

Before the  
FEDERAL TRADE COMMISSION  
WASHINGTON, DC 20580

In the Matter of )  
 )  
Request to Investigate Facebook, Inc.'s )  
Misrepresentations of its Face Recognition )  
Setting for Violating the Federal Trade )  
Commission Act and the 2011 )  
Consent Agreement )  
 )

Submitted by

Consumer Reports

Katie McInnis  
Policy Counsel  
Consumer Reports  
1101 17th Street NW  
Suite 500  
Washington, DC 20036  
(202) 462-6262

May 20, 2019

## Table of Contents

|                                                                                                                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Summary.....                                                                                                                                                                                           | 2  |
| I. Background.....                                                                                                                                                                                     | 4  |
| A. Tag Suggestions Control.....                                                                                                                                                                        | 4  |
| B. Face Recognition Control.....                                                                                                                                                                       | 6  |
| C. Instances of Consumers Lacking Important Face Recognition Control Documented.....                                                                                                                   | 8  |
| D. Consumers who lack Face Recognition control also faced increased difficulty navigating to their available facial recognition control: Tag Suggestions.....                                          | 10 |
| II. Facebook’s practices are deceptive under the Federal Trade Commission Act.....                                                                                                                     | 12 |
| A. Facebook represents to consumers that they would have access to the Face Recognition Setting and this setting would be “off” by default or align with the user’s older Tag Suggestions setting..... | 12 |
| B. Facebook’s representations mislead consumers.....                                                                                                                                                   | 16 |
| C. Facebook’s misleading representations are material to the consumer.....                                                                                                                             | 18 |
| D. Under the precedent of <i>Chitika</i> , <i>InMobi</i> , <i>Nomi</i> , and the <i>Google/Safari</i> settlements, the Commission should investigate Facebook’s conduct.....                           | 18 |
| III. Facebook’s practices violate the 2011 <i>Consent Agreement</i> .....                                                                                                                              | 20 |
| IV. Conclusion and Request for Relief .....                                                                                                                                                            | 21 |

## Summary

Consumer Reports<sup>1</sup> (CR) asks the Federal Trade Commission (FTC) to investigate whether Facebook, Inc. is violating the Federal Trade Commission Act (FTC Act) and the 2011 *Consent Agreement* in connection with its Face Recognition control provided to users on their Facebook platform.

The Federal Trade Commission Act makes it unlawful for one to engage in “unfair or deceptive acts or practices in or affecting commerce.”<sup>2</sup> Under the Federal Trade Commission’s Deception Statement, for an act to be deceptive, it must be a representation, omission or practice that is likely to mislead a reasonable consumer and this representation, omission, or practice must be material. The FTC clarified that materiality is assessed on the basis of whether or not the practice is “likely to affect the consumer’s conduct or decision with regard to a product or service.”<sup>3</sup>

In 2011, Facebook entered into a settlement agreement with the Federal Trade Commission to settle charges “that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.”<sup>4</sup> The *Consent Agreement* reached between Facebook and the Commission states that Facebook:

...shall not misrepresent 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:

- A. Its collection or disclosure of any covered information;
- B. The extent to which a consumer can control the privacy of any covered information maintained by [Facebook] and the steps a consumer must take to implement such controls;<sup>5</sup>

Under the *Agreement*, “covered information” is defined to include “information from or about an individual consumer, including but not limited to...(e) photos and videos.”<sup>6</sup>

---

<sup>1</sup> Consumer Reports is the world’s largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

<sup>2</sup> Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

<sup>3</sup> Fed. Trade Comm’n, FTC Policy Statement on Deception (1983), <http://www.ftc.gov/bcp/policystmt/ad-decept.htm> [hereinafter FTC Deception Policy].

<sup>4</sup> *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, FED. TRADE COMM’N (Nov. 29, 2011), <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep> [hereinafter *Facebook Settles*].

<sup>5</sup> In the Matter of Facebook, Inc., Decision and Order, No. C-4365, p. 3-4, <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf> [hereinafter 2011 Consent Agreement].

<sup>6</sup> *Id.*

Facebook provides an online social media platform that allows users to upload their own content to the site, including photos and videos. From December 2011, Facebook has provided users with a control called “Tag Suggestions” that allows users to decide whether or not other users on the site will be served with suggested tags for photos that appear to match the physical characteristics of the individual user. Facebook’s Tag Suggestions feature uses facial recognition technology to identify whether or not a particular user is in the photo or video that is uploaded to the site.

In December 2017, Facebook announced a new setting, “Face Recognition,” which would replace the older Tag Suggestions control for consumers in the US. With this new control, US-based users are able to control whether or not the company’s facial recognition technology is used on the content they upload to the site. This setting, unlike the prior one, also allows the user to opt out of future applications of facial recognition technology on the site.

Since at least May 1, 2019, but perhaps as early as June 2018, Facebook has not provided access to the Face Recognition tool to all US-based users. Consumer Reports first noticed that some profiles lacked access to the Face Recognition control, but instead had the older Tag Suggestions setting, in June 2018. At that time, Facebook declined to provide a comment on the record about this inconsistency in access to privacy controls. However, in early May 2019, Consumer Reports conducted a study with 31 participants across the United States, finding that 8 out of 31, or 26 percent, of those users lacked access to the new Face Recognition tool. These users instead could access the older, and less protective opt-out, Tag Suggestions tool.

Facebook deceived their users by representing that US-based consumers over the age of 18 would have access to the new, and more protective opt-out control of Face Recognition. However, some consumers lack this control. In addition, Facebook represented to consumers that this new control would reflect their prior facial recognition preferences, as indicated by the Tag Suggestions setting. Therefore, if a consumer opted-out of the Tag Suggestions setting they could reasonably assume that they have already opted-out of Facebook’s facial recognition processing, when in fact all they opted-out of was allowing their friends to get tag suggestions for them. Further, these users faced greater difficulty navigating to even the less protective opt-out of facial recognition processing because the new interface and help pages do not provide clear links to the Tag Suggestions system.

Facebook also deceived their users by representing that the new Face Recognition setting would be set to “off”/“no” by default or would align with the user’s past expressed preferences with regards to facial recognition as indicated by whether they changed their default Tag Suggestions setting (i.e., by changing the setting from “Friends” to “No one,” thus opting out of this narrow control on facial recognition technology). First, our study documented that new accounts are initially given the older Tag Suggestions setting, which is on by default. For those users, they have no previous settings to inherit and have no facial recognition protection by default, despite Facebook’s representations. Further, even if they eventually get the new Face Recognition setting,

which would be “on”/“yes” by default, Facebook’s public statements that the default for the Face Recognition control is “off”/“no” leaves them in the position of assuming that they are protected when they are not

In light of these findings, we respectfully request the Commission to investigate these practices and assess civil penalties that demonstrate that violations of the Federal Trade Commission Act and 2011 *Consent Agreement* are impermissible.

