at sec. 5.9.
[74] Facebook, *Is there an option to approve a tag before I am tagged in a photo?* https://www.facebook.com/help/?faq=15559&ref_query=untag

82. Instead, Facebook suggests that users untag themselves after an unwanted tag is applied or "ask the photo owner to delete the photo."[75]



83. Facebook has established the *Facebook Principles* as the foundation of the rights and responsibilities mentioned above.[76] Within these principles, Facebook states its commitment to a transparent process, where "Facebook should publicly make available information about its purpose, plans, policies and operations."[77]

I. Facebook Previously Made Public Commitments to Ensuring Users' Privacy

84. Facebook's Privacy Policy states that "[c]ertain downloadable software applications and applets that we offer, such as our browser toolbars and photo uploaders, transmit data to [Facebook]."[78]

85. Furthermore, Facebook's Privacy Policy states that it "may not make a formal disclosure if [Facebook] believe[s] [its[collection of and use of the information is the *obvious purpose of the application*."[79]

---

[75] *Id*.

76 Facebook, *Facebook Principles*, http://www.facebook.com/principles.php.

77 *Id*.

[78] Facebook, *Privacy Policy*, https://www.facebook.com/policy.php.

[79] *Id.*

86. For non-obvious information collection and use, Facebook states it "will make a disclosure to you the first time you provide the information to [Facebook] so that you can decide whether you want to use that feature."[80]

87. Facebook has been secretly collecting biometric data, "summary information," about photos with respect to specific users tagged in photos uploaded to Facebook.[81]

88. Photos uploaded to Facebook, including those uploaded through Facebook's photo uploader, "may be compared automatically to the summary information we've stored about what your tagged photos have in common. The results of this comparison may also be used to group photos or suggest that photos look like you."[82]

89. Facebook's photo uploader does not disclose the collection of this biometric photo comparison data to users to allow them to decide whether to use the technology.

90. Facebook does not allow users to opt-out of allowing Facebook friends to manually tag them in photos or to approve tags prior to being tagged in photos.[83]

J. Facebook Has a History of Improperly Changing Its Service in Ways that Harm Users' Privacy

91. In September 2006, Facebook disclosed users' personal information, including details relating to their marital and dating status, without their knowledge or consent through its "News Feed" program.[84] Hundreds of thousands of users objected to Facebook's actions.[85] In response, Facebook stated:

> We really messed this one up. When we launched News Feed and Mini-Feed we were trying to provide you with a stream of information about your social world. Instead, we did a bad job of explaining what the new features were and an even worse job of giving you control of them.[86]

---

[80] *Id.*

[81] Facebook, Help Center, https://www.facebook.com/help/?faq=19518.

[82] Facebook, Help Center, https://www.facebook.com/help/?faq=218540514842030.

[83] Facebook, Help Center, https://www.facebook.com/help/?faq=226951353986675.

[84] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/.

[85] Justin Smith, *Scared students protest Facebook's social dashboard, grappling with rules of attention economy*, Inside Facebook (Sept. 6, 2006), http://www.insidefacebook.com/2006/09/06/scared-students-protest-facebooks-social-dashboard-grappling-with-rules-of-attention-economy/.

[86] Mark Zuckerberg, *An Open Letter from Mark Zuckerberg* (Sept. 8, 2006), http://blog.facebook.com/blog.php?post=2208562130.

92. In 2007, Facebook disclosed users' personal information, including their online purchases and video rentals, without their knowledge or consent through its "Beacon" program. [87]

93. Facebook is a defendant in multiple federal lawsuits[88] arising from the "Beacon" program.[89] In the lawsuits, users allege violations of federal and state law, including the Video Privacy Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California's Computer Crime Law.[90]

94. On May 30, 2008, the Canadian Internet Policy and Public Interest Clinic filed a complaint with Privacy Commissioner of Canada concerning the "unnecessary and non-consensual collection and use of personal information by Facebook."[91]

95. On July 16, 2009, the Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[92]

96. On February 4, 2009, Facebook revised its Terms of Service, asserting broad, permanent, and retroactive rights to users' personal information—even after they deleted their accounts.[93] Facebook stated that it could make public a user's "name, likeness and image for any purpose, including commercial or advertising."[94] Users objected to Facebook's actions, and Facebook reversed the revisions on the eve of an EPIC complaint to the Commission.[95]

---

[87] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/ (last visited Dec. 15, 2009).

