Before the
FEDERAL TRADE COMMISSION
Washington, DC

In the Matter of	)
	)
Facebook, Inc. and	)
Facial Recognition	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center, The Campaign for a Commercial Free Childhood, The Center for Digital Democracy, The Constitutional Alliance, Consumer Action, The Consumer Federation of America, Consumer Watchdog, The Cyber Privacy Project, Defending Rights & Dissent, The Government Accountability Project, The Privacy Rights Clearinghouse, Patient Privacy Rights, The Southern Poverty Law Center, and The U.S. Public Interest Research Group

I. Introduction

1. This complaint concerns recent changes in Facebook's business practices that threaten user privacy and violate the 2011 Consent Order with the Federal Trade Commission. As set forth in detail below, Facebook now routinely scans photos for biometric facial matches without the consent of the image subject. Moreover, the company seeks to advance its facial recognition techniques by deceptively enlisting Facebook users in the process of assigning identity to photo images. This unwanted, unnecessary, and dangerous identification of individuals undermines user privacy, ignores the explicit preferences of Facebook users, and is contrary to law in several states and many parts of the world. The Commission must undertake an investigation, enjoin these unlawful practices, establish sanctions, and provide appropriate remedies.

2. The 2011 Consent Order is clear: Part I of the proposed order prohibited Facebook from misrepresenting the privacy or security of "covered information."[1] According to the proposed order, "'Covered information' is defined broadly as 'information from or about an individual consumer, including but not limited to: . . . (e) photos and videos. . .'"[2] Part II of the proposed order required Facebook to "give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds

[1] Federal Trade Commission, *Facebook, Inc.; Analysis of Proposed Consent Order To Aid Public Comment*, 76 Fed. Reg. 75883 (Dec. 5, 2011), https://www.ftc.gov/sites/default/files/documents/federal_register_notices/facebook-inc.analysis-proposed-consent-order-aid-public-comment-proposed-consent-agreement/111205facebookfrn.pdf.
[2] *Id.* (emphasis added).

the restrictions imposed by their privacy settings."[3] Part IV "requires Facebook to establish and 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, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook's size and complexity, the nature and scope of its activities, and the sensitivity of covered information."[4]

3. Facebook violated the 2011 Consent Order in multiple ways. Facebook's changes to its facial recognition practices exposed users' covered information in a way that materially exceeded the restrictions imposed by their privacy settings. Moreover, Facebook did not provide users with clear and prominent notice nor obtain their affirmative express consent before enacting these changes. Facebook also misrepresented the privacy and security of covered information. Finally, Facebook failed to establish and maintain a comprehensive privacy program to address the privacy risks of new and existing products and to protect the privacy and confidentiality of covered information.

II. The Parties

4. 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. The 2011 FTC Consent Order arises from a series of complaints filed by EPIC from 2009 to 2011 concerning material changes to privacy settings made by Facebook. EPIC has continued to advocate for the Commission's enforcement of consent decrees to ensure that companies adhere to their obligations to consumer privacy.

5. The Campaign for a Commercial Free Childhood ("CCFC") is a national advocacy organization dedicated to countering the harmful effects of commercialism on children. CCFC organizes campaigns against corporations that target children with harmful marketing, helps parents and professionals reduce the amount of time kids spend with ad-supported screens, and advocates for policies that limit marketers' access to children.

6. The Center for Digital Democracy ("CDD") is a not-for-profit D.C.-based organization focused on protecting consumers in the digital marketplace.[5] During the 1990's (and then operating as the Center for Media Education) its work to protect privacy on the Internet led to the passage of the Children's Online Protection Act (COPPA) by Congress in 1998.[6] CDD's advocacy on the Google-Doubleclick merger played a major role in the FTC's decision to address privacy concerns arising from

[3] *Id.* (emphasis added).
[4] *Id*. (emphasis added).
[5] Ctr. for Digital Democracy, *About CDD*, http://www.democraticmedia.org/about-cdd.
[6] Katherine C. Montgomery, *Generation Digital*, MIT Press, http://mitpress.mit.edu/books/generation-digital.

online behavioral advertising.[7] Through a series of complaints filed at the commission, CDD has brought attention to privacy concerns with mobile devices, real-time tracking and targeting platforms, social media, and from the databroker industry. CDD's four-year campaign to ensure that COPPA was effectively implemented across all major platforms and applications resulted in the FTC's December 2012 decision to strengthen its rules on children's privacy.

7. The Constitutional Alliance is the only national organization in the United States that specifically focuses on the issue of the use of biometrics, including but not limited to Facial Recognition Technology (FRT). We work with state lawmakers and Congress to educate our elected representatives on the risk to a free society, when FRT is used by government and corporations. The Constitutional Alliance opposes the use of biometrics by any company absent informed consent, which includes a customer/user must need to opt-in before their biometrics can be used. Further, the biometrics of an individual must not be able to be shared with other companies and/or entities without the knowledge and consent of the customer/user.

8. Consumer Action has been a champion of underrepresented consumers nationwide since 1971. A non-profit 501(c)(3) organization, Consumer Action focuses on consumer education that empowers low- and moderate-income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers to advance consumer rights and promote industry-wide change.

9. The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

10. Consumer Watchdog is a nonprofit, nonpartisan, public interest corporation organized to represent the interests of consumers and taxpayers. A core focus of Consumer Watchdog's Privacy and Technology Project is protecting people's online privacy and enabling them to have control over data about them.

11. The Cyber Privacy Project (CPP) addresses issues about privacy raised in a networked world. In upholding the belief that privacy is essential to democratic society, Cyber Privacy Project anchors its approach in realizing the beneficial potential of the Constitution, laws, and policies of the U.S. CPP calls for implementation of privacy protections based on First Amendment rights of privacy and anonymity, Fourth Amendment rights against unreasonable searches and seizures, the Fifth and Fourteenth Amendment rights to due process and protection of liberty, and Article IV Privileges and Immunities to Travel and Work. It also calls upon similar principles in international human rights documents, state constitutions, and codes of ethics. CPP particularly questions the proliferation of digital

[7] Louise Story, *F.T.C. Approves Doubleclick Deal*, N.Y. Times, Dec. 21, 2007, at C3, http://www.nytimes.com/2007/12/21/business/21adco.html.

photography requirements, interoperability and recognition as magnifying privacy violations.

12. Defending Rights & Dissent ("DRAD") is a not-for-profit public education and advocacy organization based in Washington, DC. The mission of the organization is to strengthen participatory democracy by protecting the right to political expression. The ability to safeguard one's privacy is recognized as an important factor in protecting free speech and expression. Given the role of Facebook as a modern-day town square where matters of public concern are debated, DRAD is concerned that continued violations of user's privacy by Facebook adversely impact the rights of Facebook users to freely engage in political expression.

13. The Government Accountability Project ("GAP") is a non-profit, non-partisan public interest organization that promotes government and corporate accountability by litigating whistleblower cases, publicizing whistleblowers' concerns, and developing legal reforms to support the rights of employees to use speech rights to challenge abuses of power that betray the public trust. GAP, as an organization committed to protecting the public from the effects of an unaccountable institutions—illegality, corruption, abuses of authority, and dangers to fundamental public interests—joins this Complaint.

14. Patient Privacy Rights (PPR) was founded in 2004 by Deborah C. Peel, MD. Our mission is to honor and empower the individual's right to privacy through personal control of health information wherever such information is collected and used. Patient Privacy Rights educates, collaborates and partners with people to ensure privacy in law, policy, technology, and maximize the benefits from the use of personal health information with consent. PPR is recognized as the world's most prominent human and civil rights organization dedicated to restoring health privacy. PPR projects include leading a bipartisan coalition of 50+ organizations representing 10.3M people who want to control personal health data. The coalition successfully pressed for tough new penalties for data breaches and new privacy protections in HITECH and other federal regulations.

15. The Privacy Rights Clearinghouse (PRC) is a 501(c)(3) nonprofit consumer education and advocacy organization, located in San Diego, California. Established in 1992, PRC's mission is to engage, educate, and empower consumers to protect their privacy. PRC publishes extensive consumer education resources, provides one-to-one assistance, and advocates for strong privacy protections.

16. The Southern Poverty Law Center (SPLC) is a not-for-profit organization that uses litigation, education, and other forms of advocacy to fight hate, discrimination, and other forms of unfairness. In 2017, it launched a digital literacy campaign to provide tools and lesson plans to help educators teach their students about, among other things, the impact of online activity on their personal privacy and about how companies mine social media data. The SPLC is also concerned about the possible misuse of social media data for law enforcement purposes.

17. U.S. Public Interest Research Group serves as the national federation of state PIRGs, which are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members. U.S. PIRG has long advocated at the state and national level for greater consumer control of their information, greater data security and greater accountability for data collectors. U.S. PIRG has filed, or co-filed, numerous petitions and complaints to the FTC on issues including data brokers, the Internet ecosystem and the general sharing, selling and scoring of personal information.