## **I. Background**

### **A. Tag Suggestions Control**

On December 15, 2010, Facebook first announced its “Tag Suggestions” feature, which uses “face recognition software—similar to that found in many photo editing tools—to match your new photos to other photos you're tagged in.”<sup>7</sup> The setting was on by default,<sup>8</sup> meaning that users were automatically opted into Facebook’s facial recognition technology recommending tags to connections if the user’s face was identified in a photo or video uploaded to Facebook. However, Facebook did provide the ability to opt out.<sup>9</sup>

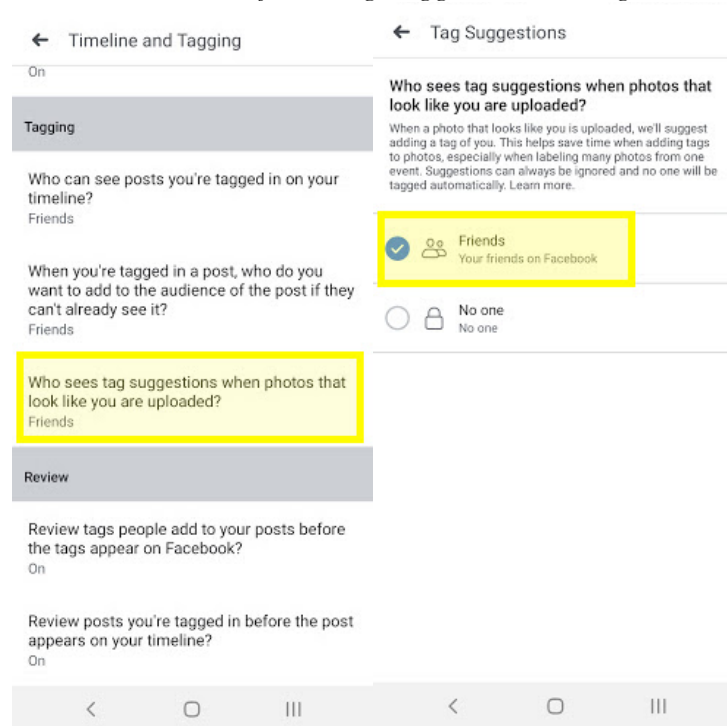
---

<sup>7</sup> Matt Hicks, *Making Photo Tagging Easier*, FACEBOOK (June 30, 2011, 5:16 PM), <https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/> [hereinafter *Making Photo Tagging*].

<sup>8</sup> “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.” *Id.*; and, see, Ian Paul, *Facebook Photo Tagging: A Privacy Guide*, PC WORLD (June 9, 2011), [https://www.pcworld.com/article/229870/Facebook\\_Photo\\_Tagging\\_A\\_Privacy\\_Guide.html](https://www.pcworld.com/article/229870/Facebook_Photo_Tagging_A_Privacy_Guide.html).

<sup>9</sup> “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. You can learn more about this feature in our Help Center.” *Making Photo Tagging*, *supra* note 7.

### *A user's default Tag Suggestions setting*



The Tag Suggestions featured on Facebook uses a four-step facial recognition process:

Initially, the software tries to detect faces (the “detection” step) and standardizes any detected faces for qualities like orientation and size (the “alignment step”). For each face that is detected and aligned, Facebook computes a “face signature,” which is a “string of numbers that represents a particular image of a face” (the “representation” step). Face signatures are then run through a stored database of user “face templates” to look for matches (the “classification” step). A face template is “a string of numbers that represents a boundary” between the face signatures of a given Facebook user and the face signature of others, and is calculated based on that user’s photographs. If a computed face signature falls within the boundary described by a user’s face template, Facebook suggests tagging the user. Facebook represents, with no challenge from plaintiffs, that face signatures are not stored. Only face templates are kept by Facebook.<sup>10</sup>

With this tool, the site’s users are not able to stop Facebook from scanning photos, creating “templates” of each face, and retaining the data. However, this setting did allow users to prevent Facebook’s facial recognition system from suggesting that others tag you in photos.<sup>11</sup> According

<sup>10</sup> Citations omitted. Order re Class Certification, In Re Facebook Biometric Information Privacy Litigation, No. 3:15-cv-03747-JD, (N.D. Cal. Apr. 16, 2018), *available at* <https://docs.justia.com/cases/federal/district-courts/california/candce/3:2015cv03747/290385/333>.

<sup>11</sup> *Making Photo Tagging*, *supra* note 7.

to Facebook, if you untag a photo or video, “information from those photos and videos is no longer used in the face template.”<sup>12</sup>

## B. Face Recognition Control

On December 19, 2017, Facebook announced that they updated the privacy settings on the site to allow users to turn off the use of facial recognition technology on their photos:

We also decided to update Facebook’s settings. Concerns about updated settings are as old as Facebook, so we didn’t take the decision lightly. But we learned in our research that people want a way to completely turn off face recognition technology rather than on a feature-by-feature basis. We knew that as we introduced more features using this technology, most people would find it easier to manage one master setting rather than navigate a long list of products deciding what they want and what they don’t. Our new setting is an on/off switch. Some may criticize this as an “all or nothing” approach, but we believe this will prevent people from having to make additional decisions among potentially confusing options.<sup>13</sup>

The underlying facial recognition technology for both the Face Recognition and Tag Suggestions settings appears to be the same,<sup>14</sup> but the new tool seems to have been designed to allay consumer concerns, while also introducing new features.<sup>15</sup> Furthermore, if a user sets their face recognition setting to “off”/“no,” Facebook “delete[s] the template”<sup>16</sup> and opts the user out of all facial recognition features, including any new features based on this technology that the site might introduce in the future. By contrast, the older tool (Tag Suggestions) only allowed users to prevent Facebook from recommending that others tag them in photos, and did not prevent Facebook from: scanning photos and videos; creating face templates and retaining that data; or any further

---

<sup>12</sup> *Tagging Photos*, Facebook, <https://www.facebook.com/help/463455293673370> (last visited May 16, 2019).

<sup>13</sup> Rob Sherman, *Hard Questions: Should I Be Afraid of Face Recognition Technology?*, FACEBOOK NEWSROOM (Dec. 19, 2017), <https://newsroom.fb.com/news/2017/12/hard-questions-should-i-be-afraid-of-face-recognition-technology/> [hereinafter *Hard Questions*].

