CAUSE NO. 22-0121

THE STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	Sherry Griffis
	§	
	§	
	§	
Plaintiff,	§	
	§	
v.	§	
	§	71ST JUDICIAL DISTRICT
Meta Platforms, Inc., f/k/a Facebook, Inc.	§	
	§	
	§	
	§	
	§	
Defendant.	§	HARRISON COUNTY, TEXAS

PLAINTIFF'S PETITION

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff, STATE OF TEXAS, acting by and through the Attorney General of Texas, KEN PAXTON (the "State"), on behalf of the public interest, complains of Defendant META PLATFORMS, INC., also known as "FACEBOOK." In this action, the State alleges that Facebook unlawfully captured the biometric identifiers of Texans for a commercial purpose without their informed consent, disclosed those identifiers to others, and failed to destroy collected identifiers within a reasonable time, all in violation of the Texas Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code § 503.001 ("CUBI"); and that Facebook engaged in false, misleading, and deceptive acts and practices in violation of the Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), Tex. Bus. & Com. Code §§ 17.41 *et seq.* Facebook has, for over a decade, built an Artificial Intelligence empire on the backs of Texans by deceiving them while capturing their most intimate data, thereby putting their well-being, safety, and security at risk. Under Texas law, the Attorney General has the exclusive authority to vindicate Texans' rights under CUBI, and he, therefor, brings this Petition before the Court. In support hereof, General Paxton, acting for the State, will respectfully show the Court the following.

INTRODUCTION

Defendant Meta Platforms, Inc., better known as "Facebook," was founded in 2004. The ostensible premise behind Facebook's social-media platform was as simple as it was appealing: With only a few keystrokes, users could connect with friends and family, and share photographs, milestones, and other life updates in their community of "Facebook friends."

Facebook was an instant hit, and within months, "Facebook" became synonymous with social media. Since 2008, Facebook has operated the largest social-media platform in the world.

In 2011, approximately 12 million Texans had a Facebook account; by 2021, that number had ballooned to an estimated *20.5 million Texans*. The popularity of its brand has made Facebook one of the most valuable companies in the world, with one of the top ten market capitalizations in the world, and revenue of over $85 billion last year.

But Facebook's omnipresent empire was built on deception, lies, and brazen abuses of Texans' privacy rights—all for Facebook's own commercial gain. Of relevance here, for over a decade, while holding itself out as a trusted meeting place for Texans to connect and share special moments with family and friends, Facebook was secretly capturing, disclosing, unlawfully retaining—and profiting off of—Texans' most personal and highly sensitive information: records of their facial geometries, which Texas law refers to as biometric identifiers.

Facebook deceived the public by concealing the nature of its practices. Facebook knew that the term "biometric data" "tends to scare people off." *See* Pls.' Opp'n to Facebook, Inc.'s Mot. for Summ J. at 6, *In re Facebook Biometric Information Privacy Litigation*, No. 3:15-cv-03747-

JD (N.D. Cal. 2018), ECF No. 341. And so it did not use it, or otherwise inform users of its practices.

Texans who used Facebook's social-media services were oblivious to the fact that Facebook—without their permission—was capturing biometric information from photos and videos that users had uploaded for the sole purpose of sharing with family and friends.

Also unbeknownst to users, Facebook was disclosing users' personal information to other entities who further exploited it.

Moreover, Facebook often failed to destroy collected biometric identifiers within a reasonable time, exposing Texans to ever-increasing risks to their well-being, safety, and security. When information is wrongfully obtained to begin with, holding it for any amount of time is unreasonably long.

Facebook's illegal and deceptive conduct did not end with its users. For Texans who did *not* use Facebook's social-media services, Facebook was still capturing hundreds of millions of biometric identifiers from photos and videos innocently uploaded by friends and family who did use Facebook. There was no way for such non-users to know of or contest this exploitation.

Facebook knowingly captured biometric information for its own commercial benefit, to train and improve its facial-recognition technology, and thereby create a powerful artificial intelligence ("AI") apparatus that reaches all corners of the world and ensnares even those who have intentionally avoided using Facebook services.

The scope of Facebook's misconduct is staggering. Facebook repeatedly captured Texans' biometric identifiers without consent not hundreds, or thousands, or millions of times—but *billions* of times, all in violation of CUBI and the DTPA.

After paying $650 million for engaging in this same conduct in Illinois, being called out by whistleblowers who exposed Facebook's indifference to the societal harms it caused, and paying billions of dollars in fines to the Federal Trade Commission, Facebook finally claimed to have ceased its invasive and unlawful facial-recognition practices in late 2021. By that point, however, it had spent more than a decade secretly exploiting Texans and their personal information to perfect its AI apparatus.

There can be no free pass for Facebook unlawfully invading the privacy rights of tens of millions of Texas residents by misappropriating their data and putting one of their most personal and valuable possessions—records of their facial geometry—at risk from hackers and bad actors, all to build an AI-powered virtual-reality empire. The State brings this suit to hold Facebook accountable for covertly flouting Texas law for more than a decade, and to stop Facebook from ever again violating the rights of Texans for its commercial gain.

DISCOVERY CONTROL PLAN

1. The discovery in this case is intended to be conducted under Level 3 pursuant to Texas Rule of Civil Procedure 190.4. This case is not subject to the restrictions of expedited discovery under Texas Rule of Civil Procedure 169 because the State's claims include a claim for non-monetary injunctive relief and claims for monetary relief, including penalties and attorneys' fees and costs, in excess of $250,000, and the claims are within the jurisdictional limits of the Court.