III. The Privacy Risks of Facial Recognition

18. Facial recognition systems include computer-based biometric techniques that detect and identify human faces.[8]

19. The National Academy of Sciences has stated:

> 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.[9]

20. There is significant controversy surrounding the use of facial recognition technology. Private companies covertly deploy facial recognition techniques to obtain the identity of unsuspecting individuals. For example, Madison Square Garden deploys facial recognition on attendees at public sporting events:[10]

> The technology uses cameras to capture images of people, and then an algorithm compares the images to a database of photographs to help identify the person and, when used for security purposes, to determine if the person is considered a problem. The technology, which is sometimes used for marketing and promotions, has raised concerns over personal privacy and the security of any data that is stored by the system.

21. Commercial deployment of facial recognition is also pervasive in the advertising industry. For example, Unilever has utilized facial scanning to measure shoppers' emotional engagement with on-shelf displays.[11]

---

[8] EPIC, *Facial 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.

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

[10] Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times, Mar. 13, 2018, at B8, https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.

[11] Michael Barnett, *Unilever trials in-store facial recognition technology*, Marketing Week, (Mar. 7, 2018), https://www.marketingweek.com/2018/03/07/unilever-in-store-facial-recognition/.

22. EPIC's Jeramie Scott has explained the privacy and surveillance issues of commercial deployment of facial recognition:[12]

> As large institutions begin using facial recognition on the public, it normalizes a privacy-invasive technology that lacks meaningful safeguards. The lack of regulation of facial recognition and other biometric surveillance methods means the data collected and used now for one purpose can easily be utilized for purposes not even imagined yet and without the consent from the targets of the technology. Each instant where mass surveillance is implemented, especially where little to no regulation exists like it does with facial recognition, takes us one step closer to ubiquitous surveillance and one step farther from the liberties we are supposed to hold dear.

23. The use of facial recognition technology by governments also raise significant privacy concerns.

24. The United States Custom and Border Protection ("CBP"), Department of Homeland Security ("DHS"), and the Federal Bureau of Investigation ("FBI") coordinate various programs on facial recognition technology that raise substantial privacy and civil liberties concerns.

25. Facial recognition technology can be done covertly, even remotely, and on a mass scale. There is little that individuals can do to prevent collection of one's image. Participation in society involves exposing one's face. Ubiquitous and near effortless identification eliminates individuals' ability to control their identities and poses a special risk to the First Amendment rights of free association and free expression, particularly to those who engage in lawful protests.

26. Governments around the world seek access to images of political organizers to obtain actual identities and to enable investigation and prosecution.

27. In Canada, police coordinated with the Canadian Bankers Association to deploy facial recognition software to identify protestors at the 2010 G20 summit in Toronto.[13]

28. In Iran, government agents have posted pictures of political activists online and used "crowd-sourcing" to identify individuals.[14] There is also evidence that Iranian

---

[12] Dave Zirin and Andrew Tan-Delli Cicchi, *Fans Are the Target of Madison Square Garden's New Facial-Recognition Technology: Facial recognition is a threat to privacy and the latest frontier in surveillance, The Nation* (Mar. 23, 2018),, https://www.thenation.com/article/fans-are-the-target-of-madison-square-gardens-new-facial-recognition-technology/.

[13] Ashley Csanady, *Police using facial recognition software to help ID G20 suspects*, National Post, (Jul. 15, 2010), http://nationalpost.com/posted-toronto/police-using-facial-recognition-software-to-help-id-g20-suspects.

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

researchers are working on developing and improving facial recognition technology to identify political dissidents.[15]

29. 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."[16]

30. Following earlier efforts by consumer privacy organizations, the FTC acknowledged the privacy concerns raised by the commercial use of facial recognition:

> [T]he use of facial recognition technologies can raise privacy concerns. For example, panelists voiced concerns that databases of photos or biometric data may be susceptible to breaches and hacking. Further, panelists discussed how some consumers may perceive digital signs equipped with cameras using facial recognition technologies as invading their privacy because they can detect consumers from a distance and process their images without their knowledge or consent."
>
> Perhaps of most concern, panelists surmised that advances in facial recognition technologies may end the ability of individuals to remain anonymous in public places. For example, a mobile app that could, in real-time, identify anonymous individuals on the street or in a bar could cause serious privacy and physical safety concerns, although such an app might have benefits for some consumers. Further, companies could match images collected by digital signs with other information to identify customers by name and target highly-personalized ads to them based on past purchases, or other personal information available about them online. Social networks could identify non-users of the site – including children – to existing users, by comparing uploaded images against a database of identified photos.[17]

31. EPIC has previously advised the Commission that, "[c]entral to the meaningful safeguards to face recognition technology are (1) subject control over image enrollment, (2) subject control over the processing and identification of images, (3)

---

[15] 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) http://dehshibi.com/files/papers/Iranian%20Face%20Database%20and%20Evaluation%20with%20a%20new%20detection.pdf.

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

[17] Fed. Trade Comm'n, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

transparency in the functioning, use, and purpose of the facial recognition system, and (4) independent accountability of the image processing entity.[18]

32. Facebook has failed to adopt one or more of these safeguards in violation of the 2011 FTC Consent Order.

IV. Facebook's Deployment of Facial Recognition Techniques

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

33. Facebook is the largest social network service provider in the United States. There are over 2.13 billion monthly active Facebook users worldwide, of whom 214 million are American.[19]

34. Approximately 350 million photos are uploaded every day, with 14.58 million photo uploads per hour.[20]

B. Facebook's Early Development of Facial Recognition Technology Was Dependent on Collecting Biometric Data on Users Without Knowledge or Consent

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

36. Facebook collects facial recognition data through a deceptive practice: it suggests a tag identifying a user, for the user to confirm by approving the suggestion. Facebook routinely encourages users to "tag," others, i.e. provide actual identifying information about themselves, their friends, and other people they may recognize. Facebook does not explain that this practice enables the company to identify images in other contexts.

37. Facebook associates the tags with a user's account, compares what these tagged photos have in common and stores a summary of this comparison.

38. Facebook compares uploaded photos "to the summary information we've stored about what your tagged photos have in common."

39. Facebook's Help Center describes this technology as "[analyzing] the pixels in photos and videos, such as your profile picture and photos and videos that you've been tagged in, to calculate a unique number, which we call a template. We compare other

---

[18] EPIC, *In the Matter of Facebook, Inc. and the Facial Identification of Users (EPIC Complaint, Request for Investigation, Injunction, and Other Relief*) (Jun. 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.

[19] *See,* Zephoria Digital Marketing, *The Top 20 Valuable Facebook Statistics – Updated March 2018,* https://zephoria.com/top-15-valuable-facebook-statistics/.

[20] *Id.*

photos and videos on Facebook to this template and if we find a match we'll recognize you."[21]

40. The Tag Suggestions technology identifies users in photos without their consent. However, Facebook gave no clear and conspicuous notice to users and failed to obtain meaningful express consent prior to collecting "Photo Comparison Data," generating unique biometric identifiers, and linking biometric identifiers with individual users.

41. Facebook's subsequent facial recognition technique ("2018 Facial Recognition Practice") notifies users when their biometric face print is detected on an image, even if it has not been tagged by another user.

42. The 2018 Facial Recognition Practice derives biometric data from Facebook users in a materially different manner than Facebook represented when they first collected the data using Tag Suggestions.

C. Facebook Never Obtained Affirmative Express Consent for Any Use of Facial Recognition Technology and Continues to Benefit from its Privacy Misrepresentations

43. Facebook never obtained "affirmative express consent" for its deployment of facial recognition, as required by Part II of the 2011 Consent Order. The Commission's analysis of the Order makes clear that Facebook must "give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings."[22]

44. Since 2010, Facebook deployed extensive facial recognition practices on an opt-out basis without providing clear and conspicuous notice, without obtaining users' affirmative express consent, and without effectively guiding users on how to opt-out of the default Tag Suggestions setting.

45. In 2013, Facebook abruptly lifted its brief suspension of the Tag Suggestions program despite significant backlash, and automatically reinstated it for every user in the United States.

46. A review of the company's approach to facial recognition from 2010 to 2018 clearly invalidates any claim of implied or continuing consent that could justify the implementation of the 2018 Practice without renewed and affirmative consent.

i. No User Consent Obtained for Tag Suggestions in 2010-2011

47. In 2010, Facebook announced face detection technology for photos:

[21] Facebook, Help Center, *How does Facebook's face recognition work?*, https://www.facebook.com/help/218540514842030.
[22] Facebook, Inc., Proposed Consent Order (emphasis added).

> 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.[23]

48. Facebook subsequently announced in 2010 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.[24]

49. 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.[25]

50. In 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

[23] Sam Odio, *Making Photos Better*, Facebook Blog (Jul. 1, 2010), http://blog.facebook.com/blog.php?post=403838582130.
[24] Sam Odio, *More Beautiful Photos*, Facebook Blog (Sept. 30, 2010), http://blog.facebook.com/blog.php?post=432670242130.
[25] Caroline McCarthy, *Facebook Photos Get High Resolution, Bulk Tagging*, CNET (Sept.30, 2010), https://www.cnet.com/news/facebook-photos-get-high-resolution-bulk-tagging/.