<sup>14</sup> “But how does this technology really work? It starts with showing a computer photos of the same person. The computer analyzes the pixels in each image and generates a string of numbers to represent a person’s face. Then, the computer analyzes images of other people and creates strings for each of them too. So whenever the system is presented with a new photo, it can quickly find matches on the photos it already has.” Transcript of *Hard Questions: Face Recognition* Animated Video, FACEBOOK (Dec. 17, 2019), <https://www.facebook.com/facebook/videos/10156872585996729/> [hereinafter *Hard Questions Video*]; “On Facebook, face recognition helps people tag photos with the names of their friends. When you have face recognition enabled, our technology analyzes the pixels in photos you’re already tagged in and generates a string of numbers we call a template. When photos and videos are uploaded to our systems, we compare those images to the template.” *Hard Questions*, *supra* note 13.

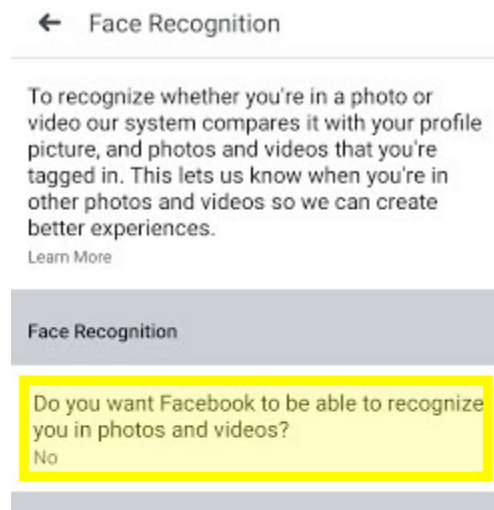
<sup>15</sup> “We recently announced new features that use face recognition technology. People can now find photos of themselves even when they aren’t tagged in them, making it possible for people to manage their privacy in new ways. They may also know when someone is using their image as a profile photo — which can help stop impersonation. In addition, those with vision impairments can now hear aloud who’s in the photos they come across on Facebook. Just as in 2010, we had to evaluate how we’d inform people and give them choice over these new uses of the technology.” *Hard Questions*, *supra* note 13.

<sup>16</sup> *Tagging Photos*, *supra* note 12.

application of facial recognition technology to their photos or videos or those uploaded by others.

The new Face Recognition setting is set to “off”/“no” by default, meaning that users are not automatically opted into allowing Facebook’s facial recognition technology to scan their photos and videos uploaded to the site.<sup>17</sup>

*Screenshot of the default Face Recognition setting*



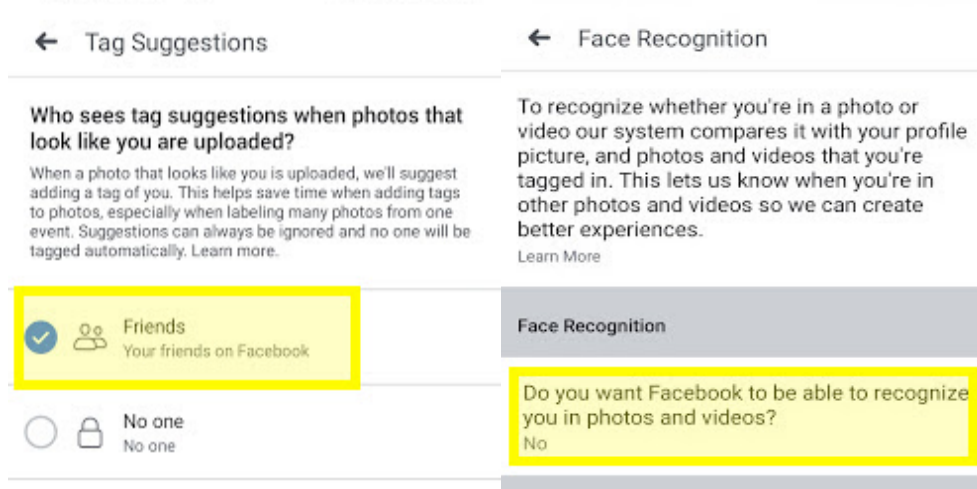
However, in order to respect a user's present privacy practices, Facebook stated that the default Face Recognition control would reflect the settings users had chosen with the older Tag Suggestions feature (i.e., if a person set their Tag Suggestions setting to “off”/“no one” in the past, their Face Recognition setting would be set to “off”/“no” automatically, opting the user out of the use of facial recognition technology).<sup>18</sup>

---

<sup>17</sup> Lily Hay Newman, *How to Turn Off Facebook's Face Recognition Features*, WIRED (Feb, 28, 2018), <https://www.wired.com/story/how-to-turn-off-facebook-face-recognition-features/> [hereinafter *Facebook's Face Recognition*].

<sup>18</sup> *Id.*

*If a user changed their Tag Suggestions setting to “off”/“no one” previously, the new Face Recognition control would also be set to “off”/“no”*



### C. Instances of Consumers Lacking Access to Important Face Recognition Control Documented

Consumer Reports documented through a small, qualitative study of US-based Facebook users that some of the site’s users lack the Face Recognition setting that was introduced in December 2017. We first spotted this issue in June 2018. Although we contacted Facebook about this possible anomaly, Facebook did not comment on the record at that time. In early May 2019, Consumer Reports conducted an online study with 31 Facebook users across the United States.

Consumer Reports utilized a service called UserTesting to conduct our study. Participants are paid a nominal fee for their time, and can be directed to perform various tasks and answer questions about their experiences. As participants complete tasks, the service captures video of their screens. The videos, along with recordings of written and verbal responses to questions are sent to the organization conducting the study.

Our study consisted of 34 Facebook users. Two users from our initial pool of participants reported that they lived outside the United States, and were excluded from our final results, as laws regarding biometrics or privacy writ large may affect Facebook’s practices in those countries and the distribution of its privacy settings. We also excluded one user who did not complete the study, for a final pool of 31 participants.

UserTesting lets its clients design tests and establish qualifications in order to target specific groups of consumers. Participants who meet those qualifications are then selected at random from among the service’s pool of consumers. Participants were required to use the Chrome web browser, which UserTesting recommends in order to ensure the proper functioning of the UserTesting

platform.