[88] In *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008), Facebook has requested court approval of a class action settlement that would terminate users' claims, but provide no monetary compensation to users. The court has not ruled on the matter.

[89] *See e.g.*, *Harris v. Facebook, Inc.*, No. 09-01912 (N.D. Tex. filed Oct. 9, 2009); *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008); *see also Harris v. Blockbuster*, No. 09-217 (N.D. Tex. filed Feb. 3, 2009), *appeal docketed*, No. 09-10420 (5th Cir. Apr. 29, 2009).

[90] *Id*.

[91] Letter from Philippa Lawson, Director, Canadian Internet Policy and Public Interest Clinic to Jennifer Stoddart, Privacy Commissioner of Canada (May 30, 2008), *available at* http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.

[92] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, July 16, 2009, *available at* http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

[93] Chris Walters, *Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."* The Consumerist, Feb. 15, 2009, *available at* http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html#reset.

[94] *Id*.

[95] JR Raphael, *Facebook's Privacy Flap: What Really Went Down, and What's Next*, PC World, Feb. 18, 2009, http://www.pcworld.com/article/159743/facebooks_privacy_flap_what_really_went_down_and_whats_next.html.

97. Facebook updated its privacy policy and changed the privacy settings available to users on November 19, 2009 and again on December 9, 2009.[96]

98. Facebook made the following categories of personal data "publicly available information:"

- users' names,
- profile photos,
- lists of friends,
- pages they are fans of,
- gender,
- geographic regions, and
- networks to which they belong.[97]

99. By default, Facebook discloses "publicly available information" to search engines, to Internet users whether or not they use Facebook, and others. According to Facebook, such information can be accessed by "every application and website, including those you have not connected with . . . ."[98]

[96] Facebook, *Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy* (Dec. 9, 2009), *available at* http://www.facebook.com/press/releases.php?p=133917.
[97] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).
[98] *Id.*

100. Prior to these changes, only the following items were mandatorily "publicly available information:"

- a user's name and
- a user's network.

101. EPIC and a broad coalition of organizations filed a complaint with the FTC in December 2009 regarding these changes.

102. Millions of users joined online groups and campaigns challenging Facebook's changes.

K. Facebook's Facial Recognition Techniques Put At Risk Young Children and are Contrary to COPPA

103. As of May 2011, at least 7.5 million U.S. children under the age of 13 actively use Facebook.[99] This includes more than 5 million children under the age of 10.[100]

104. Congress enacted the Children's Online Privacy Protection Act of 1998 ("COPPA") to address the special concerns associated with the collection of personal information from children.[101]

105. Facebook collects e-mail addresses and first and last names, which constitute personal information under COPPA, from each child with a Facebook account.[102]

106. Facebook has failed to establish that it does not collect photo summary data from minors.

107. Facebook's face recognition technology links a user's photo summary data to the user's account, including the user's email address and first and last name. Because it is combined with other personal information, the photo summary data also falls within COPPA's definition for personal information.[104]

---

[99] *Online Exposure: Social Networks, Mobile Phones, and Scams Can Threaten Your Security*, CONSUMER REPORTS, June 2011, at 30.