THE DEFENDANT

2. Meta Platforms, Inc. ("Facebook") is a Delaware corporation with its headquarters and principal place of business at 1601 Willow Road, Menlo Park, California. Facebook directly

contracts with consumers in Texas to provide access to its social-media platforms. The number of Facebook's Texas users is likely in the tens of millions.

JURISDICTION AND VENUE

3. This enforcement action is brought by Attorney General of Texas Ken Paxton, through his Consumer Protection Division (CPD), in the name of the State and in the public interest, under the authority granted to him by section 503.001(d) of CUBI, on the ground that Facebook has (1) captured the biometric identifiers of individuals without their informed consent, as defined in, and declared unlawful by, section 503.001(b) of CUBI; (2) disclosed the biometric identifiers to other entities, as declared unlawful by section 503.001(c)(1) of CUBI; and (3) failed to destroy within a reasonable time the biometric identifiers it has collected, as declared unlawful by section 503.001(c)(3) of CUBI. General Paxton also brings this enforcement action pursuant to the authority granted to him by section 17.47 of the DTPA, on the ground that Facebook has engaged in false, deceptive, and misleading acts and practices in the course of trade and commerce. as defined in, and declared unlawful by, sections 17.46 (a) and (b) of the DTPA. In enforcement suits filed pursuant to section 503.001(d) of CUBI and section 17.47 of the DTPA, the Attorney General is authorized to seek civil penalties, redress for consumers, and equitable relief.

4. Venue of this suit is proper in Harrison County under section 17.47(b) of the DTPA because Facebook has done business in Harrison County, and under section 15.002(a)(1) of the Texas Civil Practices and Remedies Code because a substantial part of the events and omissions giving rise to the claims in this Petition occurred in Harrison County.

PUBLIC INTEREST

5. The State of Texas has reason to believe that Facebook has engaged in, and will continue to engage in, the unlawful practices set forth below; that Facebook has, by means of these unlawful acts and practices, caused damage to and acquired money or property (including

biometric identifiers) from persons; and that Facebook adversely affected the lawful conduct of trade and commerce, thereby directly and indirectly affecting the people of the State of Texas. Therefore, the Consumer Protection Division of the Office of the Attorney General of the State of Texas believes and is of the opinion that these proceedings are in the public interest.

TRADE AND COMMERCE

6. Facebook has, at all times described below, engaged in conduct that constitutes "trade" and "commerce," as those terms are defined in section 17.45(6) of the DTPA.

CONDITIONS PRECEDENT

7. All conditions precedent to the State's claim for relief have been performed or have occurred. The Consumer Protection Division informed Defendant, in general, of the alleged unlawful conduct described below at least seven days before filing suit, as may be required by subsection 17.47(a) of the DTPA.

ACTS OF AGENTS

8. Whenever in this Petition it is alleged that Facebook did any act, it is meant that Facebook performed or participated in the act, or that its officers, agents, or employees performed or participated in the act on behalf of and under the authority of Facebook.

BACKGROUND

A. Biometrics are used for everything from the benign unlocking of phones to criminal targeting and religious persecution.

9. "Biometrics" refer to physical characteristics that are unique to each individual. The most well-known example is the fingerprint.

10. Over the past two decades, the use of other biometrics has become increasingly common. Such biometric identifiers include retina or iris scans, records of face geometry, voiceprints, and the lay of blood vessels beneath an individual's skin. These biometric identifiers

were once difficult to capture without a live person, but Silicon Valley has been hard at work to enable machines to create biometric profiles without a live subject and without a human operator.

11. Today, one of the most prevalent uses of biometric identifiers by Big Tech is facial-recognition technology. This technology captures biometric identifiers by transforming a facial image—portrayed in photographs or videos—into an electronic map of the face.

12. When facial-recognition technology examines an image of a face, it extracts data from facial features and generates a face map through the use of facial-recognition algorithms. It can then compare the captured face map to other face maps it has stored in databases to see if there is a match.

13. Like a fingerprint, every record of facial geometry is unique, allowing face maps to serve a variety of security, financial, and law-enforcement functions. The more advanced the facial-recognition technology, the better it is at matching two facial images of the same individual.

14. Figure 1, below, shows an example of the data points that are captured by facial-recognition technology in mapping the image of a human face.

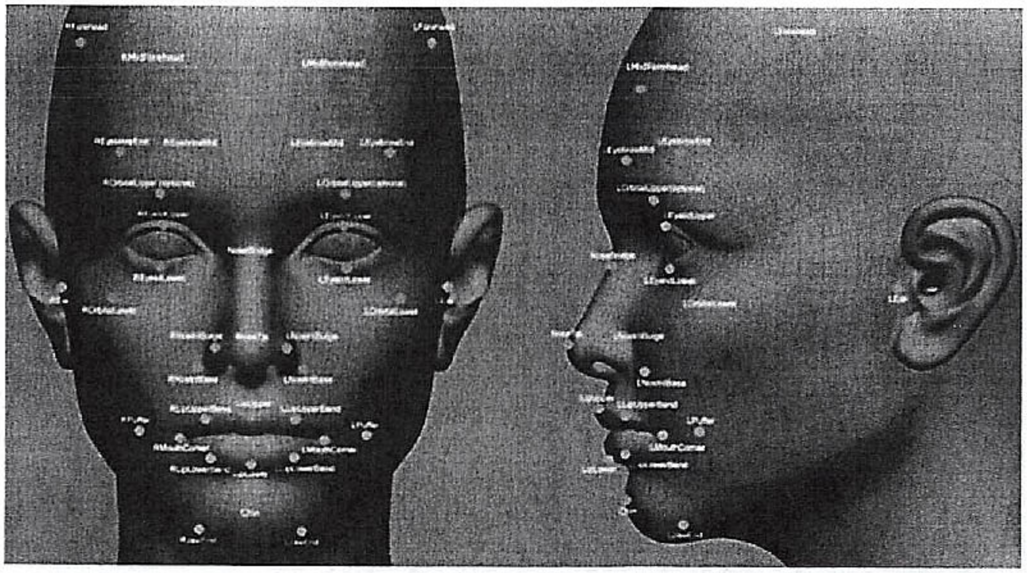


Figure 1

15. Advancements in computer processing and machine learning have vastly improved facial-recognition technology, generating many commercial applications for it, while rapidly raising alarming privacy concerns about its scale, scope, and secrecy—and about the improper uses it could serve when in the wrong hands.