After running a small test of five participants to confirm that our protocol would be easy to follow, we added more participants with additional requirements: We excluded participants from outside the United States, and targeted some users who were residents of Illinois. The goal with that requirement was to research whether a state law, the Illinois Biometrics Information Privacy act, has any effect on the availability of the setting. Our findings did not indicate that the Facebook platform treats Illinois residents any differently when it comes to the availability of the Face Recognition setting.

We had participants log in to Facebook.com, and directed them to navigate to different areas of the site in order to document whether the Face Recognition setting was available. We also had users show us the availability of a Tag Suggestions setting, to test our hypothesis that users are granted access to one of those two settings, but not both. We documented whether these settings were turned on or off, and asked whether users had adjusted them in the past.

We found that the Face Recognition setting to be available to most users, but the setting was missing from eight out of the final pool of 31 accounts we documented.

As part of our test, we asked users a number of questions to research whether demographic or behavioral patterns had any effect on the availability of the setting. Questions included how often participants use Facebook, what kind of phones and computers they use, whether or not they use the Facebook mobile app, and whether the participants had ever used Facebook while traveling outside of the United States. In addition, we had users navigate to certain pages that would allow us to document how many “friends” they had, when their accounts were created, and whether or not the users’ “profile pictures” were photographs of their faces. We also gathered information about each user’s age and gender from self-reported information through the UserTesting platform. None of these factors seemed to affect the availability of the Face Recognition setting.

In addition to our formal test, we asked members from two Consumer Reports Facebook groups to check if the setting was available. Among hundreds of replies, a number of users reported that the Face Recognition setting is unavailable to them. While this anecdotal evidence reinforces the findings of our study, we did not include these results in our analysis as we did not have documentation to confirm the accuracy of these responses.

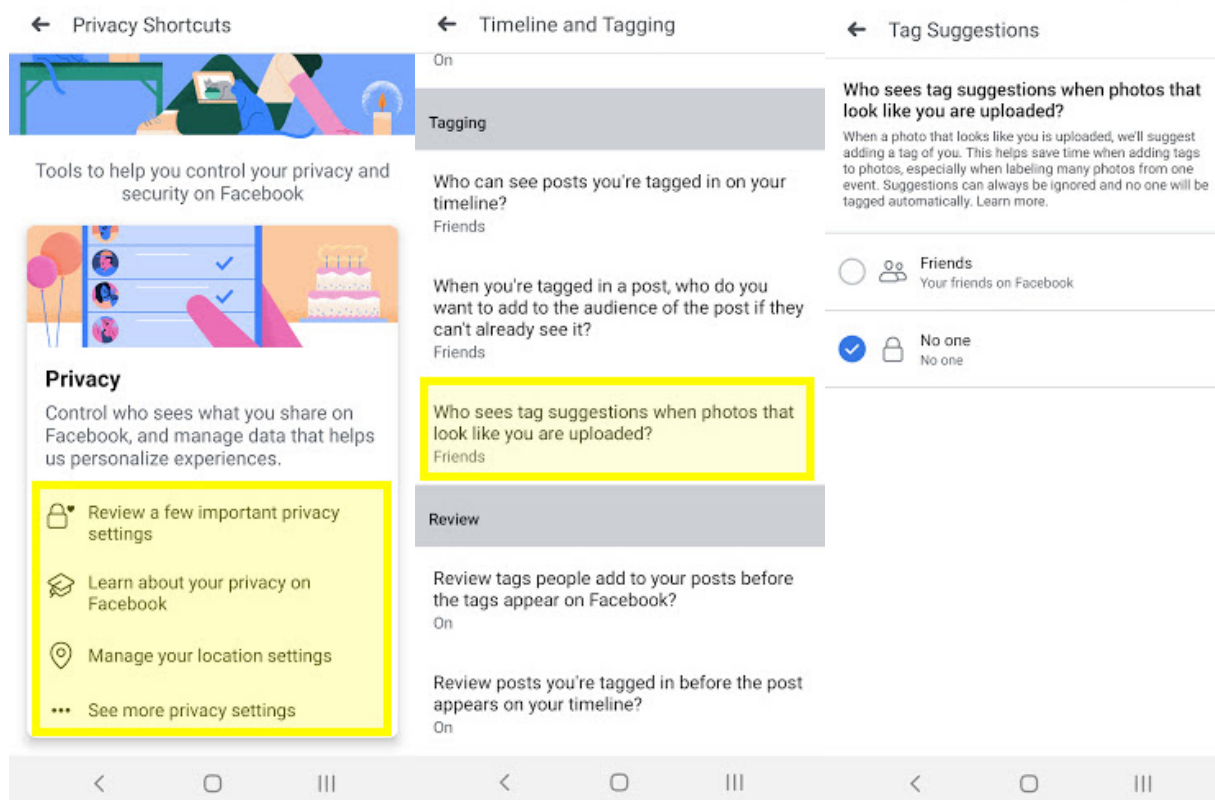
In a separate experiment, Consumer Reports tried to see whether the Face Recognition setting worked. We downloaded archives of Facebook data from user accounts that did have the Facial Recognition setting. If the feature had been turned on for several days, the archive included a file labeled Face Recognition containing a long string of characters that may have been the facial recognition template. If Facial Recognition had been turned off, that file did not appear in our

archive, indicating the setting is likely working when it is available.

D. Consumers who lack Face Recognition control also faced increased difficulty navigating to their available facial recognition control: Tag Suggestions