> 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.[26]

51. Facebook later announced that it had deployed "Tag Suggestions" technology over the last several months, and that the technology had been available internationally. Facebook did not provide users with any other notice about this facial recognition technology.[27]

52. Facebook admitted in a later statement, that "we should have been more clear during the roll-out process when this became available to them."[28] (At the date of this complaint, the blog post apologizing for user confusion in the roll-out process of Tag Suggestions has been removed from Facebook Newsroom.)

53. However, in each subsequent deployment of facial recognition techniques for the ensuing eight years, Facebook has made no effort to rectify that matter or to allow users to opt-in if they so choose.

54. Facebook's automated identification of facial images continues to occur in the absence of any user intervention.

55. Facebook enables Tag Suggestions by default; users may opt-out if they are aware of the default setting, but do not affirmatively opt-in to Tag Suggestions or subsequent facial recognition techniques.

ii. Post-FTC Consent Decree, 2013: Facebook Automatically Reinstated Tag Suggestions without User Consent

56. In 2012, Facebook was questioned by the Senate Judiciary Subcommittee on facial recognition technology.[29] In response to a question on why the platform does not implement an opt-in choice for users rather than turning on Tag Suggestions by default, Facebook Privacy and Policy manager Rob Sherman answered:[30]

> Facebook itself is an opt-in experience. People choose to be on Facebook because they want to share with each other. We think that it's the right choice to let people who are uncomfortable with it to decide to opt out.

---

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

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

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

[29] Ricardo Bilton, *Facebook hit with tough questions on facial recognition in Senate hearing* (July 18, 2012), Venture Beat, https://venturebeat.com/2012/07/18/facebook-hit-with-tough-questions-on-facial-recognition-in-senate-hearing/.

[30] *Id*.

57. This response was heavily scrutinized by Senator Blumenthal and Senator Franken for deflecting the question on Facebook's lack of informed choice mechanisms that enable users to fully understand their enrollment in facial recognition, the privacy implications of the technology, and to easily withdraw from tag suggestions.[31]

58. The Office of the Data Protection Commissioner, Ireland published a comprehensive assessment of Facebook's data practices as part of an audit to investigate Facebook's compliance with European privacy laws.[32] As a result of scrutiny from European data protection regulators, Facebook discontinued facial recognition by automatic photo tagging in Europe.[33]

59. In late 2012, Facebook temporarily suspended Tag Suggestions in the United States after significant public backlash by consumer privacy groups. In a press release, Facebook claimed that it will "make improvements to the tool's efficiency" without specifying when or how Tag Suggestions will be re-engineered to address salient user privacy concerns.

60. In 2013, Facebook automatically reinstated Tag Suggestions for users in the United States without any additional safeguards to address consumer privacy concerns. Tag Suggestions were enabled by default for every user in America.[34]

[31] T.C. Sottek, *Senator Al Franken grills FBI, Facebook, and others on facial recognition technology*, The Verge, July 18, 2012, https://www.theverge.com/2012/7/18/3167864/senator-al-franken-fbi-facebook-facial-recognition-hearing.

[32] Data Protection Commissioner, *Report of Review of Facebook Ireland's Implementation of Audit Recommendations Published – Facebook turns off Tag Suggest in the EU*, https://www.dataprotection.ie/docs/21-09-12-Press-Release--Facebook-Ireland-Audit-Review-Report/1233.htm; *see also,* EPIC, *EPIC Recommends Safeguards For Facial Recognition Technology,* https://epic.org/2014/02/epic-recommends-safeguards-for.html.

[33] Somini Sengupta and Kevin O'Brien, *Facebook Can ID Faces, but Using Them Grows Tricky* N.Y. Times, Sept. 21, 2012, at A1, https://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html.

[34] Emil Protalinski, *Facebook re-enables Tag Suggestions facial-recognition feature in the US, on by default for all* The Next Web, Feb. 1, 2013, https://thenextweb.com/facebook/2013/02/01/facebook-re-enables-tag-suggestions-facial-recognition-feature-in-the-us-on-by-default-for-all/; Paul Ducklin, *Facebook is turning facial recognition back on – so here's how to check your "photo tagging" settings* Naked Security, Feb. 2, 2013, https://nakedsecurity.sophos.com/2013/02/02/facebook-turns-facial-recognition-back-on/.

61. On the "Facebook and Privacy" page, Facebook admitted that the reinstated Tag Suggestions was the "same feature that millions of people previously used to help them quickly share billions of photos with friends and family." Facebook did not explicitly clarify that Tag Suggestions remained opt-out for users or explain the privacy implications of the default setting.

62. The hyperlink to "learn more about tag suggestions and how to control them" did not direct the user to a clear and conspicuous opt-out setting. An archive of the page on February 1, 2013 shows that the hyperlink led to Facebook's Help Center with a list of FAQs on "Tagging Photos." The term "facial recognition" was not used at all.

63. Users had to scroll down to the end of the page to locate "How can I turn off tag suggestions for photos of me?" Clicking on this link still did not direct the user to a clear and conspicuous opt-out setting. Instead, the page set out a 4-step instruction on how to navigate the user's privacy settings to exercise opt-out.

64. Facebook actively discouraged users from opting out with a disclaimer that read:

> Before you opt out of using this feature, we encourage you to consider how tag suggestions benefit you and your friends. Our tagging tools (including grouping photos that look similar and suggesting friends who might be in them) are meant to make it easier for you to share your memories and experiences with your friends.

> Before you opt out of using this feature, we encourage you to consider how tag suggestions benefit you and your friends. Our tagging tools (including grouping photos that look similar and suggesting friends who might be in them) are meant to make it easier for you to share your memories and experiences with your friends.

65. Facebook never obtained affirmative express consent to reinstate Tag Suggestions in 2013, and it actively convoluted the process of opting-out to discourage users from disabling facial recognition settings.

66. Facebook's claim to "respect users' existing privacy settings" in rolling out the 2018 Facial Recognition Practice is misleading and deceptive, and also constitutes a violation of the FTC Consent Decree.

iii. Post-FTC Consent Decree, 2014: Facebook Developed DeepFace Facial Recognition Technology from Analyzing User Photos

67. In 2014, Facebook and its subsidiary Face.com published a research paper on DeepFace.[35] Facebook presented DeepFace at the IEEE Conference on Computer Vision and Pattern Recognition in June 2014.

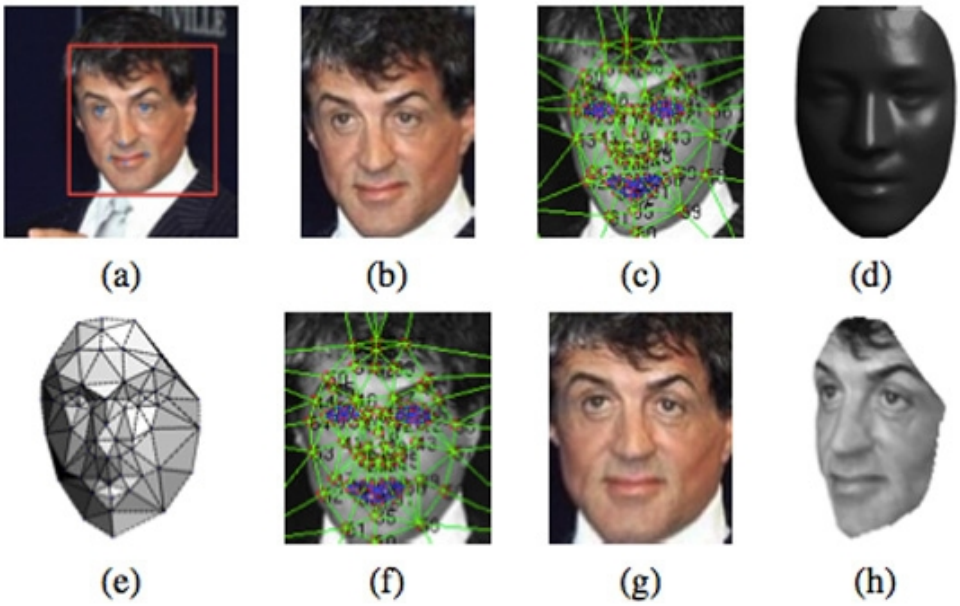
68. At present, the post on https://research.fb.com/, entitled "Closing the Gap to Human Level Performance in Face Verification" has been deleted from Facebook.[36]

69. DeepFace is an artificial intelligence system that trained on 4 million photos "from a popular social network" to match different images of the same person using their biometric face print. The research claimed an accuracy rate of 97.25 percent, even when the images presented contextual differences in angle, lighting, and facial expressions.[37]

[35] Tom Simonite, *Facebook Creates Software That Matches Faces Almost as Well as You Do* MIT Tech. Rev., (Mar. 17, 2014), https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.