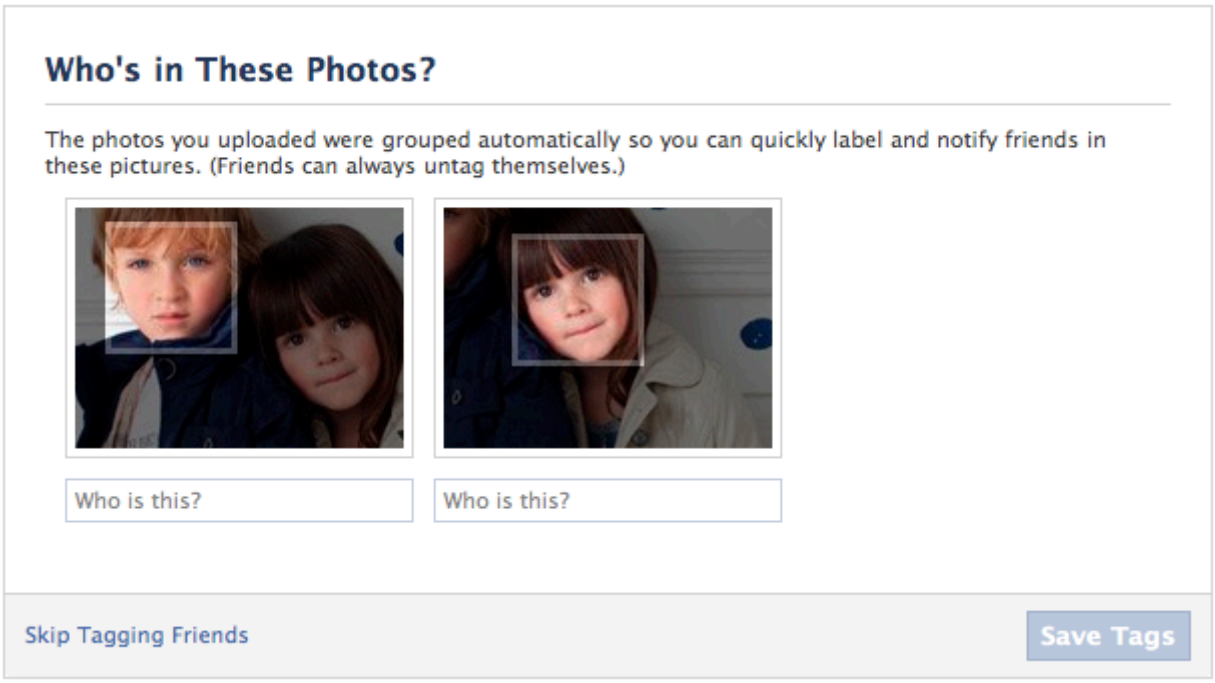
[100] *Id*.

[101] 16 C.F.R. 312 (1999).

[102] Facebook collects an e-mail address from each registered user. *See* Facebook's Privacy Policy, Facebook, http://www.facebook.com/policy.php (last updated Dec. 22, 2010).

[104] COPPA defines "personal information" to include "a first and last name," "an e-mail address," or "information

108. Facebook prompts users to provide data that enables Facebiij to create biometric profiles of children. Facebook recognizes children's faces when a photo is uploaded, and it prompts users to answer the question, "Who is this?"



109. Facebook users are encouraged to tag a child in photos even if the child is not a Facebook member. The only difference with this photo tag is that it will not yet link to a Facebook user profile. Facebook, however, will retain the data of the child's face paired with the child's name. This information can enable Facebook to create a biometric profile for the tagged child that has no other relationship with Facebook.

110. Facebook conditions a minor user's participation in photo sharing and tagging on the user's disclosure of photo summary data

111. Minors lack the capacity to consent to Facebook's Terms of Service and to understand the implications of disclosing personal information to Facebook.

---

concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph." 15 U.S.C. § 6501(8)(A), (C), (G) (2006).

112. Facebook materially benefits from the collection and use of personal information from its minor users.

L. Other Companies Have Been Far More Cautious About the Use of Facial Recognition Technology in Consumer Products

113. Apple first included facial recognition technology in its iPhoto picture management software in January 2009. iPhoto automatically detects faces in photos and allows the user to click on boxes drawn around detected faces and enter a name in a text field. iPhoto then searches the user's library for matching faces, including those in newly imported photos. The facially-matched photos appear as recommendations that the user is prompted to approve or deny.

114. iPhoto Faces currently only accesses and photos stored on a user's computer, as opposed to a network or service provider's servers. Apple's iCloud service, announced on June 6, 2011, automatically uploads and stores all photos from every user device to Apple servers. It is unclear if iPhoto Faces facial recognition data created by users will be transmitted to iCloud, or if Apple will have access to that data.

115. Google began utilizing facial recognition technology after acquiring a biometric and photo recognition company in 2006.

116. Google's photo software, Picasa, uses face-detection technology to scan a user's images for faces by default, unless the user opts-out. Unless it is disabled, Google scans and groups together the images that it believes to be of the same person. The user can add an associated name tag. If the user is signed in through her Google Account, she can use her Google contacts to add personal information to faces.

117. Google uses the same technology in its web-based photo product, Picasa Web Albums. Users can add a name tag by hovering the cursor over an image or clicking 'Add People.' When a user begins typing, the field auto-populates with the user's Google contacts. Selecting a Google contact for the name tag links the image to that person's e-mail address or other identifying information saved under the contact.