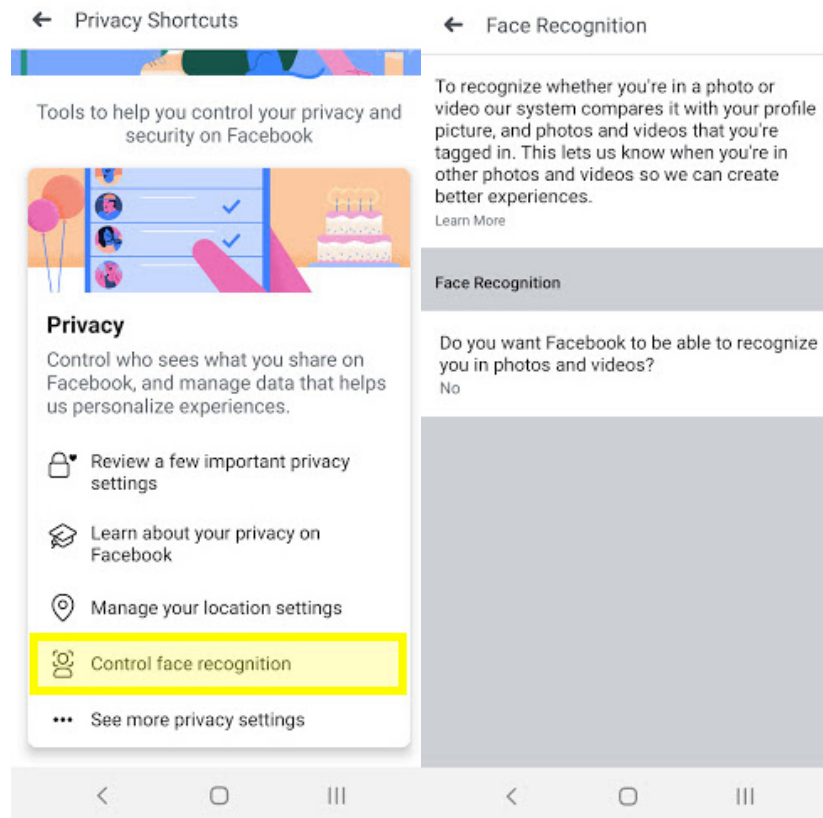
As shown in the screenshots below, the privacy shortcuts page for users who do not have the new Face Recognition setting lacks any shortcut to modify their Tag Suggestions control. A user must instead find their Tag Suggestions setting by navigating to their main account settings page through a different menu.

*Screenshots of A User's Tag Suggestions Setting*



As documented in the screenshots below, a user who does have access to the Face Recognition setting Facebook introduced in December 2017 can easily access and change their facial recognition control from their privacy shortcuts page. This ease of navigation is contrasted with the relative difficulty with which a user who only has the older Tag Suggestions control would have finding their Tag Suggestions setting.

### Screenshots of a User's Face Recognition Setting



If a user was presented with the older Tag Suggestions control and not the newer Face Recognition control, it was harder for the user to navigate to the appropriate setting. A slide show on Facebook's "Privacy Basics"<sup>19</sup> page explains how the Face Recognition control works and provide illustrations of what the setting looks like, and how to use it. The penultimate informational final slide reads, "You can turn the setting on or off at any time, which will also apply to any features we add later," and includes a link<sup>20</sup> which directs users to the page where they can adjust the setting.<sup>21</sup>

<sup>19</sup> *Manage Your Privacy: Face Recognition*, FACEBOOK, <https://www.facebook.com/about/basics/manage-your-privacy/face-recognition> (last visited May 20, 2019).

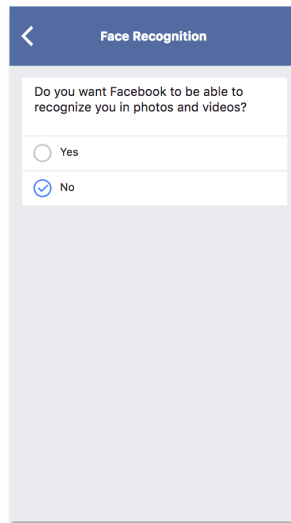
<sup>20</sup> *Settings: Face Recognition*, FACEBOOK, <https://www.facebook.com/settings?tab=facerec> (last visited May 20, 2019).

<sup>21</sup> *Id.*

### *Screenshot of the penultimate informational slide*

< Manage Your Privacy

MENU >



You can turn the [setting](#) on or off at any time, which will also apply to any features we add later.

But if the user does not have the Face Recognition control, that link just takes them to their main account settings page. Then it is up to the user to figure out that, on their account, the setting does not exist. Aside from concerns about the availability of this important control, the lack of usable links in these explanations for consumers about Facebook’s face recognition technology makes the process of changing one’s privacy settings even more complicated and onerous. Consumers already have a hard time utilizing the few privacy controls they do have, and this broken disclosure system only serves to exacerbate the problem.

## **II. Facebook’s practices are deceptive under the Federal Trade Commission Act**

The Federal Trade Commission has the ability under the Federal Trade Commission Act to prevent the use of “unfair or deceptive acts or practices in or affecting commerce.”<sup>22</sup> Under the Federal Trade Commission’s Deception Statement, for an act to be deceptive, it must be a representation, omission or practice that is likely to mislead a reasonable consumer and this representation, omission, or practice must be material. The FTC clarified that materiality is assessed on the basis of whether or not the practice is “likely to affect the consumer’s conduct or decision with regard to a product or service.”<sup>23</sup>

### A. Facebook represents to consumers that they would have access to the Face

---

<sup>22</sup> Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

<sup>23</sup> FTC Deception Policy, *supra* note 3.

Recognition Setting and this setting would be “off” by default or align with the user’s older Tag Suggestions setting

From at least December 2017 to the present, Facebook represented to US-based consumers that they would be able to turn off facial recognition on the site. In an animated video in the post announcing the new Face Recognition control the company says: “Anyone can opt out of face recognition entirely through their Facebook account settings.”<sup>24</sup>

*A Screenshot of the Animated Video by Created and Hosted by the Company on their Facebook Newsroom site<sup>25</sup>*



Facebook also states in their blog post announcing this new setting that “when it comes to face recognition, control matters.”<sup>26</sup>

*Screenshot from the blog post in the Facebook Newsroom site announcing the new Face Recognition Control*

### **Our Responsibility**

When it comes to face recognition, control matters.

We listen carefully to feedback from people who use Facebook, as well as from experts in the field. We believe we have a responsibility to build these features in ways that deliver on the technology’s promise, while avoiding harmful ways that some might use it.

<sup>24</sup> *Hard Questions Video*, *supra* note 14.

<sup>25</sup> *Id.*

<sup>26</sup> *Hard Questions*, *supra* note 13.

In addition, in Facebook’s Help Center, the company provides consumers with explanations on how to turn off facial recognition for their account. These instructions represent that these users should be able to turn off the use of this technology, despite the fact that Consumer Reports documented that some consumers lack this control entirely.<sup>27</sup>

*Screenshot of a section of the Facebook Help Center page*


## How do I turn face recognition on or off for my account?

[Computer Help](#) [Mobile Help](#) ▾

[Share Article](#)

Face recognition helps Facebook recognize you in photos or videos based on your profile picture and photos or videos you are tagged in. Learn about [how face recognition may be used on Facebook](#).

To turn face recognition on or off for your account:

- 1 Click  in the top right of Facebook and select **Settings**.
- 2 In the left column, click **Face Recognition**.
- 3 Go to **Do you want Facebook to be able to recognize you in photos and videos?** and click **Edit**.
- 4 Select **Yes** or **No** to confirm your choice.

When Face Recognition is set to off, templates are deleted.