16. Facial recognition is now used for a variety of day-to-day functions that formerly required passwords, secondary verification, or in-person confirmation of identity.

17. For instance, many cell phones and tablets now offer biometric functionality that allows users to unlock their devices by scanning their facial geometry; face geometry is used by banks to secure access to account information and authorize transactions; and businesses are using facial-recognition systems to control access to secure facilities.

18. But the use of biometrics and facial-recognition technology goes far beyond these innocuous examples.

19. Facial-recognition technology is a favorite of stalkers and criminals because, by simply having a photo of their target, they are able to locate that target's name, social-media account, and other personal information.[1] This technology is also used by retailers to identify potential thieves, but because the technology is not perfect, innocent individuals have been treated as criminals—which is particularly pernicious given that the technology is at its worst when purporting to identify minorities.[2] And governments have used this technology to suppress their constituents; the Communist Party of China, for example, has used its facial-recognition dragnet

[1] Drew Harwell, *This facial recognition website can turn anyone into a cop – or a stalker,* The Wash. Post, (May 14, 2021), https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/

[2] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match, N.Y. Times, (Dec 19, 2020),* https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

to surveil and persecute the ethnic Uyghur minority,[3] and to target Christians by deploying its technology in churches.[4]

20. The creation and maintenance of sprawling databases containing millions of people's biometrics generates an enormous risk that cyber criminals and other dangerous actors will access these unique identifiers and encroach into virtually every aspect of their owners' lives. The risk is particularly treacherous when those people have no knowledge of—or authority over—the capture and use of their biometrics.

21. Unlike other identifiers, such as Social Security numbers, which can be changed when stolen or misappropriated, biometric identifiers are permanent. Once a biometric identifier is captured, a bad actor can access and exploit the identifier for the rest of the victim's life. These unique and permanent biometric identifiers, once exposed, leave victims with no means to prevent identity theft, unauthorized tracking and targeting, or other threats to privacy, safety, and security.

B. <u>Texas implements CUBI to protect Texans from danger.</u>

22. Foreseeing the dangers that the capture of biometrics posed for Texans—dangers that have become only more severe as facial-technology has improved dramatically—the Texas Legislature enacted a law in 2001 to regulate the commercial capture of biometric identifiers. That law was recodified in 2009 as CUBI. To protect Texans from abuse, the Legislature chose to impose a requirement that is commonplace in the law: obtain informed consent.

[3] Chris Buckley and Paul Mozer, *How China Uses High-Tech Surveillance to Subdue Minorities*, N.Y. Times, *(May 22, 2019)*, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

[4] Chris Meserole, Technological surveillance of religion in China, Brookings, (July 22, 2020), https://www.brookings.edu/testimonies/technological-surveillance-of-religion-in-china/

23. Specifically, under CUBI, "A person may not capture a biometric identifier of an individual for a commercial purpose unless the person first:

(i) informs the individual before capturing the biometric identifier; and

(ii) receives the individual's consent to capture the biometric identifier."[5]

24. Moreover, an entity in possession of a biometric identifier may not disclose it to anybody else for any purpose (with the exception of limited, enumerated purposes, such as law enforcement).[6]

25. If an entity comes into possession of a biometric identifier, the entity must destroy it within a reasonable time, but no later than one year after the purpose for collecting the identifier expires.[7]

26. And the entity possessing a biometric identifier must store it, transmit it, and protect it from disclosure using reasonable care, in a way that is at least as protective as the way it stores, transmits, and protects other confidential information.

27. These prohibitions and protections are not only reasonable, but necessary in light of the risks inherent in allowing a Big Tech firm to access Texans' most sensitive and immutable personal information.

28. CUBI defines a biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[8]

29. Silicon Valley firms like Facebook are not safe guardians of this highly sensitive

[5] Tex. Bus. & Comm. Code § 503.001(b).

[6] Tex. Bus. & Comm. Code § 503.001(c)(1).

[7] Subject to limited exceptions. *See* Tex. Bus. & Comm. Code § 503.001(c)(3).

[8] Tex. Bus. & Comm. Code § 503.001(a).

information. On the contrary, such firms have been caught acting recklessly with others' private information on myriad occasions. For example, in 2011, Facebook entered into a settlement agreement with the FTC after the FTC caught the company engaging in widespread violations of users' privacy. The FTC allegations included: (a) that, in December 2009, Facebook changed its website so that certain information users had specifically designated as private was made public—with no warning to users and no opportunity for them to withhold consent; (b) that Facebook gave third-party apps access to *nearly all of users' personal data*, despite representing to users that the apps would have access only to the information they needed to operate; (c) that Facebook shared users' personal information with advertisers—after promising users it would not do so; and (d) that Facebook continued to allow access to the photos of users who had deleted their accounts, despite telling users that their photos would become inaccessible.

30. Further, in Europe, Facebook has been involved in litigation since 2015 over its practice of gathering the personal information of users and non-users for advertising purposes without first obtaining their consent

31. And in 2019, Facebook was fined $5 *billion* by the FTC for an array of privacy violations.

32. These examples illustrate Facebook's pattern of betraying users—promising privacy while secretly disclosing personal information to third parties for its commercial gain, and failing to remove users' personal information even after they had left Facebook.