118. Google developed the technology to integrate this facial recognition technology into its mobile-based object detection product, Google Goggles. Google Chairman Eric Schmidt recently announced, however, that the company would not release it, noting that this technology could be used for good but also in a "very, very bad way." He pointed out that an "evil dictator" could use facial-recognition technology against people.

M. The Federal Trade Commissions Failure to Act on Pending Consumer Complaints Concerning Facebook's Unfair and Deceptive Trade Practices May Have Contributed to Facebook's Decision to Deploy Facial Recognition

119. On December 17, 2009, EPIC and 14 consumer and privacy organizations filed a Complaint with the FTC concerning Facebook's unfair and deceptive trade practices. The complaint cited widespread opposition from Facebook users, Senators, bloggers, and news organizations.[107]

120. EPIC's Complaint noted that "Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations."[108]

121. On January 14, 2010, EPIC filed a second Complaint with the Commission concerning Facebook's unfair and deceptive trade practices.[109]

122. EPIC's amended Complaint observed that Facebook's business practices "violate user expectations, diminish user privacy, and contradict Facebook's own representations."[110]

---

[107]

[108] *Id*.

[109]

[110] *Id*.

123. In a subsequent letter to Congress, EPIC urged the Members of the House and Senate oversight committees to pay careful attention to a new complaint that the consumer and privacy organizations had presented to the Federal Trade Commission regarding Facebook and change to user profile information and the disclosure of user data to third parties without consent.[111] The complaint alleged that these actions "violate user expectations, diminish user privacy, and contradict Facebook's own representations." EPIC noted that the complaint alleged unfair and deceptive trade practices that "subject to investigation and prosecution under Section 5 of the Federal Trade Commission Act."[112]

124. The letter cited numerous other complaints concerning regarding Facebook brought to the attention of the FTC in which the Commission failed to act. The EPIC letter warned:

> In the past, the Federal Trade Commission has taken decisive steps to safeguard consumer privacy. These decisions help spur innovation and competition, reduce risk to consumers, and promote trust and confience in new business services. But the current FTC appears reluctant to take similar steps on behalf of American consumers.

125. To date, the Federal Trade Commission has announced no action in the several complaints filed by consumer and privacy organizations regarding Facebook.

126. The Commission's failure to act on these prior complaints may have contributed to Facebook's decision to deploy face recognition technology as it did.

[111] Letter to Senator Rockefeller, et al from EPIC Executive Director Marc Rotenberg (May 5, 2010), http://epic.org/privacy/facebook/EPIC_FB_FTC_Complaint_Letter.pdf
[112] *Id.*

6. Legal Analysis

The FTC's Section 5 Authority

127. Facebook is engaging in unfair and deceptive acts and practices.[113] Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions.[114] These powers are described in FTC Policy Statements on Deception[115] and Unfairness.[116]

128. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[117]

129. The injury must be "substantial."[118] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[119] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[120] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces."[121] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[122] Finally, "the injury must be one which consumers could not reasonably have avoided."[123] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or

---

[113] *See* 15 U.S.C. § 45.
[114] *Id.*
[115] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), *available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm* [*hereinafter* FTC Deception Policy].
[116] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [*hereinafter* FTC Unfairness Policy].
[117] 15 U.S.C. § 45(n); *see, e.g.*, *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").
[118] FTC Unfairness Policy, *supra* note 113.
[119] *Id.*; *see, e.g.*, *Fed. Trade Comm'n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").
[120] FTC Unfairness Policy, *supra* note 113.
[121] *Id.*
[122] *Id.*
[123] *Id.*

takes advantage of an obstacle to the free exercise of consumer decisionmaking."[124] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[125]

130. The FTC will also look at "whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise."[126] Public policy is used to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present."[127]

131. The FTC will make a finding of deception if there has been a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[128]

132. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[129] The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[130] Second, the act or practice must be considered from the perspective of a reasonable consumer.[131] "The test is whether the consumer's interpretation or reaction is reasonable."[132] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[133]

---

[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] FTC Deception Policy, *supra* note 112.
[129] FTC Deception Policy, *supra* note 112; *see, e.g.*, *Fed Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).
[130] FTC Deception Policy, *supra* note 112.
[131] *Id.*
[132] *Id.*
[133] *Id.*

133. Finally, the representation, omission, or practice must be material.[134] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[135] Express claims will be presumed material.[136] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[137] The harms of this social networking site's practices are within the scope of the FTC's authority to enforce Section 5 of the FTC Act and its purveyors should face FTC action for these violations.