Note: This setting isn't available in all countries, and will only appear in your profile if you are at least 18 years old.

Users who visited their Facebook home page following the release of the new setting in December 2017 were alerted to this new control via a pop-up dialogue box in their newsfeed,<sup>28</sup> similar to one that was included in a Wired story<sup>29</sup> in February 2018.

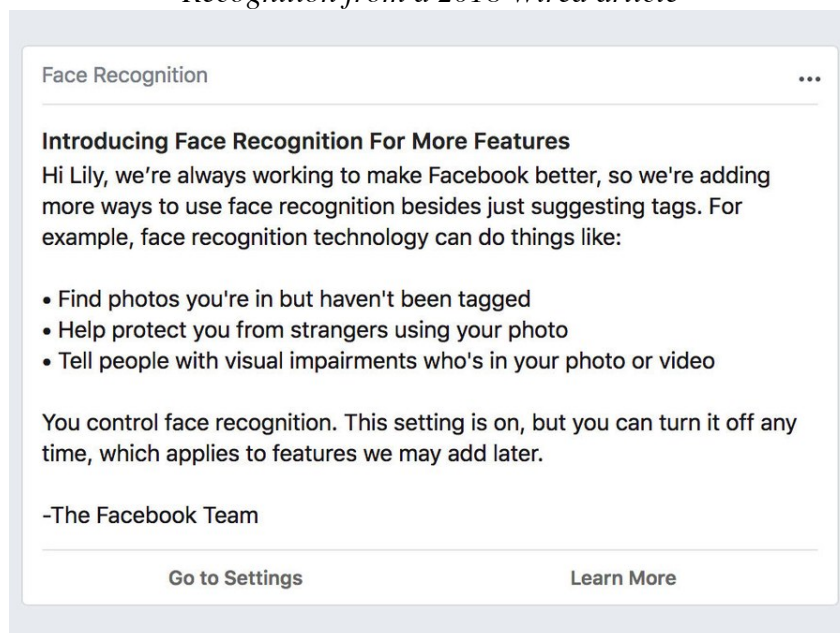
---

<sup>27</sup> *How do I turn face recognition on or off for my account?*, FACEBOOK HELP CENTER, [https://www.facebook.com/help/187272841323203?helpref=uf\\_permalink](https://www.facebook.com/help/187272841323203?helpref=uf_permalink) (last visited May 18, 2019).

<sup>28</sup> “People asked us to explain how face recognition works more clearly, and to provide more prominent information about how we might use it on Facebook. To address this feedback, we’re informing people about updates to face recognition in News Feed – the doorstep of Facebook.” *Hard Questions*, *supra* note 13.

<sup>29</sup> *Facebook’s Face Recognition*, *supra* note 17.

*Screenshot of a Facebook pop-up dialogue box that gives users more information about the Face Recognition from a 2018 Wired article*



This dialogue box tells users “You control face recognition...you can turn it off at any time.” Although CR has not documented instances where a user was presented with this disclosure even though they lacked the setting, this dialogue box is another instance where Facebook represented that users can control this setting and turn off the application of facial recognition technology “at any time.”

In Facebook’s Data Policy, the company has a section entitled “How do we use this information?” Under the subsection titled “Provide, personalize and improve our Products” Facebook has a separate bullet about their facial recognition technology. In this section, Facebook includes links to their site’s privacy settings. However, the section on facial recognition technology does not mention that some users may have an older Tag Suggestions setting. In addition, the section specifically states that users can: “...control our use of this technology in Facebook settings.” This statement would lead users to believe that they have the ability to change how Facebook uses this technology, when in fact some users lack this control entirely.

*Screenshot of the section on Face Recognition in Facebook's Data Policy*

- **Face recognition:** If you have it turned on, we use face recognition technology to recognize you in photos, videos and camera experiences. The face-recognition templates we create may constitute data with special protections under the laws of your country. Learn more about how we use face recognition technology, or control our use of this technology in Facebook Settings. If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.

As documented by Consumer Reports, from at least May 1, 2019, but perhaps as early as June 2018, some consumers *did not* have access to this control. Specifically, eight out of 31, or 26 percent, of participants did not have the new Face Recognition setting, but rather the older Tag Suggestions setting, despite the fact that Facebook indicated to consumers that access to this control would be ubiquitous for adults in the United States.<sup>30</sup> Although this study only examined a small subset of Facebook users, since we could not find any clear commonalities between these users, we can infer that many more users in the US likely also lack this control. As of April 2019, Facebook has approximately 190 million users in the US,<sup>31</sup> a significant proportion of which are adults.<sup>32</sup>

#### B. Facebook's representations mislead consumers

Most consumers do not change the default settings in their accounts.<sup>33</sup> Facebook spokesperson Rochelle Nadhiri publicly stated that the Face Recognition setting “is not on by default.”<sup>34</sup> In

---

<sup>30</sup> A Facebook spokesman told Wired: “Anyone can opt out of face recognition entirely through their Facebook account settings.” (*Facebook's Face Recognition*, *supra* note 17.) However, the company did make it clear that the control was only available to individuals over the age of 18 and was not available in all countries: “Note: This setting isn't available in all countries, and will only appear in your profile if you are at least 18 years old.” (*Tagging Photos*, *supra* note 12); *see, also*: “Even in this renewed push to incorporate face recognition, people in Canada and the European Union won't have access to the features at all, because those regions have regulations about how companies can collect and store biometric data.” (*Facebook's Face Recognition*, *supra* note 17.)

<sup>31</sup> *Leading countries based on number of Facebook users as of April 2019 (in millions)*, STATISTA, <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/> (last visited May 20, 2019).

<sup>32</sup> A Pew Research Center study found: “Facebook is no longer the dominant online platform among teens...In 2018, three online platforms other than Facebook – YouTube, Instagram and Snapchat – are used by sizable majorities of this age group. Meanwhile, 51% of teens now say they use Facebook.” Monica Anderson & Jingjin Jiang, *Teens, Social Media & Technology 2018*, PEW RESEARCH CTR. (May 31, 2018), <https://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/>.

<sup>33</sup> Len V. Groeger, *Set It and Forget It: How Default Settings Rule the World*, PROPUBLICA (July 27, 2016), <https://www.propublica.org/article/set-it-and-forget-it-how-default-settings-rule-the-world>.