[36] "404 Page Not Found. It looks like nothing was found at this location,", https://research.fb.com/search?q=%22DeepFace%3A+Closing+the+Gap+to+Human-Level+Performance+in+Face+Verification%22.

[37] Will Oremus, *Facebook's New Face-Recognition Software Is Scary Good*, Slate, Mar. 18, 2014, http://www.slate.com/blogs/future_tense/2014/03/18/deepface_facebook_face_recognition_software_is_97_percent_accurate.html.



70. Facebook's unprecedented access to extensive biometric data on users enabled its facial recognition capacity to surpass the accuracy of systems deployed by law enforcement and the FBI in 2014.[38]

71. Facebook spokeswoman Lydia Chan claimed in 2014 that, "this is theoretical research, and we don't currently use the techniques discussed in the paper on Facebook."[39]

72. However, the research relied on Facebook's user data to expand the neural network of the machine learning system to increase DeepFace's facial recognition capabilities.

73. The 2018 Facial Recognition Practice, which scans for a user's biometric face print on any photo uploaded to Facebook—viewable by that user with or without tags—demonstrates that Facebook is indeed commercially deploying its facial recognition technology beyond research purposes and outside the scope of what is permitted under the 2011 Consent Decree.

[38] Russell Brandom, *Why Facebook is beating the FBI at facial recognition*, The Verge, July 7, 2014, https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.
[39] Will Oremus, *supra*; *see also,* James O'Toole, *Facebook's new face recognition knows you from the side*, CNN Tech, Apr. 4, 2014, http://money.cnn.com/2014/04/04/technology/innovation/facebook-facial-recognition/index.html.

iv. Post-FTC Consent Decree, 2017-2018: Facebook Has Deployed Additional Facial Recognition Technology In Violation of State Biometric Information Privacy Laws

74. Facebook currently faces a class action lawsuit alleging that it violated the Illinois Biometric Information Privacy Act (BIPA) when it implemented the Tag Suggestions technology to extract biometric data without obtaining affirmative consent. [40]

75. The United States District Court for the Northern District of California denied Facebook's motion to dismiss for lack of standing, explaining, "Facebook insists that the collection of biometric information without notice or consent can never support Article III standing without 'real-world harms' such as adverse employment impacts or even just 'anxiety.' That contention exceeds the law." [41]

76. Despite the court's ruling, Facebook continues to disregard not only its obligation under the FTC Consent Order but the laws of several states, including Illinois, Texas and Washington.[42]

77. Facebook has continued to misrepresent its collection, use and disclosure of biometric data knowing that state laws prohibit the use of facial recognition without affirmative, express opt-in consent.

D. No Affirmative Consent Sought in 2017-2018 to Materially Change the Use of Facial Templates and to Gain More Rights to Collect Biometric Data

i. Discloses Non-Public Information in a Matter That Materially Exceeds Current Privacy Settings

78. The 2011 FTC Consent Order defines nonpublic user information as "covered information that is restricted by one or more privacy settings."

79. Facebook's updated setting notifies users to "find" photos that they are in but have not been tagged, as long as the photo's privacy settings allow the user to view it as a Friend, Public, or Custom Audience.

80. For example: User A posts a picture and applies the privacy setting of "Friends Only" and does not tag anyone; although this is non-public information under the 2012 Consent Order, User B, who is a friend of User A but has not been invited to share the content via a tag, will be notified of a facial recognition match.

81. Facebook has implemented changes to the facial recognition technology that materially exceeds users' current privacy settings. As detailed below, this constitutes several violations of the 2011 FTC Consent Order due to Facebook's insufficient

[40] *In re Facebook Biometric Information Privacy Litig*., No 3:15-CV-03747-JD, *Order Re Renewed Mot. to Dismiss*, Dkt. No. 227 at 1, 5-7 (N.D. Cal Feb. 26, 2018).
[41] *Id*.
[42] *See,* Tex Bus & Com § 503.001; Wash. Rev. Code Ann. § 40.26.020 (2017).

notice to users on the privacy implications of additional facial recognition and its failure to obtain affirmative express consent.

ii. Consent Decree Violations by Misrepresentation and Failure to Obtain Affirmative Express Consent

82. Part II(B) of the 2011 FTC Consent Order requires Facebook to "obtain the user's affirmative express consent" prior to disclosing a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy settings.[43]

83. Part I(A)-(B) of the 2011 FTC Consent Order prohibits Facebook from misrepresenting "in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:[44]

> 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 Respondent and the steps a consumer must take to implement such controls.

84. According to a report by WIRED, Facebook spokesperson Rochelle Nadhiri stated that "the new setting is not on by default." Nadhiri said, "[t]he 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."[45]

85. This representation is misleading to consumers. Functionally, Facebook's 2018 changes to facial recognition automatically applied to a majority of users who were enrolled into Tag Suggestions by default in 2013.

86. Tag Suggestions dates back five years. Many users remain unaware that Tag Suggestions applied to them by default in 2013, and that there is a choice to opt-out. Therefore, Facebook's reliance on this prior setting to infer consent for invasive changes to biometric data practices gives Facebook unprecedented control over facial templates without affirmative express consent.

87. Facebook's recent notice to users on the changes to the extent of facial recognition does not "conspicuously" present an opt-out button, but merely links a "Go to Settings" button.

---

[43] Fed Trade Comm'n, *In re Facebook*, Decision and Order, FTC File No. 092-3184 (Jul. 27, 2012) (Hereinafter "Facebook Consent Order").
[44] *Id*.
[45] 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/.

88. This lack of clear and conspicuous notice violates Part I(A)-(B) of the Consent Order by misrepresenting "the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls." Specifically, Facebook misrepresents the extent to which users can control the privacy of biometric information, and the extent of Facebook's collection and disclosure of the facial templates and photo comparison data to third parties.

89. Facebook violated Part II(B) of the Consent Order by failing to obtain affirmative express consent before implementing business changes to facial recognition techniques. Any claims of inferred or continuing consent from the user's prior setting on Tag Suggestions is invalid, as Facebook has never given users a choice to opt-in to facial recognition.

E. Users Were Not Clearly and Prominently Notified of Facebook's Changes to Facial Recognition Practices

90. Part II(A) of the 2012 FTC Consent Order requires Facebook to:

> Clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user…prior to any sharing of a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy settings.

91. The Consent Order defines "clear and prominent" to mean:

> A. In textual communications (e.g., words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
>
> C. In communications disseminated through video means… the required disclosures shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them
>
> D. In all instances, the required disclosures: (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

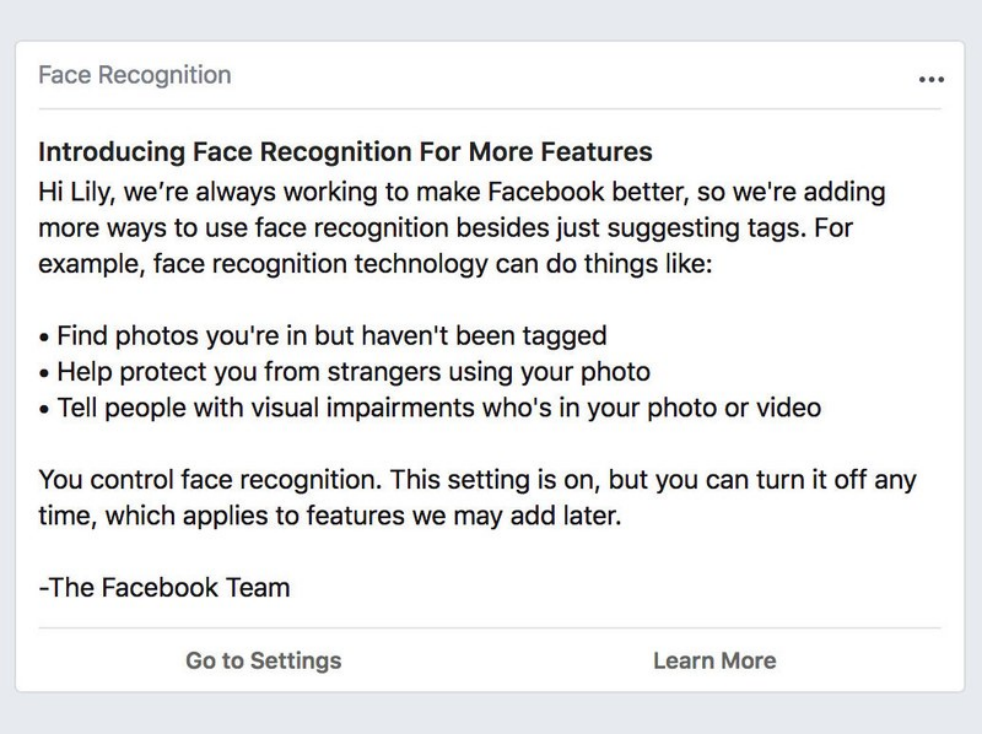
92. Facebook violated this provision and failed to meet the standards of a "clear and prominent" notice for the reasons detailed below.

i. Facebook's Announcement was Difficult to Locate and Notice

93. From December 2017 to early 2018, Facebook posted a short notice regarding its revised facial recognition practice through a disclaimer that appeared on users' news feeds.