33. We now know that, consistent with its track record, Facebook has done it again, this time secretly and recklessly disregarding the privacy of its users—and of any children, family members, or friends pictured in the users' uploaded images and videos—to capture maps of their faces. It has thereby created one of the world's largest databases of human face maps. Facebook

has committed this abuse and placed these individuals in danger all in order to train its AI apparatus in facial recognition—and all in violation of CUBI and the DTPA.

34. For over a decade, Facebook has brazenly violated CUBI and the DTPA. Facebook did not inform Texans that it was capturing their private biometric identifiers as part of its widespread facial-recognition program, let alone obtain their consent; it then disclosed those biometric identifiers to other entities; and it failed to delete its collected biometric identifiers within a reasonable time, compounding the risk of harm for tens of millions of Texans.

SPECIFIC FACTUAL ALLEGATIONS

35. Facebook's social-media platform allows users to upload and share photographs and videos with friends and relatives. Once a user uploads a photograph or video on Facebook, the user can "tag" (i.e., identify by name) other Facebook users and non-users who appear in the photograph or video.

36. Tagging has been pivotal to the explosive expansion of the Facebook empire. As articulated by Ezra Callahan, an early Facebook employee, "[t]he single greatest growth mechanism ever [for Facebook] was photo tagging. It shaped all of the rest of the product decisions that got made."[9]

37. Facebook's founder and CEO Mark Zuckerberg has similarly commented that, "the coolest thing about [Facebook] photos is that you can tag them . . . in the way that makes them linked to people's profiles."[10] He has also stated that photo tagging is "more important than every other [Facebook] feature put together," and that "very quickly" Facebook's "photo product became

[9] Adam Fisher, *Valley of Genius: The Uncensored History of Silicon Valley (As Told by the Hackers, Founders, and Freaks Who Made It Boom)* 365 (2018).

[10] Guest Lecture by Mark Zuckerberg, Harvard University at 25:44-57, YouTube (Dec. 7, 2005), *available at* https://www.youtube.com/watch?v=_YpaWA_-XRw.

the most used photos product on the web."[11] Other Facebook executives have similarly described photo-tagging as a "core piece of functionality" that made Facebook the "biggest photo product on the web."[12] And its Vice President of Product Design stated:

> One of the stories we used to tell in the early days of Facebook was how a small, two-engineer project came to dominate the entire photo sharing landscape in the late 2000s. . . . There were no bells and whistles, save one... The one feature Facebook Photos *did* have, even in its earliest incarnation, was this: photo tagging. . . . What a simple feature. And yet. It made all the difference. Facebook Photos skyrocketed in popularity. Within a few years, it was the most popular photo sharing service on the Internet.[13]

C. <u>Facebook launches Tag Suggestions.</u>

38. To boost use of the tagging feature, Facebook announced a program in 2010 called "Tag Suggestions."[14]

39. Tag Suggestions worked by using Facebook's proprietary facial-recognition process to capture and analyze the records of facial geometry—of both users *and* non-users—obtained from user-uploaded photos and videos. One part of the facial-recognition process is shown in Figure 2, below:

[11] A Conversation with Mark Zuckerberg, Web 2.0 Summit 2010 at 19:15-22, YouTube, (Nov. 19, 2010), *available at* https://www.youtube.com/watch?v=CRUOl03nZIc.

[12] Kim-Mai Cutler, *Q&A: Facebook's Bret Taylor on privacy, the transition from FriendFeed*, VentureBeat (May 28, 2010), *available at* https://venturebeat.com/2010/05/28/bret-taylor-facebook.

[13] *See* Julie Zhou Twitter (Apr. 8, 2021), *available at* https://twitter.com/joulee/status/1380183017025511430.

[14] This feature was later upgraded and called simply "Face Recognition."