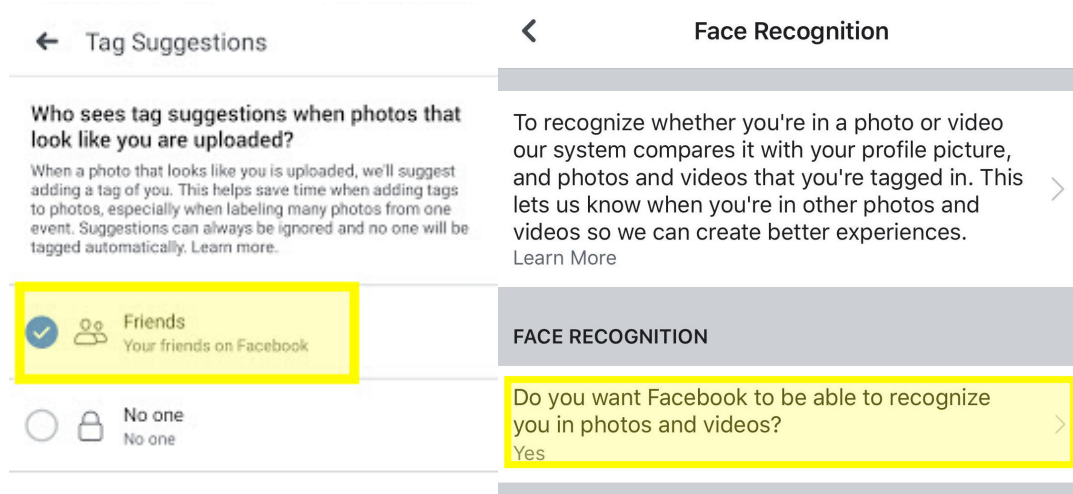
<sup>34</sup> “The new setting is not on by default,” says Facebook spokesperson Rochelle Nadhiri. True, but not so simple. “The new setting respects people's existing choices, so if you've already turned off tag suggestions then your new

addition, the same spokesman stated: "The new setting respects people's existing choices, so if you've already turned off tag suggestions then your new face recognition setting will be off by default. If your tag suggestions setting was set to 'friends' then your face recognition setting will be set to on."<sup>35</sup>

Therefore, consumers who previously changed their setting for Tag Suggestions to "off"/"no one" would reasonably assume that their Face Recognition setting was likewise set to "off"/"no." However, since some consumers lack the Face Recognition setting, their Face Recognition has not been set to off, despite Facebook's claim. Such consumers could therefore incorrectly expect that their previous actions already opted them out of Facebook's facial recognition technology collection and processing of their data when in fact they lack the tool.

However, consumers who never changed their Tag Suggestions setting from the default of "on"/"friends" would then be opted-in to new Face Recognition setting and thus the setting for this new control would be "on"/"yes." This automatic opt-in is in contradiction with the statement from Facebook spokesperson Rochelle Nadhiri who states that the setting "is not on by default."<sup>36</sup>

*If a user previously had their Tag Suggestions setting set to "Friends," then the new Face Recognition setting would be set to "Yes," in accordance with Facebook's statements*



This means that, despite the public affirmation made by Facebook spokesperson Rochelle Nadhiri that this setting "is not on by default,"<sup>37</sup> new users who never changed the default setting on their Tag Suggestions control will automatically be opted-in to allowing facial recognition processing on their photos and videos.

---

face recognition setting will be off by default. If your tag suggestions setting was set to 'friends' then your face recognition setting will be set to on," Nadhiri explains." *Facebook's Face Recognition*, *supra* note 17.

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

This misrepresentation could lead some consumers to assume, in error, that they do not need to change their settings. In addition, on all four new accounts Consumer Reports created in early May 2019, the Tag Suggestion was set to “on” by default (i.e., the setting was set to “friends” in response to the setting “Who sees tag suggestions when photos that look like you are uploaded?,” as opposed to “no one”), which implies that if the Face Recognition is rolled out to these accounts, the new setting will be set “on” by default as well.

C. Facebook’s misleading representations are material to the consumer

Finally, the gap in understanding between the privacy controls each consumer has access to on the Facebook site is material to a consumers’ choices. If a consumer knows that they lack the newer and stronger opt-out of the Face Recognition setting, the consumer might reconsider uploading personal photos or videos to the site in order to protect their privacy and the privacy of the people featured, including children. In addition, if a subset of consumers lacks a stronger opt-out that is provided to other consumers, consumers in that subset may reconsider their relationship to the social media company, especially in light of the company’s recent privacy violations and controversies.<sup>38</sup>

D. Under the precedent of *Chitika*, *InMobi*, *Nomi*, and the *Google/Safari* settlements, the Commission should investigate Facebook’s conduct

The results of our research indicate that Facebook may be misrepresenting the ability of their users to control what data is collected and processed by the company using their facial recognition technology. The misrepresentations made by Facebook can be compared to the *Chitika*, *InMobi*, *Nomi*, and *Google/Safari* settlements.

The Federal Trade Commission has brought enforcement cases against companies that misrepresent the extent to which consumers can control the collection, use, or sharing of their data in violation of the Federal Trade Commission Act. For instance, in the *Chitika, Inc.* settlement,<sup>39</sup> the Commission found that the company had violated the FTC Act by misleading users about the extent to which they could control the collection, use, or sharing of their data because the online site offered users an opt-out that served to only opt the consumer out for a period of ten days, due to a self-expiring cookie. The opt-out control offered by Chitika resulted in an opt-out cookie being placed on the user’s computer that prevented other cookies from being placed from the site. If the user navigated to view whether or not they were opted out of such tracking, the website attested that the consumer was “currently opt-ed out.” However, and unbeknownst to the user, the opt-out

---

<sup>38</sup> See Alyssa Newcomb, *A Timeline of Facebook’s Privacy Issues—and Its Responses*, NBC NEWS (Mar. 24, 2018), <https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651>.