94. The FTC requires truthful disclaimers to be displayed clearly and conspicuously, but Facebook's notice was buried in the densely packed text of users' news feeds.[46]

95. The brief post appeared at the top of users' news feeds, but did not make clear that Facebook had in fact changed users' privacy settings.



96. Facebook did not ensure that the notice appeared on screen for a duration sufficient for an ordinary consumer to notice, read, and comprehend. Users could easily scroll down on their mobile or computer device and miss out on the notice.

97. If the user continued to scroll down without having read the announcement, it was difficult to re-locate the disclaimer and the "Learn More" hyperlink to Facebook's press release on the implications of facial recognition technology.

98. Moreover, the buried notice on the news feed actually disappeared if a user refreshed the page.

[46] Fed. Trade Comm'n, *.com Disclosures*, (Mar. 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

99. As the change "rolled-out" to Facebook users gradually, users received notice at different times. The impact of Facebook's announcement on December 19, 2017 dissipated when some users were being notified in early January 2018, while others were not aware until mid-March 2018.

ii. Privacy Misrepresentations and Vagueness in the Announcements

100. Facebook's announcements of the change in facial recognition practice include significant misrepresentations and omissions, contrary to the requirements of the Consent Order.

101. On December 19, 2017, Facebook's Deputy Chief Privacy Officer Rob Sherman posted a blog post, entitled "Hard Questions: Should I Be Afraid of Face Recognition Technology?"[47]

102. On the potential risks of facial recognition technology, Sherman wrote:

> This tension isn't new. Society often welcomes the benefit of a new innovation while struggling to harness its potential. "Beware the Kodak," one newspaper intoned in 1888 as inexpensive equipment came onto the market making photography available to the masses. They called it a "new terror for the picnic." Confronting amateur photography for the first time, society could have restricted this technology – and fundamentally changed the way history was documented for more than a century.

103. The statement misleadingly equates highly sophisticated AI techniques, which can extract the exact biometric dimensions of a face, with the early development of film photography.

104. Facebook's announcement does not acknowledge the serious privacy implications of a large-scale, social media deployment of instantaneous facial recognition on the personal data of billions.

105. On Facebook's decision to adopt the business change on an opt-out basis, Sherman wrote:

> When we first introduced this feature in 2010, there was no industry standard for how people should be able to control face recognition. We decided to notify people on Facebook and provide a way to disable it in their account settings at any time … Just as in 2010, we had to evaluate how we'd inform people and give them choice over these new uses of the technology.

[47] 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/.

106. This is a significant misrepresentation and an omission of Facebook's regulatory obligations to the FTC under the Consent Order.

107. After the FTC settlement in 2011, Facebook was not at liberty to self-evaluate and unilaterally enact significant changes in privacy practices. The Consent Order requires Facebook to adhere to specific regulatory guidelines on obtaining affirmative consent to change privacy settings.

108. The announcement also failed to mention that in 2013, Facebook automatically applied "Tag Suggestions" to all users by default—and that if users did not opt-out of Tag Suggestions in their privacy settings, the extended facial recognition practice would automatically apply to them without consent.

109. WIRED Security Reporter Lily Hay Newman criticized this setting:

> But the "tag suggestions" preference dates back more than four years. Even if you fully understood enough about face-recognition technology at the time to make a carefully considered choice in 2013, that doesn't necessarily mean you'll be fine letting even more of it into your life now.[48]

110. Contrary to Part I(B) of the 2011 FTC Consent Order, Facebook has consistently misrepresented "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."[49]

F. Users Oppose Facebook's Additional Facial Recognition Techniques

111. Jared Bennett of Center for Public Integrity remarked on Facebook's "uniquely aggressive" opposition to any limits on its increasingly intrusive facial recognition technology. [50]

> In 2012, at a hearing of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, then-Chairman Al Franken (D-MN) asked Facebook's then-manager of privacy and public policy, Rob Sherman, to assure users the company wouldn't share its faceprint database with third parties. Sherman declined.

112. Facebook has still not clarified in 2018 which third parties have access to users' biometric data, and the purposes of disclosures.

113. WIRED Reporter Lily Hay Newman commented:[51]

---

[48] *See* Lily Hay Newman, *supra*.
[49] Facebook Consent Order.
[50] Jared Bennett, *Facebook: Your Face Belongs to Us* The Daily Beast, July. 31, 2017. https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition.
[51] Lily Hay Newman, *supra*.

> Observers also note that limited face recognition applications for users doesn't necessarily mean that Facebook as a company isn't deriving a larger benefit from all the biometric face data it gathers. As a public company, if Facebook can find opportunities to monetize the data or harness it to fuel user growth, it will take them.

114. Mashable Reporter MJ Franklin also noted:[52]

> The in-app announcement was met with a great deal of skepticism. Fast Company pointed out that Facebook's announcement coincided with legal setbacks. According to Bloomberg, a federal judge recently ruled that the social network 'must face claims that it violated the privacy of millions of users by gathering and storing biometric data without their consent.

115. Consumers publicly voiced their distrust and discomfort with Facebook's business changes to facial recognition, many of them noting that Facebook never sought their affirmative express consent:

[52] MJ Franklin, *How to turn off Facebook's new face recognition features* Mashable, Feb. 28, 2018, https://mashable.com/2018/02/28/how-to-turn-off-facebook-face-recognition/.

G. No Information on the Disclosure of Facial Recognition Data to Third Parties and Their Downstream Uses

116. Facebook announced significant changes to the facial recognition setting without explaining how the additional biometric data obtained from users and non-users will be disclosed to and used by third parties.

117. Facebook remains vague and unclear about how it utilizes the vast biometric data collected from users and non-users, with the Tag Suggestions and its subsequent facial recognition techniques.

118. Facebook's privacy policy does not specifically address the implications of facial recognition data by third-party service providers and advertisers, despite the heightened sensitivities of biometric personal information.

119. Facebook's privacy policy on "Sharing with Third-Party Partners" claims that advertisers and analytics services only have access to "non-personally identifiable information."[53]

> We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you.

[53] Facebook, *Data Policy*, (Sep. 29, 2016) https://www.facebook.com/full_data_use_policy.

120. Facebook does explain how an identity-matched facial image is not personally identifiable information.

121. Facebook's definition of PII is limited and misleading: "information like name or email address that can by itself be used to contact you or identifies who you are."[54] Facebook does not consider the privacy implications of information that may not independently be personally identifiable but can be readily matched with other demographic segments and quasi-identifiers to pinpoint one person with sufficient accuracy.

> **Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).**
> We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.
>
> Please review your advertising preferences to understand why you're seeing a particular ad on Facebook. You can adjust your ad preferences if you want to control and manage your ad experience on Facebook.

122. Facebook's Help Center claims that facial template data is stored as a "unique number."[55]

[54] *Id.*
[55] Facebook Help Center, *How does Facebook's face recognition work?* (2018), https://www.facebook.com/help/122175507864081.

> Our technology analyzes the pixels in photos and videos, such as your profile picture and photos and videos that you've been tagged in, to calculate a unique number, which we call a template.

123. From this definition, it is highly possible that Facebook may classify biometric templates as non-personally identifiable information that can be disclosed to third parties and advertisers. Facebook may consider facial recognition data to be sufficiently "de-identified" by the numerical scoring process, and overlook the privacy implications of giving third parties access to the data.

124. Facebook could also disclose biometric data to third parties by contending that the user gave consent. Given the current opt-out setting for facial recognition and the various misrepresentations made by Facebook to induce consumers into adopting privacy-invasive technologies, the FTC should investigate whether Facebook's "data-sharing programs with third parties" violate the 2011 Consent Order.

H. Facebook Fails to Establish that Application Developers, the Government, and Other Third Parties Will Not Be Able to Access Users' Biometric Data

125. The Facebook Platform makes a variety of personal data available to application developers and external websites.[56] Application developers obtain access to account information when they connect with an application.[57] Applications may also obtain users' friends' data,[58] and access connections between users who have both connected to an application.[59]

126. 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., people, photos, events, and pages) and the connections between them (e.g., friend relationships, shared content, and photo tags)."[60] Developers may leverage this API within apps.

127. 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."[61]

128. To obtain personal data to develop applications, developers may only request the information that they need to operate their application. However, Facebook does not

[56] Facebook Platform Policies, Storing and Using Data You Receive From Us, https://developers.facebook.com/policy ("Platform Policies").
[57] *Id.* at ¶5.
[58] *Id.* at ¶4.
[59] *Id.* at ¶11.
[60] Facebook Developers, Graph API, https://developers.facebook.com/docs/reference/api.
[61] Facebook for Websites, Personalization, https://developers.facebook.com/docs/guides/web/#personalization.

define what is necessary, and the terms leave developers to determine what they need.[62]

129. 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.[63]

130. 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…"[64] Facebook claims that 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.[65] Advertisers may cache Facebook user data indefinitely.