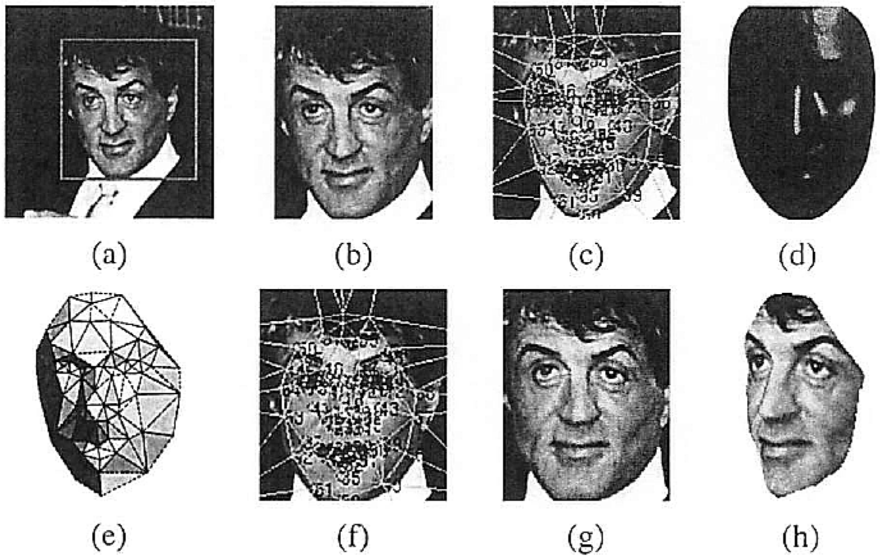
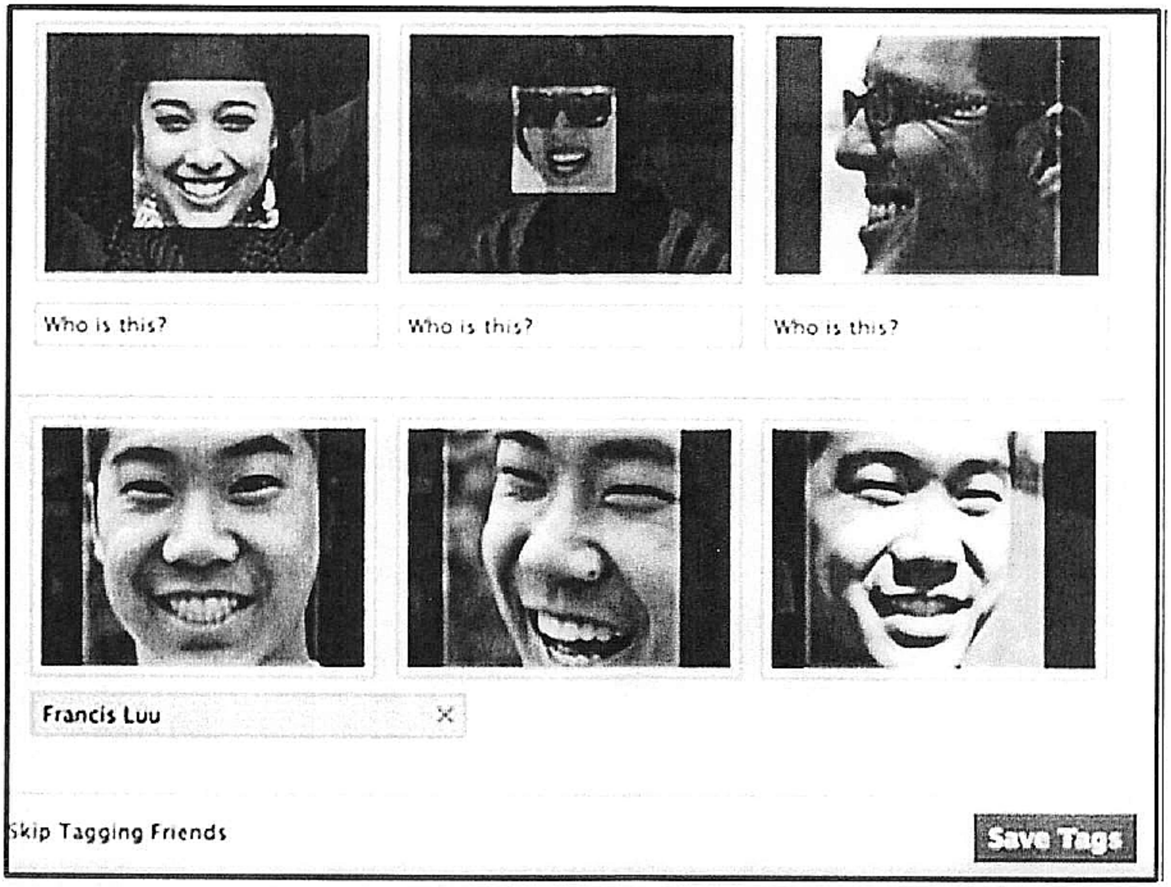


Figure 2

40. Tag Suggestions would then use the captured records of face geometry to compare the faces in the photo or video to the faces of individuals in its database.

41. If Tag Suggestions recognized and identified one of the faces appearing in the photograph, Facebook would suggest to the user the individual's name, so that the user could tag the individual.

42. Figure 3, below, shows an example of what Tag Suggestions looked like to a Facebook user:



Francis Luu

Figure 3

43. As shown, users could accept a tag suggestion from Facebook or enter in a name for each pictured individual. By entering the name of the person in a photograph once, users were unwittingly giving Facebook's facial-recognition algorithm a baseline against which to compare every other photo ever uploaded on the platform, for Facebook to see if there was a facial-map match.

44. While touting Tag Suggestions as a means to improve user experience, Facebook never disclosed that Tag Suggestions was capturing facial geometry from photographs and continuously training its AI. Little did users know that when they answered the simple question of who was in a photograph, they were helping to teach Facebook's facial-recognition technology to better map and recognize human faces for the benefit of Facebook's commercial endeavors—

and to the detriment of users' and non-users' personal safety and security. Each time a user confirmed or changed a suggested tag, Facebook's algorithms learned to "see" a little bit better and a little bit more.

45. Facebook began rolling out Tag Suggestions across the United States beginning in December 2010.

46. By June of 2011, Facebook had secretly forced millions of Texans into a facial-recognition scheme without their informed consent.

47. As a result, for the next ten years, tens of millions of Texans who appeared in media uploaded to Facebook unsuspectingly had records of their facial geometry captured by Facebook.

48. While Tag Suggestions initially captured records of face geometry only from photographs, its capabilities evolved, and it eventually captured such records from videos, as well.

49. Facebook never required users to acknowledge its capture of their records of facial geometry, much less obtained their informed consent before capturing those records. In fact, Facebook intentionally avoided using the term "biometric" to describe Tag Suggestions, because it knew that doing so would "scare people off" from using the service. Facebook's deception was calculated and complete.

50. And Facebook has never to this day obtained informed consent from non-users to capture their biometric identifiers, which happened each time a photo or video of their faces was uploaded to Facebook's platform.

51. Facebook has acknowledged as much, stating that it believes "it would be impossible to provide anyone (user or non-user) with prior notice, or obtain his consent, before" subjecting the person to its facial-recognition process.[15]

52. On information and belief, Facebook also disclosed to third parties the biometric identifiers it captured.

53. And Facebook failed to destroy the biometric identifiers it captured within a reasonable time. When information is wrongfully obtained in the first instance, holding it for any amount of time is unreasonably long.