Facebook's Implementation of Facial Recognition Technology Constitutes Consumer Harm

134. Facebook's actions injure users throughout the United States by invading their privacy; allowing for disclosure and use of information in ways and for purposes other than those consented to or relied upon by such users; causing them to believe falsely that they have full control over the use of their information; and undermining the ability of users to avail themselves of the privacy protections promised by the company.

135. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices that constitute consumer harm.[138] The Commission realizes the importance of transparency and clarity in the collection of information about consumers. "Without real transparency, consumers cannot make informed decisions about how to share their information."[139]

Facebook's Use of Facial Recognition Technology Constitutes Constitutes an Unfair and Deceptive Trade Practice

136. Facebook has said that it "may not want everyone in the world to have the information you share on Facebook," and that users "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

[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] 15 U.S.C. § 45.
[139] Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection, New York University: "Promoting Consumer Privacy: Accountability and Transparency in the Modern World" (Oct. 2, 2009).

available to search engines and other outside entities."[140]

137. Facebook encouraged users to submit personal photographs to Facebook with the explicit assurance that they would retain control over their photographs.

138. Facebook further represented to users that they could "untag" themselves if they did not wish to be identified in photographs obtained by Facebook.

139. Users could not reasonably have known that Facebook would use their photos to build a biometric database in order to implement a facial recognition technology under the control of Facebook.

140. Facebook representations to users regarding the use of the photos they have provided to Facebook are a sham intended to induce users to provide personal information while concealing Facebook's true intent

141. Moreover, Facebook failed to establish adequate safeguards to prevent the misuse of this information by third parties, including the Government and application developers.

142. Absent injunctive relief by the Commission, Facebook is likely to continue its unfair and deceptive business practices and harm the public interest, as evidence by the company's repeated changes to its privacy policy and aggressive efforts to make more user data "publicly available."

143. Absent injunctive relief by the Commission, Facebook will likely expand the use of the facial recognition database it has covertly established for purposes over which Facebook users will be able to exercise no meaningful control.

[140] Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), *available at* http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf.

7. Prayer for Investigation and Relief

144. Petitioners request that the Commission investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users. Specifically, Petitioners ask the Commission to:

a. require Facebook to suspend immediately any form of Facebook-initiated "tagging" or other forms of person-identification of Facebook users based on Facebook's internal database of facial images

b. Require Facebook to not misrepresent in any manner, expressly or by implication the extent to which Facebook maintains and protects the security, privacy, confidentiality, and integrity of any consumer information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses consumer information (2) the extent to which consumers may exercise control over the collection, use, or disclosure of consumer information**.**

c. Require that Facebook, prior to any new or additional sharing by Facebook of a user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, Facebook shall: A. clearly and prominently disclose: (1) that the user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for Facebook's sharing; and B. Obtain express affirmative consent from the user to such sharing.

d. Require Facebook to establish and implement, and thereafter maintain, 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 security, privacy, confidentiality, and integrity of consumer information. Such program should include:

1. the identification of reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of consumer information or in unauthorized administrative control of Facebook, and an assessment of the sufficiency of any safeguards in place to control these risks.
2. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or

monitoring of the effectiveness of the safeguards' key controls, systems, and procedures

e. Permit Facebook to reintroduce auto-tagging features only after it has:
    1. Established appropriate security safeguards
    2. Revised its privacy policy to limit disclosure of user information, including tagged images, to third parties only where required by law and not simply where Facebook has a "good faith" reason to believe that there is a legal requirement to do so
    3. Obtain informed user consent that also allows individuals to subsequently opt-out of the auto-tagging features

f. Seek appropriate injunctive and compensatory relief.

145. EPIC, and the consumer organizations listed above, reserve the right to amend this complaint and to bring other relevant matters to the attention of the Commission.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
John Verdi, EPIC Senior Counsel
Ginger McCall, EPIC Open Government Counsel
Sharon Goott Nissim, EPIC Consumer Protection Counsel
ELECTRONIC PRIVACY INFORMATION CENTER[141]
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

[141] EPIC is grateful for the assistance of EPIC Clerks Pamela Hartka, James Kleie, Sapna Mehta, Francisco Riojas, Jeramie Scott, Alexander Stout,and Alexandra Wood, who contributed to this Complaint.