131. 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."[66] The U.S. Department of Justice ("DOJ") has stated that the "standard data production" from 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."[67]

132. The U.S. government has an interest in accessing the information present on Facebook and other social networking sites,[68] and law enforcement has used Facebook in pursuing investigations.[69] 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."[70]

---

[62] Platform Policies, *supra*, at ¶1.
[63] Reach and Targeting, *Reach Real People with Precise Targeting, at Location Targeting*, https://www.facebook.com/adsmarketing/index.php?sk=targeting_filters.
[64] Ethan Beard, *A New Data Model*, Facebook Developer's Blog, Apr. 21, 2010, https://developers.facebook.com/blog/post/378.
[65] 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.
[66] Facebook, Privacy Policy, https://www.facebook.com/policy.php.
[67] 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, at 17, http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.
[68] *Id.*
[69] *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 .
[70] John Lynch & Jenny Ellickson, *supra*.

The same training materials include a screenshot of the picture "tagging" process[71] and makes reference to the one billion pictures being added every month.

I. Privacy Controls to Opt-Out of Facial Recognition Are Not Clear and Prominent

133. The 2011 FTC Consent Order requires that Facebook obtain affirmative express consent to override existing privacy settings. The Commission authoritatively expressed that Facebook must respect user consent by providing an affirmative opt-in choice for new business practices that implicate consumer privacy.[72]

> Part II of the proposed order requires Facebook to give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings.

134. Consent must be meaningful and specific, and obtained from informed users. Cumbersome opt-out settings violate the high standard of compliance imposed by Consent Order.

135. Notwithstanding the clear requirements of the Consent Order, Facebook placed the burden on its users to opt-out of facial recognition. It has further misrepresented the simplicity of the opt-out choice as a "simple setting,"[73] toggled by a "single on/off control" when it announced changes to the facial recognition practice.

136. On December 19, 2017, Facebook's Director of Applied Machine Learning Joaquin Quiñonero Candela posted an announcement entitled, "Managing Your Identity on Facebook with Face Recognition Technology."

> You control whether Facebook can recognize you in photos and videos. Soon, you will begin to see a simple on/off switch instead of settings for individual features that use face recognition technology. We designed this as an on/off switch because people gave us feedback that they prefer a simpler control than having to decide for every single feature using face recognition technology. To learn more about all of these features, visit the Help Center or your account settings.

137. The "on/off switch" requires the user to navigate multiple Facebook settings to locate. Facebook did not operationalize opt-out with an intuitive and distinguishable setting.

138. On a phone, the user must open the Facebook app and tap on the overflow button (three-line icon). Then go to Settings > Privacy Shortcuts > More Settings > Face

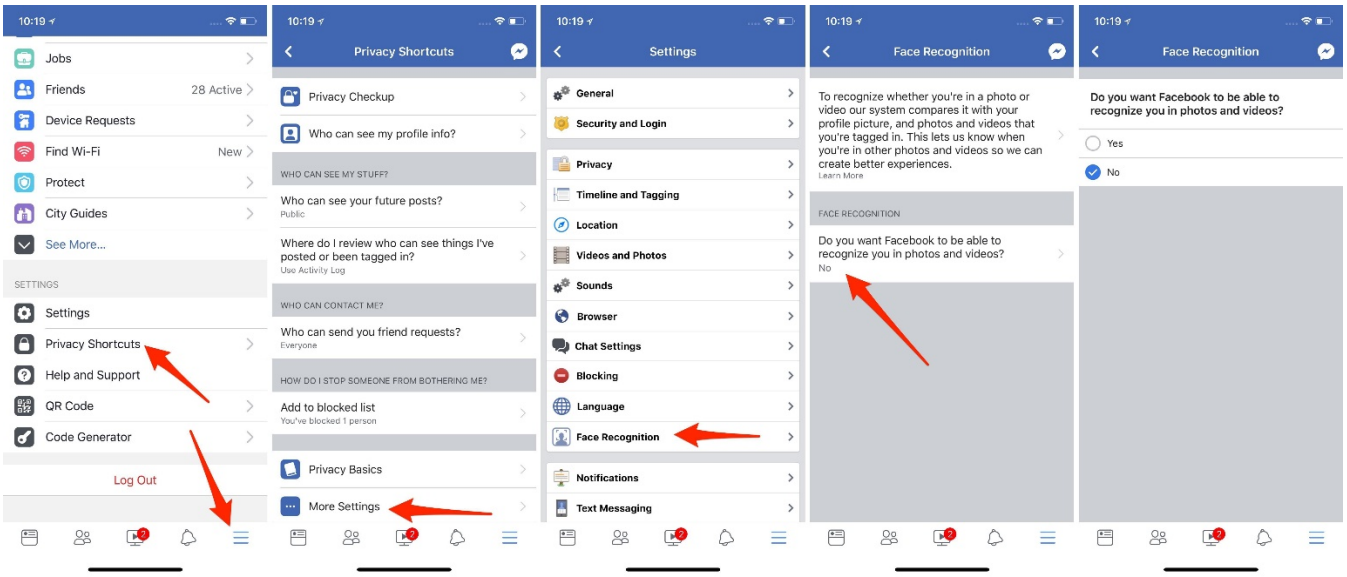
---

[71] *Id*. at 15.
[72] Facebook, Inc. Proposed Consent Order.
[73] Joaquin Quiñonero Candela, *Managing Your Identity on Facebook with Face Recognition Technology*, Facebook Newsroom, (Dec.19, 2017), https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/.

Recognition, then tap on the Face Recognition question. Finally, they can select No after this five-step process.

139. Ordinary consumers will face immense difficulty in locating the opt-out switch, just like they did in 2013 when Tag Suggestions were automatically turned on.

140. This indicates a violation of the Consent Order regarding affirmative consent as well as clear and prominent notice. The confusing setting invalidates affirmative consent by making the exercise of choice inaccessible for a majority of users. It also diminishes user awareness of the existence of this facial recognition setting.



J. Facebook is Pursuing the Commercialization of Biometric Data

141. Facebook economically benefits from the development of facial recognition techniques.

142. Facebook routinely makes misrepresentations to induce consumers to adopt wider and more pervasive uses of facial recognition technology. Therefore, the FTC must exercise the fullest extent of its legal authority to prohibit and limit these privacy-invasive technologies by enforcing the 2011 Consent Order.

i. Facebook's Facial Recognition Patents

143. In 2017, Facebook submitted four patent applications[74] on facial recognition techniques.

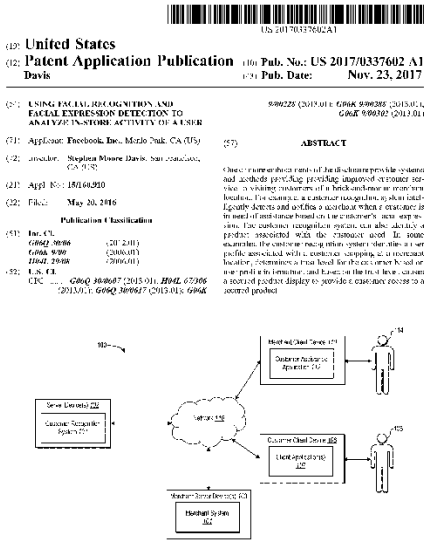
144. On March 9, 2017, Facebook submitted a patent application for "Facial Recognition Using Social Networking Information," which details a system that detects and tracks

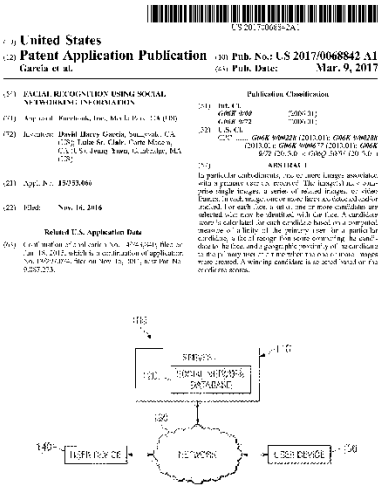
[74] USPTO Applicaton #: #20170337602; USPTO Applicaton #: #20170323299; USPTO Applicaton #: #20170140214; USPTO Applicaton #: #20170068842.

the exact geographic dimensions of a candidate's facial features to apply a template "score" that can be compared across various "faces in video, photos, or other media hosted on the social network"[75] for biometric matches.

145. On November 2017, Facebook filed two patents for "Facial Recognition Identification for In-Store Payment Transactions" and "Using Facial Recognition and Facial Expression Detection to Analyze In-Store Activity of a User."

146. The two applications detail a customer recognition system which "intelligently detects and notifies a merchant when a customer is in need of assistance based on the customer's facial expression. The customer recognition system can also identify a product associated with the customer need."