54. After facing public backlash over its facial-recognition program, and after facing a massive lawsuit for these same biometric-capture practices in Illinois (a suit that Facebook ultimately had to settle for $650,000,000), Facebook announced, in November 2021, that it would cease use of the face-recognition feature on its Facebook social-media platform, lamenting that "the experiences it made possible have been disabled."[16]

55. Facebook has made no such commitment with respect to any of the other platforms or operations under its corporate umbrella, such as Instagram, WhatsApp, Facebook Reality Labs, or its upcoming virtual-reality metaverse.

[15] *In re Facebook Biometric Info. Privacy Litig.*, Case No. 3:15-cv-03747-JD, ECF No. 299 at 30:2–4 (N.D. Cal. Mar. 16, 2018).

[16] Facebook, https://www.facebook.com/help/mobile-touch/187272841323203 (last visited Feb. 8, 2022).

D. Facebook illegally captures biometrics through Instagram.

56. In 2012, Facebook acquired the photo-sharing site Instagram.

57. Instagram allows users to each create a personal page where they can upload photographs and videos, participate in live video broadcasts, and communicate and interact with other Instagram users.

58. Facebook has never informed its Instagram users—or non-users—that it has been capturing their biometric identifiers. On the contrary, Facebook has maintained that Instagram does not run its face-recognition technology on Instagram media. The Instagram Data Policy states, "If we introduce face-recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you." None of it is true.

59. On information and belief, Facebook has been secretly subjecting all photos uploaded to Instagram to its facial-recognition technology, with no way for Instagram users (or non-users) to know about it, let alone prevent Facebook from harvesting maps of their facial geometry.

60. Facebook has been doing this for its commercial gain, to continue to train and improve its AI apparatus and to improve Facebook's Tag Suggestions.

61. Facebook has therefore captured the biometric identifiers of millions of Texans without their informed consent, for a commercial purpose, and failed to destroy them in a reasonable time—all in violation of CUBI.

E. In Sum: Facebook exploits Texans' most sensitive data to create DeepFace.

62. Facebook's campaign of unlawful biometric capture has led to Facebook's creating the largest facial dataset in the world. That dataset is powered by DeepFace, Facebook's deep-

learning facial-recognition system.[17] DeepFace closely approaches human-level accuracy in identifying faces. And it exists only because—for over a decade—Facebook illegally and surreptitiously captured the biometric identifiers of tens of millions of Facebook and Instagram users and non-users.

63. In creating and maintaining this facial dataset, Facebook has also failed to destroy within a reasonable time the illicitly captured records of facial geometry belonging to users and non-users.

64. On information and belief, Facebook has shared the biometric identifiers it harvested from users and non-users whose images appeared on its Facebook and Instagram platforms with third parties, including other Facebook subsidiaries and related entities (the "Disclosure Parties").

65. Facebook's social-media platforms, including its eponymous social network and Instagram, share infrastructure, systems, and technology with one another and with the Disclosure Parties.

66. On information and belief, this sharing includes sharing the biometrics harvested by various platforms, which Facebook then uses to improve the algorithms that power its facial-recognition technology.

67. Facebook's capture of protected biometric identifiers in Texas is for a commercial purpose: Facebook exploits users and non-users to improve the accuracy of its own facial-

[17] Yaniv Taigman, Ming Yang, Marc'Aurello Ranzato, & Lior Wolf, *DeepFace: Closing the Gap to Human-Level Performance in Face Verification,* (Jun. 24, 2014) (Meta Research, Tel Aviv University), https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face- verification/

recognition services, to expand the datasets that enable its facial-recognition software to work, and to cement its market-leading position in facial recognition and social media.

68. Several of Facebook's patent filings further attest to Facebook's commercial purposes in training and strengthening its facial-recognition technologies. Its patents reportedly describe systems where consumers wandering in stores or standing at checkout counters have their faces scanned and matched with their social-networking profiles.

69. Until at least November 2021, Facebook never informed Texas users (or non-users) of the scope of its facial-recognition program in either its terms of use or privacy policy, or sought consent from them before capturing records of their facial geometries. Nor has it made any effort to obtain consent from the millions of Texans who have had their facial geometrics captured but who have never once used the Facebook or Instagram platforms.

70. Through these practices, Facebook has not only disregarded its users' privacy, it has also violated the DTPA and CUBI, which was designed to protect Texas residents from practices precisely like Facebook's covert facial-recognition program. In particular, Facebook has violated CUBI by failing to obtain consent prior to capturing Texans' biometric identifiers for its commercial gain, disclosing those identifiers to other entities, and failing to timely destroy them—continuously putting the well-being, safety, and security of tens of millions of Americans at risk.

CAUSES OF ACTION

Count I

Violation of Tex. Bus. & Comm. Code § 503.001(b)

71. The State re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

72. CUBI makes it unlawful for any person to "capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier." Tex. Bus. & Comm. Code § 503.001(b).

73. Facebook is a Delaware corporation and thus qualifies as a "person" under CUBI.

74. Under CUBI, a record of face geometry qualifies as a biometric identifier.

75. Facebook's practices, as alleged in the State's complaint, constitute countless captures of users' and non-users' face geometries, and therefore their biometric identifiers.

76. Each of these captures serves a commercial purpose.

77. In violation of Tex. Bus. & Comm. Code § 503.001(b), Facebook has never obtained informed consent from users or non-users before capturing their biometric identifiers.