<sup>39</sup> In the Matter of Chitika, Inc., FED. TRADE COMM’N (June 7, 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikacmpt.pdf>.

cookie was set to self-expire after ten days, thus preventing the consumer from effectively opting out.<sup>40</sup>

Likewise, in the case of *InMobi*, the FTC brought an enforcement action against the company for misrepresenting that its advertising software would only track consumers' locations when they opted in and in a manner consistent with their privacy settings. The FTC complaint alleges that the company used a database of the locations of wireless networks created from opted-in users to infer the physical locations of consumers who had opted out of sharing their location.<sup>41</sup> In order to settle this charge and others, the FTC and the company reached a settlement under which InMobi was required to pay almost a million dollars in civil penalties and implement a comprehensive privacy program.<sup>42</sup>

In addition, the FTC has found that it is unlawful under the FTC Act for a company to misrepresent the choices consumers have to control data collection by a company. Specifically, the Commission alleged in the *Nomi* case that the company misled consumers with promises that it would provide an in-store mechanism for consumers to opt out of tracking.<sup>43</sup> However, the company did not provide such controls and thus the Commission approved a final order in 2015 against Nomi for this misrepresentation and other allegations.<sup>44</sup>

In the case of the Facebook Face Recognition setting, the company similarly misrepresented to consumers that consumers are able to restrict the extent to which the company collects information about them, in possible violation of the FTC Act. Facebook has represented to their users for at least 18 months that “[a]nyone can opt out of face recognition entirely through their Facebook account settings,”<sup>45</sup> despite the fact that 26 percent of our participants cannot because they lack access to this control. These users are distributed across the US and our researchers could not find any commonalities between the users that could explain this discrepancy. Under the history of *Chitika*, *InMobi*, and *Nomi* cases, the Federal Trade Commission should bring an enforcement action against Facebook for this misrepresentation.

---

<sup>40</sup> *Id.*

<sup>41</sup> “The complaint alleges that InMobi created a database built on information collected from consumers who allowed the company access to their geolocation information, combining that data with the wireless networks they were near to document the physical location of wireless networks themselves. InMobi then would use that database to infer the physical location of consumers based on the networks they were near, even when consumers had turned off location collection on their device.” *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers’ Locations Without Permission*, FED. TRADE COMM’N (June 22, 2016), <https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked>.

<sup>42</sup> *United States v. InMobi Pte Ltd.*, No. 3:16-cv-03474, (N.D. Cal. June 22, 2016) (Stipulated Order for Permanent Injunction and Civil Penalty Judgment), *available at* <https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf>.

<sup>43</sup> *In the Matter of Nomi Technologies, Inc.*, No. C-4538, FED. TRADE COMM’N (Aug. 28, 2015), <https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter>.

<sup>44</sup> *FTC Approves Final Order in Nomi Technologies Case*, FED. TRADE COMM’N (Sept. 3, 2015), <https://www.ftc.gov/news-events/press-releases/2015/09/ftc-approves-final-order-nomi-technologies-case>.

<sup>45</sup> *Hard Questions Video*, *supra* note 14.

Facebook also made misrepresentations about the availability of their Face Recognition setting in their Help Center. Facebook's misrepresentations in their Help Center about the availability and use of the Face Recognition tool can be compared to Google's misrepresentations of Safari's settings in the 2012 settlement between the FTC and Google.<sup>46</sup> In that case, Google told Safari browser users that they would automatically be opted out of third-party cookies like Google's on their Advertising and Privacy page, which was located in the consumer help/frequently-asked-questions center.<sup>47</sup> Similarly, in Facebook's Help Center, the site tells users how to "turn face recognition on or off for my account." However, for the users that do not have access to this control, these explainers misrepresent what settings they have for they lack access to the Face Recognition control entirely. In addition, the links in the Help Center on this setting fail to navigate users who lack the Face Recognition control to settings that they can use to modify what information Facebook can collect about them. The links instead take users without this setting to the main account settings page, leaving it up to the user to figure out that they lack this control.

### III. Facebook's practices violate the 2011 Consent Agreement

The misrepresentations documented in this letter are also possible violations of the *Consent Agreement* reached by Facebook and the Federal Trade Commission in 2011. Under the *Agreement*, Facebook:

...shall not misrepresent 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:

- C. Its collection or disclosure of any covered information;
- D. The extent to which a consumer can control the privacy of any covered information maintained by [Facebook] and the steps a consumer must take to implement such controls;<sup>48</sup>

Under the terms of this *Consent Agreement*, photos or videos are included within the definition of "covered information."<sup>49</sup> Since Facebook made misrepresentations of the extent to which a consumer could control the privacy of their photos and videos under the privacy settings provided by Facebook, the instances reported in this letter are covered by said *Agreement*.<sup>50</sup> Therefore, the Commission should explore whether or not to bring an enforcement action against Facebook due to this violation of the 2011 *Consent Agreement*.

---

<sup>46</sup> *Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>.

<sup>47</sup> *United States v. Google, Inc.*, No. 12-04177 (N.D. Cal. Aug. 8, 2012) (Complaint for Civil Penalties and Other Relief), p. 8, <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf>.

<sup>48</sup> 2011 Consent Agreement, *supra* note 5.

<sup>49</sup> 2011 Consent Agreement, *supra* note 5.

<sup>50</sup> The agreement extends until 2032. *See* 2011 Consent Agreement, *supra* note 3.

#### IV. Conclusion and Request for Relief

Facebook misrepresented the extent to which their users can control the amount of information that is collected and processed about them under the company's facial recognition technology, in violation of the Federal Trade Commission Act<sup>51</sup> and the 2011 *Consent Agreement*.<sup>52</sup> The public statements made and Help Center resources provided by Facebook could mislead consumers to believe that they have certain privacy protections when they in fact lack those protections. Our research with 31 of Facebook users demonstrates that this new setting has not been deployed to all users. Therefore, many users of this site could be misled to think they have this control when in fact they do not, leading them to a false sense of control and privacy of their data. Furthermore, since the links in the Help Center page and in the Facebook Newsroom announcement fail to navigate to the correct setting for those individuals who lack the new Face Recognition setting, consumers could be additionally confused and unable, without extra effort, to find out they do not have this new setting.

Finally, Facebook also deceived their users by representing that the new Face Recognition setting would be set to "off"/"no" by default or would align with the user's past expressed preferences with regards to facial recognition as indicated by whether they changed their default Tag Suggestions setting (i.e., by changing the setting from "Friends" to "No one," thus opting out of this narrow control on facial recognition technology). But in fact, most users never change their default settings, so many users likely were opted-in to Facebook's facial recognition processing of their photos due to the default setting of the older Tag Suggestions feature (which was on by default). Additionally, we found that new accounts are often given the older Tag Suggestions feature initially (which is on by default) and thus these accounts, when they do receive the newer Face Recognition control, will be opted into facial recognition processing of their photos.

These misrepresentations by Facebook potentially constitute violations of the FTC Act and the 2011 *Consent Order*. We therefore urge the FTC to investigate these practices.

Respectfully submitted,

/s/ Katie McInnis

Katie McInnis

Policy Counsel

Consumer Reports

Suite 500

1101 17th Street NW

Washington, DC 20036

(202) 462-6262

---

<sup>51</sup> 15 U.S.C. § 45(a)(1).

<sup>52</sup> *Facebook Settles*, *supra* note 3.