147. Facebook's patent applications attest to the company's primary commercial purpose in expanding its biometric data collection, and the pervasive uses of facial recognition technology that it envisions for the near future. The FTC must ensure that Facebook adheres to its obligations for user privacy as compelled by the 2011 Consent Order.

ii. Facebook's Annual Report to the Securities and Exchange Commission

148. Facebook's annual filing to the Securities and Exchange Commission ("SEC") for the 2017 fiscal year explicitly states that compliance with the FTC Consent Order and

[75] *Available at,* http://www.freshpatents.com/-dt20170309ptan20170068842.php; http://www.freshpatents.com/-dt20171109ptan20170323299.php.

modifying the company's practices to obtain affirmative express consent could "adversely affect financial results."[76]

149. On enforcement actions on the Consent Order, Facebook claimed:

> Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices. Such incidents may also result in a decline in our active user base or engagement levels. Any of these events could have a material and adverse effect on our business, reputation, or financial results.

150. On modifying practices to obtain consent, Facebook claimed:

> [R]egulatory or legislative actions affecting the manner in which we display content to our users or obtain consent to various practices could adversely affect user growth and engagement. Such actions could affect the manner in which we provide our services or adversely affect our financial results.[77]

151. These financial disclosures expressly indicate that Facebook is structurally and economically incentivized to monetize greater data collection. Facebook admits that modifying its practices to obtain consent for various practices will detriment its user growth and "engagement," leading to negative financial results. The FTC must affirmatively enforce the Consent Order against Facebook to ensure that it fully complies with all the provisions of the settlement.

K. Facebook Has Consistently Failed to Ensure Compliance by App Developers

152. In 2009, Facebook operated a deceptive Verified Apps program which claimed that Facebook gives preferential treatment to Platform Applications whose security standards exceed expectations in Facebook's "detailed review process."

153. Facebook misrepresented to its users that Verified Apps will "offer extra assurances to help users identify applications they can trust -- applications that are secure, respectful and transparent, and have demonstrated commitment to compliance with Platform policies."[78]

154. However, an investigation by the Commission revealed that Facebook had misrepresented the heightened security of Verified Apps. The FTC detailed this

[76] Facebook, Annual Report, SEC File No., 001-35551, at 13, (2016), https://www.sec.gov/Archives/edgar/data/1326801/000132680117000007/fb-12312016x10k.htm.
[77] *Id.* at 16.
[78] Facebook, *Facebook Expands Power of Platform Across the Web and Around the World*, Press Release, July 23, 2008, https://newsroom.fb.com/news/2008/07/facebook-expands-power-of-platform-across-the-web-and-around-the-world/.

deceptive practice in the complaint that underlies the 2011 Consent Order against Facebook: [79]

> Contrary to the statements set forth … before it awarded the Verified Apps badge, Facebook took no steps to verify either the security of a Verified Application's website or the security the Application provided for the user information it collected, beyond such steps as it may have taken regarding any other Platform Application.

155. Unfortunately, recent revelations of Facebook's negligence in disclosing the personal data of 50 million American voters to Cambridge Analytica and various affiliates show that Facebook has not improved its verification of app developers in the post-FTC Consent Order era.

156. On March 20, 2018, a former Facebook Operations Manager from 2011 to 2012 Sandy Parakilas published an article entitled "I worked at Facebook. I know how Cambridge Analytica could have happened."[80]

> Critically, once the data passed from Facebook's servers to the developer, Facebook lost all insight into or control over how the data was used. To prevent abuse, Facebook created a set of platform policies that forbade certain kinds of activity, such as selling the data or passing it to an ad network or data broker such as Cambridge Analytica. However, Facebook had very few ways to discover abuse or act on it once discovered.

157. Parakilas details Facebook's routine indifference to apps that violated policies and the Terms of Service.

> Facebook had the following tools to deal with these cases: It could call the developer and demand answers; it could demand an audit of the developer's application and associated data storage, a right granted in the platform policies; it could ban the developer from the platform; it could sue the developer for breach of the policies, or it could do some combination of the above. During my 16 months at Facebook, I called many developers and demanded compliance, but I don't recall the company conducting a single audit of a developer where the company inspected the developer's data storage. Lawsuits and outright bans were also very rare. I believe the reason for lax enforcement was simple: Facebook didn't want to make the public aware of huge weaknesses in its data security.

---

[79] Fed. Trade Comm'n, Facebook, Inc., FTC File No. 092 3184 (2011) (Complaint), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

[80] Sandy Parakilas, *I worked at Facebook. I know how Cambridge Analytica could have happened* The Washington Post, Mar. 20, 2018, https://www.washingtonpost.com/opinions/i-worked-at-facebook-i-know-how-cambridge-analytica-could-have-happened/2018/03/20/edc7ef8a-2bc4-11e8-8ad6-fbc50284fce8_story.html.

158. Parakilas compares Facebook's disregard for data protection in 2012 to the 2018 Cambridge Analytica scandal, and concludes that compliance has not improved:

> Facebook will argue that things have changed since 2012 and that the company has much better processes in place now. If that were true, Cambridge Analytica would be small side note, a developer that Facebook shut down and sued out of existence in December 2015 when word first got out that it had violated Facebook's policies to acquire the data of millions. Instead, it appears Facebook used the same playbook that I saw in 2012. It took the developer's word rather than conducting an audit, and it ignored press reports about Cambridge Analytica using Facebook data in violation of its terms during the election.

159. On March 20, 2018, EPIC and a coalition of consumer organizations urged the FTC to reopen the investigation of Facebook, and to sanction the company's clear violations of the 2011 Consent Order.[81]

> "As the Facebook Order makes clear, Facebook must "get consumers' approval before it changes the way it shares their data," and must "obtain consumers' affirmative express consent before enacting changes that override their privacy preferences." The FTC also barred Facebook from "making misrepresentations about the privacy or security of consumers' personal information."
>
> Yet Facebook's business practices resulted in the disclosure of consumers' "names, education, work histories, birthdays, likes, locations, photos, relationship statuses, and religious and political affiliations" to Cambridge Analytica without their knowledge or consent. In 2014, Facebook acknowledged that it allowed app developers to access profile information on an app users' friends without the friends' knowledge or consent, stating that consumers "are often surprised when a friend shares their information with an app." Facebook's admission that it disclosed data to third parties without users' consent suggests a clear violation of the 2011 Facebook Order."

160. The FTC has an affirmative duty to undertake a review of substantial changes in Facebook's business practices that implicate user privacy and to ensure compliance with the Consent Order.

161. Facebook's change to the facial recognition setting was implemented without the affirmative express consent of users. This substantial change in business practice is a serious consent decree violation which the FTC must enjoin immediately. It is imperative that the Commission pursue an investigation to prohibit the unlawful proliferation of biometric data collection by Facebook and its unaccountable commercial counterparts.

[81] EPIC, *EPIC, Consumer Groups Urge FTC To Investigate Facebook* (Mar. 20, 2018), https://epic.org/2018/03/epic-consumer-groups-urge-ftc-.html. f

L. Facial Recognition is Illegal in Other Countries

162. Canada and Europe limit how companies can collect and store biometric data. The deployment of commercial facial recognition technology is widely considered an invasion of privacy rights in Canada and Europe.

163. The Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[82]

164. The EU Article 29 Data Protection Working Party issued an opinion on developments in biometric technologies which states that consent must be obtained for the storage and use of biometric data. [83]

165. On October 15, 2012, Facebook disabled its tagging facial recognition practice for users in the European Union, following an investigation by the Irish Data Protection Commissioner.

166. In 2015, Facebook created a photo-sharing app called Moments which does not use facial recognition technology for Canadian and European users.

167. The BBC reported that Facebook Moments Product Manager Will Ruben stated that the phone is given a numerical representation of a face, "but that number is not stored anywhere on our servers, and it is only used to compare against the other photos on your phone."[84]

168. The Inquirer reported that a Facebook spokesperson said: "Facebook has notified this office of the Moments app and advised us that in the EU version of the Moments app they do not control or initiate the use of any feature recognition technology." [85]

169. Facebook is capable of developing alternative techniques that are less privacy-invasive. The photo sharing aspect of the social media network can be facilitated without the use of privacy-pervasive facial recognition technology, as it has been done for Canada and Europe.

170. The disparity of privacy protections afforded for the nationals and residents of the United States due to the lack of enforcement action against Facebook is unacceptable.

---

[82] 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), http://priv.gc.ca/cfdc/2009/2009_008_0716_e.pdf.

[83] Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* (Apr. 27, 2012), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[84] Leo Kelion, *Facebook Moments facial-recognition app launches in Europe* BBC News, May 10, 2016, http://www.bbc.com/news/technology-36256765.

[85] Carly Page, *Facebook launches facial recognition app in Europe, without facial recognition tech,* The Inquirer, May 11, 2016, https://www.theinquirer.net/inquirer/news/2457657/facebook-launches-face-recognition-app-in-europe-without-face-recognition-tech.

171. The FTC is the primary privacy regulator in the United States. The Commission must enforce the Consent Order to compel Facebook to modify its business practice to comply with strict privacy protections.