78. Each of these illicit captures constitutes a separate violation of Tex. Bus. & Comm. Code § 503.001(b).

79. The State is entitled to a civil penalty of up to $25,000 for each of these unlawful captures of a biometric identifier. Tex. Bus. & Comm. Code § 503.001(d).

Count II

Violation of Tex. Bus. & Comm. Code § 503.001(c)(1)

80. The State re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

81. CUBI prohibits any person in possession of an individual's biometric identifier for a commercial purpose from selling, leasing, or otherwise disclosing that biometric identifier unless "(A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death; (B) the disclosure completes a financial transaction that the individual requested or authorized; (C) the disclosure is required or permitted by a federal statute

or by a state statute other than Chapter 552, Government Code [the Texas Public Information Act]; or (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant[.]" Tex. Bus. & Comm. Code § 503.001(c)(1).

82. Facebook is a Delaware corporation and thus qualifies as a "person" under CUBI.

83. Through the capture of biometric identifiers detailed herein, Facebook comes into the possession of users' and non-users' biometric identifiers.

84. Each possession of a biometric identifier serves a commercial purpose for Facebook.

85. Facebook has disclosed its captured biometric identifiers to the Disclosure Parties.

86. No user or non-user has ever consented to the disclosure of his or her biometric identifier to one of the Disclosure Parties for identification purposes in the event of that person's disappearance or death.

87. Facebook's disclosure of biometric identifiers to the Disclosure Parties did not complete financial transactions that those users or non-users have requested or authorized.

88. Facebook's disclosure of biometric identifiers to the Disclosure Parties was not required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code.

89. Facebook's disclosure of biometric identifiers to the Disclosure Parties was not made by or to a law-enforcement agency for a law-enforcement purpose in response to a warrant.

90. Each disclosure of a biometric identifier to one of the Disclosure Parties constituted a violation of Tex. Bus. & Comm. Code § 503.001(c)(1).

91. The State is entitled to a civil penalty of up to $25,000 for each of these unlawful disclosures. Tex. Bus. & Comm. Code § 503.001(d).

Count III

Violation of Tex. Bus. & Comm. Code § 503.001(c)(3)

92. The State re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

93. CUBI requires any person in possession of an individual's biometric identifier for a commercial purpose to "destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires," except if that biometric identifier was "used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period [otherwise prescribed by CUBI.]" Tex. Bus. & Comm. Code § 503.001(c)(3).

94. Facebook is a Delaware corporation and thus qualifies as a "person" under CUBI.

95. Through the capture of biometric identifiers detailed herein, Facebook comes into the possession of users' and non-users' biometric identifiers.

96. Each possession of a biometric identifier serves a commercial purpose for Facebook.

97. Facebook's possession of biometric identifiers is not in connection with an instrument or document that is required by another law to be maintained for a period longer than the period otherwise prescribed by CUBI.

98. Facebook's possession of biometric identifiers is unlawful because Facebook has not obtained informed consent for the capture that led to that possession, as alleged herein.

99. Because Facebook's possession of biometric identifiers in the first instance was unlawful, maintaining possession of these biometric identifiers for any period of time is unreasonable, and violates Tex. Bus. & Comm. Code § 503.001(c)(3).

100. Facebook has not destroyed the biometric identifiers it possesses by the first anniversary of the date the purpose for collecting the identifiers expired, in further violation of Tex. Bus. & Comm. Code § 503.001(c)(3).

101. The failure to destroy each of these biometric identifiers by the date required constitutes a separate violation of Tex. Bus. & Comm. Code § 503.001(c)(3).

102. The State is entitled to a civil penalty of up to $25,000 for each failure to destroy a biometric identifier by the required date. Tex. Bus. & Comm. Code § 503.001(d).

Count IV

Violation of Tex. Bus. & Comm. Code § 17.41, *et seq.*

103. The State re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

104. The Texas Deceptive Trade Practices Act prohibits all false, misleading, or deceptive acts or practices in the conduct of any trade or commerce.

105. Facebook, as alleged herein, has in the course of trade and commerce, engaged in false, misleading, and deceptive acts and practices declared unlawful by sections 17.46(a) and (b) of the DTPA, including:

A. Representing, directly or by implication, that Facebook does not collect the biometric identifiers of Facebook users or non-users in Texas;

B. Representing, directly or by implication, that Facebook does not collect the biometric identifiers of Instagram users or non-users in Texas;

C. Failing to disclose information—including the fact that it collects biometric identifiers—with the intent to induce Facebook users in Texas into using Facebook, which such users would not have done had the information been disclosed; and

D. Failing to disclose information—including the fact that it collects biometric identifiers—with the intent to induce Facebook users in Texas into using Instagram, which such users would not have done had the information been disclosed.

106. Under the DTPA, the State may seek a temporary restraining order or permanent injunction, and also may obtain a civil penalty to be paid to the State in an amount of up to $10,000 per violation.

TRIAL BY JURY

107. Plaintiff herein requests a jury trial and tenders the jury fee to the Harrison County District Clerk's office pursuant to Tex. R. Civ. P. 216 and Tex. Gov't Code § 51.604.

PRAYER

108. The State prays that the Court permanently enjoin Facebook from violating CUBI and the DTPA by, for example, enjoining Facebook from:

A. Capturing, maintaining, or using in any way the biometric identifiers captured in Texas without the informed consent of the relevant individual;

B. Performing facial recognition in Texas without the informed consent of all individuals subject to Facebook's facial-recognition technology; and

C. Misrepresenting, directly or by implication, that Facebook does not collect biometric identifiers.

109. Plaintiff further prays that this Court will order Facebook to:

A. Discontinue its commercial use of any information obtained through its unlawful capture of biometric identifiers in Texas;

B. Destroy the information it has collected from the unlawful capture of biometric identifiers in Texas;

C. Destroy any neural network or algorithm trained or improved using biometric identifiers unlawfully captured in Texas; and

D. Make best efforts to retrieve any information from third parties that may possess such information as a result of Facebook's unlawful disclosure of that information.