V. Prior Consumer Complaints to the FTC Regarding Facebook's Facial Recognition

172. EPIC has previously urged the Commission to prohibit Facebook's facial recognition techniques on multiple occasions.

173. In June 2011, EPIC and a coalition of consumer organizations filed a complaint with the FTC alleging that Facebook's covert deployment of its facial recognition technology was unfair and deceptive.[86] EPIC stated that Facebook's "Tag Suggestions" technique, "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."[87] EPIC warned that "unless the Commission acts promptly, Facebook will routinely automate facial identification and eliminate any pretense of user control over the use of their own images for online identification."[88] EPIC emphasized that the Commission's "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."[89]

174. In December 2011, EPIC urged the Commission to strengthen its proposed settlement with Facebook by requiring it to "cease creating facial recognition profiles without users' affirmative consent."[90] EPIC contended that while the Order's broad prohibition on privacy misrepresentations already covered Facebook's deceptive use of facial recognition, the Order should have been amended to proscribe the practice explicitly.[91]

175. In January, 2012, EPIC submitted extensive comments in response to the FTC's workshop "Face Facts: A Forum on Facial Recognition Technology."[92] EPIC again emphasized that Facebook's facial recognition practice "entirely fails at informing users how their photo data will be used or to provide any meaningful consent for use," as required by the Order. EPIC advised the Commission that, "Commercial actors should not deploy facial techniques until adequate safeguards are established. As such

[86] In the Matter of Facebook, Inc. and the Facial Identification of Users (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.
[87] *Id*.
[88] *Id*.
[89] *Id*.
[90] *Comments of EPIC*, In the Matter of Facebook, Inc., FTC File No. 092 3184 (Dec. 27, 2011), https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf.
[91] *Id*.
[92] *Comments of EPIC*, "Face Facts: A Forum on Facial Recognition," Project No. P115406, (Jan. 31, 2012), https://epic.org/privacy/facerecognition/EPIC-Face-Facts-Comments.pdf.

safeguards have not yet been established, EPIC would recommend a moratorium on the commercial deployment of facial recognition techniques."[93]

VI. The Importance of Enforcing Consent Orders for Consumer Privacy

176. The effectiveness of the FTC depends upon the agency's willingness to enforce the legal judgments it obtains. However, the FTC routinely fails to enforce its consent orders, which promotes industry disregard for the FTC. Companies under consent decree have no incentive to protect consumer data if they do not anticipate the FTC to hold them accountable when they violate consent decrees.

177. EPIC and other consumer organizations have routinely called attention to the numerous changes Facebook has made to its privacy settings without obtaining users' affirmative consent, in violation of the terms of its FTC consent decree.[94]

178. In 2011, Facebook entered into a 20-year consent order with the FTC in which it agreed that it "shall not misrepresent … the extent to which it maintains the privacy or security of covered information," and would provide disclosure separate from its privacy policy.[95]

it agreed that it "shall not misrepresent … the extent to which it maintains the privacy or security of covered information," and would provide disclosure separate from its privacy policy.[96]

179. 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.[97]

180. 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."[98]

---

[93] *Id*.
[94] EPIC, *In the Matter of Facebook Inc: Complaint, Request for Investigation, Injunction, and Other Relief* (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; ("EPIC 2009 Facebook Complaint").EPIC *In the Matter of Facebook Inc: Complaint, Request for Investigation, Injunction, and Other Relief* (May 5, 2010),. ("EPIC Supplemental Facebook Complaint"), https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.
[95] Facebook Consent Order.
[96] *Id*.
[97] EPIC 2009 Facebook Complaint.
[98] *Id.*

181. On January 14, 2010, EPIC filed a second Complaint with the Commission concerning Facebook's unfair and deceptive trade practices.[99]

182. EPIC's amended Complaint observed that Facebook's business practices "violate user expectations, diminish user privacy, and contradict Facebook's own representations."[100]

183. 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.[101] 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."[102]

184. 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 confidence in new business services. But the current FTC appears reluctant to take similar steps on behalf of American consumers.

185. To date, the FTC has failed to take any action with respect to Facebook's changes in biometric privacy practices.

186. 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.

187. Companies and consumer organizations may disagree as to whether a significant change in business practices violates a consent order. That is a decision ultimately for the Commission. But it is incumbent upon the FTC to develop a process that ensures a reasoned decision, subject to public review. At present, there is no meaningful public process to ensure compliance with FTC consent orders.

VI. Legal Analysis

[99] *Id*.
[100] *Id.*
[101] 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.
[102] *Id.*

188. The 2011 FTC Consent Order arises from a series of complaints filed by EPIC and other consumer privacy organizations from 2009 to 2011concerning material changes to privacy settings made by Facebook.

189. Pursuant to EPIC's requests for investigation, the Commission filed an eight-count complaint against Facebook for unfair and deceptive practices in contravention of Section 5 of the Federal Trade Commission Act.

190. On November 29, 2011, the FTC published a press release announcing that Facebook settled charges with the Commission. The FTC enumerated a list of prohibited practices under the proposed settlement:

"Specifically, under the proposed settlement, Facebook is:

- "barred from making misrepresentations about the privacy or security of consumers' personal information;
- "required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
- "required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- "required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
- "required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected."

191. The Commission has a non-discretionary obligation to enforce a final order.

192. To date, the FTC has failed to take any action with respect to Facebook's changes in biometric privacy practices. Critically, the Commission has not filed a lawsuit pursuant to, the Federal Trade Commission Act which states that the FTC "shall" obtain injunctive relief and recover civil penalties against companies that violate consent orders. 15 U.S.C. § 45(l).

193. The FTC has exclusive authority over the enforcement of its consent orders. The enforcement provision of the FTC Act, Section 5(l), makes clear that the agency action is not discretionary; a violating party "shall forfeit" a penalty and be subject to an enforcement action.

194. The FTC is charged with performing a "discrete agency action." A "discrete agency action" is a "final agency action" under the Administrative Procedure Act. *In re Aiken County*, 645 F.3d 428, 437 (D.C. Cir. 2011). "Agency action unlawfully withheld" is a defined as "discrete agency action that [the agency] is required to take." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64 (2004).

195. Agency action is the "whole or part of an agency rule order, license, sanction, relief, or the equivalent or denial thereof, or failure to act." 5 U.S.C. § 551 (13). Agency action, including a "failure to act" is subject to judicial review. *Amador County, Cal. v. Salazar*, 640 F.3d 373, 383 (D.C. Cir. 2011)

196. Here the FTC unlawfully withheld such an action – namely commencing a civil action for violation of its consent order, and has failed to perform by not enforcing its 2012 Consent Order against Facebook.

197. EPIC may "compel agency action unlawfully withheld" pursuant to the Administrative Procedure Act. 5 U.S.C. § 706(1).

VII. Prayer for Investigation and Relief

198. 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.

199. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices that constitute consumer harm.[103]

200. Petitioners request that the Commission investigate Facebook, enjoin the deployment of additional facial recognition techniques as a violation of the 2011 Consent Order, and require Facebook to modify its biometric data practices to protect the privacy of Facebook users and non-users. Specifically, Petitioners ask the Commission to:

    a. Require Facebook to suspend immediately any form of Facebook-initiated automated facial scanning or other forms of biometric identification of Facebook users based on Facebook's internal database of facial images.

    b. Delete all facial images, facial templates, and biometric identifiers wrongfully obtained

    c. 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

[103] 15 U.S.C. § 45.

and uses consumer information (2) the extent to which consumers may exercise control over the collection, use, or disclosure of consumer information**.**

d. Require Facebook to expressly categorize the types of user information it collects, and to clarify which type of third party gets access to which categories of user information, and for what purpose.

e. Require Facebook to alert its users on the privacy implications of the services of Facebook and its subsidiaries which collect, store, and disclose biometric data. Prohibit Facebook from inducing users into embracing pervasive augmentations of facial recognition technology with announcements that misrepresent the commercial purposes for which Facebook collects users' facial templates.

f. Require that Facebook, prior to any new or additional disclosure by Facebook of a user's identified information to 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.

g. Audit and ensure that Facebook maintains a comprehensive privacy program, as required by the 2011 Consent Order, 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.

h. Require Facebook to establish appropriate security and privacy safeguards for biometric data practices, such as implementing an opt-in control for users, notifying users of business changes to encourage the exercise of informed choice, and limiting the disclosure of facial template data to third parties.

i. Seek appropriate injunctive and compensatory relief.

201. 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,

/s/ *Marc Rotenberg*
Marc Rotenberg
President EPIC

/s/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel
Coordinator, Privacy Coalition

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Counsel

/s/ *Sunny Kang*
Sunny Kang
EPIC International Consumer Counsel

Electronic Privacy Information Center
Campaign for a Commercial Free Childhood
Center for Digital Democracy
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Watchdog
Cyber Privacy Project
Defending Rights & Dissent
Government Accountability Project
Patient Privacy Rights
Privacy Rights Clearinghouse
Southern Poverty Law Center
U.S. Public Interest Research Group

April 6, 2018