110. Plaintiff further prays that this Court will:

A. Order Facebook to pay civil penalties to the State of Texas of $25,000 for each violation of CUBI;

B. Order Facebook to pay civil penalties to the State of Texas of $10,000 for each violation of the DTPA;

C. Order the disgorgement of Facebook's assets, as provided by law and equity;

D. Order Facebook to pay pre-judgment and post-judgment interest on all monetary awards, as provided by law;

E. Order Facebook to pay all costs of court, costs of investigation, and the State's attorneys' fees, as provided by the laws of the State of Texas, including but not limited to, Tex. Gov't Code § 402.006(c); and

F. Grant that the State receive such other and further relief to which it is justly entitled.

Respectfully submitted,

Dated: February 14, 2022

KEN PAXTON
Attorney General

/s/ Shawn E. Cowles
BRENT WEBSTER
First Assistant Attorney General
brent.webster@oag.texas.gov
GRANT DORFMAN
Deputy First Assistant Attorney General
grant.dorfman@oag.texas.gov
SHAWN E. COWLES
Texas State Bar No. 24108813
Deputy Attorney General for Civil Litigation
shawn.cowles@oag.texas.gov
MURTAZA SUTARWALLA
Deputy Attorney General for Legal Counsel
murtaza.sutarwalla@oag.texas.gov
AARON REITZ
Deputy Attorney General for Legal Strategy
aaron.reitz@oag.texas.gov
NANETTE DINUNZIO
Associate Deputy Attorney General for Civil Litigation
nanette.dinunzio@oag.texas.gov
RALPH MOLINA
Special Counsel to the First Assistant Attorney General
ralph.molina@oag.texas.gov

STEVE ROBINSON
Chief, Consumer Protection Division
steven.robinson@oag.texas.gov
PEDRO PEREZ
Deputy Chief, Consumer Protection Division
pedro.perez@oag.texas.gov
JENNIFER ROSCETTI
Deputy Chief, Consumer Protection Division
jennifer.roscetti@oag.texas.gov
BRAD SCHUELKE
Assistant Attorney General, Consumer Protection Division
brad.schuelke@oag.texas.gov
DOMINIC RIBAUDO
Assistant Attorney General, Consumer Protection Division
dominic.ribaudo@oag.texas.gov
ADRIAN SEPULVEDA
Assistant Attorney General, Consumer Protection Division
adrian.sepulveda@oag.texas.gov
ZACHARY BERG
Assistant Attorney General, Consumer Protection Division
zachary.berg@oag.texas.gov

OFFICE OF THE ATTORNEY GENERAL OF TEXAS
P.O. Box 12548
Austin, Texas 78711-2548
(512) 936-026

/s/ Samuel F. Baxter
SAMUEL F. BAXTER
Texas State Bar No: 01938000
sbaxter@mckoolsmith.com
JENNIFER L. TRUELOVE
jtruelove@mckoolsmith.com
MCKOOL SMITH P.C
104 East Houston, Suite 300
Marshall, Texas 75670
(903) 923-9000
Fax: (903) 923-9099

JOHN B. CAMPBELL
jcampbell@mckoolsmith.com
MCKOOL SMITH P.C.
303 Colorado Street
Austin, Texas 78701
(512) 692-8700

LEWIS T. LECLAIR
lleclair@mckoolsmith.com
ASHLEY N. MOORE
amoore@mckoolsmith.com
MCKOOL SMITH P.C.
300 Crescent Court
Dallas, Texas 75201
(214) 978-4000

ERIC B. HALPER (*pro hac vice* to be filed)
ehalper@mckoolsmith.com
JOHN C. BRIODY (*pro hac vice* to be filed)
jbriody@mckoolsmith.com
RADU A. LELUTIU (*pro hac vice* to be filed)
rlelutiu@mckoolsmith.com
AYANA M. RIVERS (*pro hac vice* to be filed)
arivers@mckoolsmith.com
MELISSA CABRERA (*pro hac vice* to be filed)
mcabrera@mckoolsmith.com
ELIZA BEENEY (*pro hac vice* to be filed)
ebeeney@mckoolsmith.com
MCKOOL SMITH P.C.
One Manhattan West
395 Ninth Avenue, 50th Floor
New York, New York 10001
(212) 402-9400

ATTORNEYS FOR PLAINTIFF STATE OF TEXAS

/s/ Zina Bash
ZINA BASH
Texas State Bar No: 24067505
zina.bash@kellerlenkner.com
111 Congress Avenue, Suite 500
Austin, TX 78701
(501) 690-0990
KELLER LENKNER LLC

ASHLEY KELLER (*pro hac vice to be filed*)
ack@kellerlenkner.com
BEN WHITING (*pro hac vice to be filed*)
ben.whiting@kellerlenkner.com
J. DOMINICK LARRY (*pro hac vice to be filed*)
nl@kellerlenkner.com
ALEX DRAVILLAS (*pro hac vice to be filed*)
ajd@kellerlenkner.com
BROOKE SMITH (*pro hac vice to be filed*)
brooke.smith@kellerlenkner.com
KELLER LENKNER LLC
150 N. Riverside Plaza, Suite 4100
Chicago, Illinois 60606
(312) 741-522

WARREN POSTMAN (*pro hac vice to be filed*)
wdp@kellerlenkner.com
KELLER LENKNER LLC
1100 Vermont Avenue, N.W., 12th Floor
Washington, D.C. 20005
(202) 749-8334